Cybersecurity under the Ocean

Submarine Cables and US National Security

Justin Sherman

For many Americans connecting to the internet, the experience is wireless. We link up a smart television to a home router to watch Netflix from our couch; we log on to Wi-Fi in a coffee shop or office building to check email and browse social media. Terms like "cyberspace" and "the cloud" make this internet connectivity even more abstract.[1]

Despite these perceptions, the internet depends on core physical infrastructure to run. Submarine cables are one component of that infrastructure. Over five hundred of these cables, laid across the ocean floor around the world, carry upward of 95 percent of intercontinental internet traffic.[2] They bring together companies and government organizations from around the world, sometimes costing hundreds of millions of dollars to construct and place.[3] Without these cables, the global internet as we know it would not exist.

This paper describes why submarine cables are critical to global internet security and resilience—as well as to economic security, national security, and crisis planning. It also describes some of the key government organizations with stakes in the issue, ranging from the Department of Transportation to interagency committees focused on foreign influence in the United States.

The paper then analyzes three growing risks to submarine cables' security and resilience: (1) authoritarian governments increasingly influencing the internet's physical layout through cables; (2) companies deploying "remote network management tools" that expose cables to increased cybersecurity risk; and (3) more data, and more sensitive data, traveling via cables. It concludes with a discussion of how national security policy makers should better understand and mitigate these risks.

Specifically, Congress should consider statutorily authorizing the committee that conducts security reviews into foreign participation in the US telecommunications sector. It should also consider providing more funding for a new government program to place ships on standby to

A Hoover Institution Essay

Aegis Series Paper No. 2301

repair national security–relevant undersea cables. Beyond that, the State Department should better integrate cables into its capacity-building work, and US-based submarine cable owners should increase their efforts to share threat information with one another and with the government. The US should work with allies and partners around the world to better protect cables' security. And all the while, policy makers must not forget the basics. Threats from malicious actors like Beijing and Moscow loom large in some minds. At the same time, many cables remain critically vulnerable to damage and disruption from natural weather events and accidents—and those core resilience issues must be part of the conversation, too.

THE BASICS OF SUBMARINE CABLES

In the 1820s, Baron Schilling von Canstatt used a cable—insulated wires laid on the riverbed of the Neva River—to detonate gunpowder mines near St. Petersburg.[4] England and the United States laid the first transatlantic subsea telegraph cable in 1856;[5] and in 1858, the British government sent the inaugural message: Queen Victoria praised President James Buchanan for cooperating to build it.[6] More than five hundred submarine cables currently carry intercontinental internet traffic around the world.[7]

Undersea cables vary in thickness from about one to twenty centimeters. Typically, it is only the inner, hair-thin fiber in a cable—subsequently encased in gel, copper, and whatever else—that transmits internet data across the cable, from emails to social media posts to sensitive government documents.

Every single cable has at least two "landing points," or places where the cable meets a shoreline. At this landing point, the cable operator in the respective country will have a "landing station." These facilities have several purposes, including terminating an international cable, supplying power to the cable, and acting as a point of domestic or international connection.[8] Landing stations are also places where the physical security of a cable is exposed, since individuals can access both the cable itself and the equipment used to keep the cable operational.

The owner of a cable is not always the same entity as the owner of a landing station. Further, there are often different companies involved in financing and owning the cable, building the inner components of a submarine cable (such as the inner fiber-optic strand and the outer cable membrane), and laying the cable along the ocean floor.[9] Each of these components involves a technological supply chain. They also each introduce opportunities for nation-states and other actors to undermine the security of submarine cables hauling internet traffic around the world.

Several US government organizations have a specific focus already on this issue, including the following:

- Federal Communications Commission (FCC): The FCC issues licenses for companies that own and operate submarine cables and landing stations in the US.[10] It also participates in

national security reviews of foreign telecom participation in the US and issues Section 214 licenses to foreign telecommunications carriers seeking to operate in the US.[11]

- Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector: Previously known as Team Telecom, the committee is an interagency body that investigates foreign participation in the US telecommunications sector for national security risks. The attorney general chairs the committee, and the Departments of Justice, Defense, Homeland Security, and others participate in the review process.[12] The committee is not statutorily authorized, and it cannot make the FCC revoke licenses. However, it can recommend that the FCC revoke licenses, and, conversely, the FCC can refer foreign telecom activities to the committee for a security review. From 2013 to 2019, for example, the FCC referred an average of 16 percent of submarine cable and international Section 214 licenses to the committee for review.[13]

- Committee on Foreign Investment in the United States (CFIUS): This interagency committee investigates foreign investments in US companies that have implications for national security. While, as noted above, Team Telecom is the primary committee focused on foreign telecom activity, CFIUS could also theoretically review investments in telecom infrastructure by foreign entities. CFIUS is statutorily authorized; the US president has the statutory authority to force a company to stop pursuing or to undo a transaction that would pose certain risks to national security.[14] (President Obama did so in December 2016, for example, when he issued an executive order blocking a proposed acquisition of a US subsidiary of a German semiconductor firm.[15])

- Department of Transportation (DoT): The DoT has been standing up the Cable Security Fleet, which was authorized in the National Defense Authorization Act for Fiscal Year 2020. It designated two government-authorized, privately owned ships to be on standby to repair damaged cables with relevance to US national security. Importantly, this definition does not limit the ships to repairing only cables that touch US borders.[16]

- Department of the Navy: The US Navy helped lay the world's first transatlantic telegraph line in the 1850s, and it maintains one ship designed to survey the ocean as well as install and maintain submarine cables.[17]

This list is not comprehensive. Other government organizations, such as the Department of Justice,[18] Department of State,[19] Coast Guard,[20] and National Security Agency,[21] have some relationship with submarine cable infrastructure as well.

SUBMARINE CABLES AND NATIONAL SECURITY

Undersea cables are an information gold mine. They carry everything from Zoom and FaceTime video calls with family members, social media posts, and emails with colleagues to e-commerce transactions, business information, and sensitive government and military

communications. Nation-states view submarine cables as an attractive spying opportunity for exactly this reason. In the late nineteenth century, British intelligence tapped into an international hub of telegram cables in Porthcurno—a small coastal village in England, within the government's territory—to gain eavesdropping advantage.[22] During the Cold War, the US National Security Agency (NSA) sent divers and submarines to tap Russian submarine cable infrastructure with recording devices.[23] Today, the same kind of espionage persists.

Edward Snowden's leaks of classified US documents in 2013 revealed programs run by the NSA and the United Kingdom's Government Communications Headquarters (GCHQ) to tap into dozens of submarine cables globally.[24] Australian intelligence sources have spoken to journalists about Australian-Singaporean cooperation to access communications transmitted over submarine cables.[25] Taiwan's Foreign Ministry has warned of Chinese cable investments in the Pacific as a means for Beijing to spy on other countries and steal valuable data.[26] In a world where every country spies—and where submarine cables are a valuable place to target espionage—the list goes on.

Damage to cables is another potential threat to internet traffic. In 2008, a ship off the Egyptian coast accidentally severed an undersea cable, leaving seventy-five million people in the Middle East and India with limited internet access.[27] Undersea earthquakes and other weather events can likewise damage cables and temporarily disrupt their ability to haul internet traffic. This is not to say that damaging one cable will take down the global internet—far from it—but it could disrupt traffic flows in a way that undermines connectivity to a region.[28]

The US and other large countries are linked to the global internet through many submarine cables, as well as cables that traverse land. Some parts of the world, however, are particularly vulnerable to cable disruptions. In January 2022, a devastating underwater volcanic eruption and tsunami hit the archipelagic nation of Tonga. The country has just one submarine cable linking it to the rest of the world, and when the disaster hit, its internet went out completely.[29] In October 2022, the undersea cable linking the Shetland Islands to the rest of Scotland was damaged, apparently by accident; it caused widespread internet broadband outages and slowdowns in mobile phone service.[30] Clearly, these places are more dependent on just a few cables, or even a single cable, staying operational.

Even though most documented cases of cable damage are due to accidents, national security concerns about deliberate attacks persist. A 2017 US Office of the Director of National Intelligence report determined that a cyberattack on overland, last mile, or near-shore submarine cables could have a high impact on their functionality.[31] In 2021, the US intelligence community's Annual Threat Assessment found that "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis."[32] Researchers at NATO's Cooperative Cyber Defence Centre of Excellence have written that "losing the ability to send and receive sovereign data via an undersea cable may be grave for individuals as well as companies and nations."[33] More recently, Russia's illegal war on Ukraine, initiated by Vladimir Putin's regime, has prompted US national security conversations about internet

infrastructure risks to Ukraine and to Europe in the current conflict, to Taiwan if Beijing invades, and other scenarios.[34]

Whether protecting undersea cables from routine foreign espionage, ensuring that cyber-criminals cannot hack into submarine cable systems, or safeguarding the infrastructure against nation-state disruption, policy makers must grapple with the importance of cable security and resilience for national and economic security. At least three major sets of risks stand out: authoritarian governments increasingly influencing the internet's physical layout through cables; companies deploying "remote network management tools" that expose cables to increased cybersecurity risk; and more data, and more sensitive data, traveling over cables.

RISK 1: AUTHORITARIAN INFLUENCE ON CABLES

Multinational cooperation is a normal and necessary part of developing and maintaining the undersea cable network. Cable projects can take years of work and cost hundreds of millions of dollars—and oftentimes multiple companies, or companies and government organizations, will step in to fund those projects. Financing for a single submarine cable, for example, might come from multiple companies incorporated in multiple countries.[35] Then, a company from one of those countries might be contracted to actually lay the cable across the ocean floor.[36]

Beyond the financing of a cable, every cable needs at least two landing stations, and organizations from multiple countries are frequently involved to manage those different connection points. The numbers bear out the reality of largely beneficial, international cooperation: as of 2021, 65 percent of cables worldwide had a single owner, and about 33 percent had multiple owners.[37] Simultaneously, though, the many actors involved in cable financing, construction, laying, and management create numerous opportunities for governments and government-linked actors to exert influence over submarine cables and the broader submarine cable network. In particular, there are organizations putting money into cables or otherwise influencing the infrastructure who could threaten the network's security and resilience.

China and Russia provide two relevant case studies. Chinese companies have greatly increased their investments in submarine cable infrastructure. Many of these companies are state-owned or state-controlled. Russian companies do not have an equally extensive economic investment in submarine cables around the world, but national security professionals have raised concern about Russian submarine activity near cables. The potential influence these governments can exert on cables comes in many forms, which highlights the risks present in some governments' influence on cables.

CHINESE INFLUENCE

The main Chinese investors in submarine cables include China Mobile, China Telecom, China Unicom, CITIC Telecom International, and CTM (Companhia de Telecomunicações

de Macau).[38] China Mobile, China Telecom, and China Unicom are all state-owned telecommunications companies.[39] CITIC Telecom International and CTM are both controlled by the Chinese government.[40] In recent years, these companies have ramped up their spending on submarine cable infrastructure. For example, until 2021, China Telecom owned just two cables (one from 1999 and one from 2016).[41] But as of 2021, it has investments in twelve different submarine cables.[42] China Unicom, to give another example, had not owned a submarine cable until 2021—when it had investments in eleven.[43]

Investing in cables potentially provides the Chinese government with several vectors of influence. Controlling a landing station enables the government to better spy on the traffic moving across the infrastructure. As of 2021, about two-thirds of the cable projects in which China Mobile, China Telecom, and China Unicom have vested interests had at least one landing station in China.[44] Broadly, financing a cable allows an actor—whether a company or a government—to influence where the cable is laid, which parts of the world it connects, and how quickly it connects them.[45] This can encourage economic dependence on the entity laying the cable to a country. It can also empower that cable investor to shape the path of internet traffic. While internet traffic does not always take the most intuitive route from its origin to its destination, placing a significantly faster and higher-bandwidth cable alongside a slower and lower-bandwidth one could encourage more traffic to move across the new cable.[46] This could potentially encourage traffic to move through points in the world that an entity, like the Chinese government, monitors.

The Justice Department raised this exact concern when the US government blocked the Pacific Light Cable Network (PLCN) in June 2020—an undersea cable project involving Google, Facebook, a New Jersey–based telecom, and a Hong Kong–based telecom owned by a Chinese company. It cited concerns about both Chinese government espionage and the project's connections to "state-owned carrier China Unicom."[47] The Justice Department then cited the following about the People's Republic of China (PRC):

> 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 US 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.[48]

The Justice Department subsequently entered into national security agreements with Google and Facebook (Meta) around the cable project—in other words, security mitigation agreements—and recommended the FCC condition any license to operate the cable on compliance with the agreements.[49] In March 2022, the Chinese company Dr. Peng Telecom & Media Group sold its stake in the cable project to Meister United, a company registered in the British Virgin Islands.[50]

In addition to possible Chinese state influence through cable owners, there is a risk of Chinese state influence through the cable builder. Companies that build parts of a cable—whether a

firm that makes optical fiber, like Corning; or a firm that lays a cable underwater, like SubCom—could potentially be compelled by a government to build backdoors into equipment before deployment. This is distinct from hacking into a cable once it is operational or tapping a cable once laid (e.g., tapping the cable deep underwater, underwater close to the shoreline, or on land). Unlike those actions, which occur once a cable has been deployed and has data moving across it, this cable-builder-influence vector would occur before a cable is even put on the ocean floor—and possibly before companies are monitoring for nation-state interference.

The Chinese company Huawei Marine has no publicly identified ownership stake in the submarine cable network. But it has been heavily involved in building and repairing cables laid around the world. In October 2020, Commissioner Geoffrey Starks of the FCC, in a prepared statement that accompanied the promulgation of a new FCC rule governing telecom applications with foreign ownership, stated that Huawei Marine has "built or repaired almost a quarter of the world's cables."[51] (The company has been the subject of numerous US government national security actions, most recently the FCC banning the future sale of Huawei equipment in the United States.[52]) Huawei subsequently announced it was divesting Huawei Marine about one month after President Trump blacklisted Huawei in 2019.[53] In November 2020, it was rebranded as Huahai Communication Technology Co., Ltd.[54] Private-sector involvement in laying cables, once again, is completely normal. Nonetheless, the question comes down to the risk that a particular company is a vector of geopolitical influence projection. Huawei Marine presents risks in this vein given the control the Chinese government exerts over technology companies—especially strategically important technology companies operating from within its borders.

RUSSIAN INFLUENCE

Russian investments in submarine cable infrastructure are not as significant or globally reaching as those from Chinese companies. Western governments are increasingly concerned, though, about Russian military activity near submarine cables. The Finnish government has reportedly expressed worries about Russian land acquisitions abroad near key telecommunications links, such as around the Turku archipelago.[55] In 2017, the commander of NATO's submarine forces said that "[w]e are now seeing Russian underwater activity in the vicinity of undersea cables that I don't believe we have ever seen."[56] He added, "[w]e know that these auxiliary submarines are designed to work on the ocean floor, and they're transported by the mother ship, and we believe they may be equipped to manipulate objects on the ocean floor."[57]

The US intelligence community's aforementioned 2021 threat assessment assessed that Russia continues to target undersea cables. Britain's newly appointed head of the armed forces entered the fray in January 2022. He said there has been a "phenomenal increase in Russian submarine and underwater activity" over the past two decades and that the Russian government could "put at risk and potentially exploit the world's real information system, which is undersea cables that go all around the world."[58] Controlling and targeting the physical aspects of the internet, from infrastructure to people, remains critical to Russian security service and military thinking about information control as well.[59]

RISK 2: INTERNET-CONNECTED, REMOTE CABLE MANAGEMENT SOFTWARE

Companies that manage cable infrastructure are turning more to internet-connected, "remote network management systems" to lower the costs of doing so. In the process, however, they expose cable infrastructure to greater cybersecurity risk. Not only could nation-states and other malicious actors (like criminals or terrorists) tap into or damage cable infrastructure at landing stations, near a shoreline, or deep underwater, they can also hack into systems to disrupt signal flows. Securing this software is important to protecting cables' security and resilience.

Historically, on-site personnel managed the operating centers located at or near landing stations. Cable operators also managed the infrastructure at landing stations through systems not directly connected to the internet, such as systems to help ensure signal connectivity and manage power flows to cables.[60] Now, however, more companies are connecting landing stations and operating centers to remotely controllable software.

Using remote tools allows a company to lower its costs, because the software does not require personnel (or as many personnel) to be on-site. Company employees can work from afar, monitoring the data sent over cables and even altering fiber-optic signals through a virtual interface. This kind of software also helps cable operators deal with cable complexity: increasingly sophisticated fiber-optic technology requires cable operators to manage complex signal configurations.[61]

But risks persist. Introducing a virtualized layer of control over cable systems opens another vector through which different actors, especially intelligence agencies, can hack into landing stations and operating centers. Poor security practices by some of these remote software vendors magnifies this risk. For example, some companies poorly secure communications between the virtualization interface and the physical infrastructure that the interface controls.[62] The relative lack of diversity among remote management system vendors creates additional risks[63]—compromises of one technology (like introducing a backdoor in a software update or developing a new software exploit) could have wider effects on cables. The fact that many remote network management systems use common operating systems, like Linux or Microsoft Windows, rather than more obscure interfaces that raise the barrier to understanding makes it more likely a hacker can easily understand the software. And the way vendors update the software and can control it once deployed could introduce security risks as well.

Hackers could break into these systems to disrupt or degrade cable signals.[64] This fear was nearly borne out at least once, in April 2022: the Department of Homeland Security "disrupted" a cyberattack on an unnamed telecommunications company's system in Hawaii, which it described as a "significant breach involving a private company's servers associated with an undersea cable."[65] While information was sparse, the department's statement added that the credentials the hackers acquired could be used to "just shut down communications."[66]

Protecting this software is difficult because many governments, the US government included, do not impose strong cybersecurity requirements on companies making software for this infrastructure. For example, the FCC has several security line-item questions it asks of companies applying for a submarine cable landing license,[67] but this is not a procurement requirement, and other parts of the government engaged in contracting have not made security requirements for submarine cable stations a priority. It is also difficult because consortia of companies and even governments invest in cables all at once—making coordination of security efforts sometimes difficult. Governments might also require companies incorporated in their borders to enable them to surveil the infrastructure in ways that create risks of others piggybacking on that surveillance.

RISK 3: EXPLOSION IN DATA—AND SENSITIVE DATA

In addition to the aforementioned authoritarian influence projection and deployments of remote cable management software, more data—and more sensitive data—is flowing over submarine cables. This makes protecting cables' security and resilience even more urgent for US policy makers.

The COVID-19 pandemic has shifted more living, learning, and working online in ways that have not completely reverted to the pre-pandemic status quo. Cloud computing is driving more data online too, as companies in the transportation, energy, defense, health, and financial sectors, among others, move data off previously backend, in-house systems to internet-linked cloud networks.[68] Fifth-generation cellular network technology, or 5G, will similarly contribute to a massive increase in data routed over undersea cables. Even though much of the 5G discussion focuses on the network's software-driven nature, 5G will not eliminate the need for undersea cables. On the contrary, when a cell phone makes a request to a cell tower for internet content, that cellular network may be retrieving data from the global internet that crosses a submarine cable. This will not change with 5G—and the more that 5G networks promise higher data speeds and bandwidth, the more they will depend on fast infrastructure (including both undersea and fiber-optic land cables) to deliver on those promises.[69]

Coincident with this shift toward more data, and more sensitive data, moving across submarine cables, US cloud and internet companies are ramping up their investments in this infrastructure. US private-sector investments were previously led by traditional telecoms, like AT&T and Verizon. Now, the fast-growing and newly dominant US investors in cables are Amazon, Facebook, Google, and Microsoft. As the *Submarine Telecoms Forum*'s 2021/2022 industry report put it, these four companies "are no longer reliant on Tier 1 network operators to provide capacity and are simply build(ing) the necessary infrastructure themselves."[70] Google went from zero cable investments to two in 2018, to three in 2020, and to ten in 2021; Facebook went from zero cable investments to three in 2020 and to five in 2021.[71] All of these companies have more investments planned in the coming years, where they can profit off both leasing access to cable infrastructure and expanding their own digital infrastructural footprint.

This may provide the US government with a unique point of leverage over cable infrastructure; American policy makers could opt, for instance, to require that these companies have greater security—thereby ensuring the US has a greater influence than some other countries have on securing the cable network globally. As of 2021, about 22 percent of cables worldwide had at least one US private owner.[72] But these investments come with a growing company responsibility to secure the infrastructure as well, and they raise questions about concentrated corporate control over the internet. For instance, Facebook controls a major social media platform and is now investing in submarine cables. Google controls a globally dominant search engine, operates a host of other services (like popular email, online document-editing, and maps applications), is one of the three major cloud providers (alongside Microsoft and Amazon), and is greatly increasing its investments in submarine cable infrastructure. The market influence of a few companies is expanding along much of the internet "stack."

THE NATIONAL SECURITY RESPONSE

Citizens, the private sector, and the government have a stake in safeguarding the security and resilience of submarine cables. Enabling unfriendly foreign actors to spy on internet traffic can undermine US national security and enable other malicious activities, like the theft of trade secrets and other proprietary company and scientific information traversing the internet. Communications disruptions could also cause public backlash, degrade people's ability to access online services, and undermine economic and national security once business, government, and other communications are slowed. It is also in the government's interest to ensure damaged cables are repaired quickly—especially given that, again, most publicly recorded cable disruptions are due to natural weather events or accidents.

Policy makers have several options available to better protect the security and resilience of submarine cable infrastructure. Congress should statutorily authorize Team Telecom to provide it with the necessary funding, review authority, and formal structure to better screen foreign telecoms that own cable infrastructure.[73] A lack of funding for both CFIUS and Team Telecom has led many of the agencies working on both groups to focus more on CFIUS reviews.[74] The review committee has additionally lacked a formal structure for conducting security reviews and a formal process for monitoring company compliance with security agreements.[75] Congress should also consider increasing the funding for the Cable Security Fleet—given the importance of rapid cable repairs to internet connectivity, economic security, and national security.[76]

Other options abound. The State Department should pursue confidence-building measures to strengthen norms against nation-states damaging or disrupting submarine cables, such as in the event of a conflict or as a means of coercing another country.[77] It should also conduct a study on ways to better integrate the security and resilience of core internet infrastructure into its capacity-building efforts overseas.[78] Without sufficient security and resilience, it is easier for malicious actors and routine accidents to disrupt internet connectivity. Submarine cable owners, for their part, should work with federal, state, and local authorities to establish a specific information sharing and analysis center (ISAC) for submarine cables, which does not

currently exist.[79] They should also increase their investments in strategies for infrastructure security—and work with federal authorities to ensure the government has requisite information about known threats to undersea cables. The Defense Department and other government organizations can also consider how federal procurement requirements and other levers could better incentivize cable operators to ensure their remote software tools are sufficiently secure.

International cooperation is also vital. As Chinese investments in cable infrastructure grow, the US can work with allies like Japan to track these activities and develop mechanisms to understand relevant security risks.[80] The US and the European Union could pursue a common framework to understand cable investments, cable projects, and their potential security implications. While the EU does not have the power to grant licenses to build digital infrastructure,[81] it can forge policy and political dialogue on submarine cables at the bloc level, and its member states can put in more comprehensive screening structures.[82] All the while, the US and its allies and partners cannot lose focus on the basics of ensuring connectivity, too: the threat of malicious disruptions aside, cable resilience in the face of accidents and climate-related disasters is vital.

To be clear, and realistic, there are many impediments to enhancing the security and resilience of submarine cable infrastructure. It can already be difficult to coordinate security decisions and damage repairs for cables that link multiple countries and may involve management or ownership by numerous companies and governments. Language barriers, cultural barriers, and legal barriers can all come into play.[83] Further, many national security conversations about cybersecurity focus lately on the digital—such as with encryption, data protection, and artificial intelligence—and can overlook the physical elements of the internet that need safeguarding, too. The US government, as with any other, only has so much budget for cybersecurity.

Increasing the resources for CFIUS and the resources and authorities for Team Telecom to ensure protection of submarine cable infrastructure seems to be one of the most politically feasible policy actions in this area. CFIUS is playing a growing role in national security, with many reviews focused lately on data and technology issues, and both the Trump and Biden administrations have generated a continued executive branch attention to telecommunications security, particularly vis-à-vis concerns about Chinese government influence through devices and underlying infrastructure. Many of the companies who own submarine cables also engage in other cybersecurity information-sharing efforts, such as in the cloud security space. Incentivizing or encouraging them to do more threat-sharing and security investment around cables should not be as big a lift, either. Likely, some of the bigger political challenges would lie around imposing additional security requirements to an ever-growing list of Federal Acquisition Regulation items—as well as around coordinating submarine cable security efforts with international partners.

Submarine cables underpin the internet as we know it. Protecting their security and resilience, in the face of growing risks, is essential to keeping people online and securing their data into the future.

NOTES

1. This paper draws on a previously published study with the Atlantic Council's Cyber Statecraft Initiative: Justin Sherman, Atl. Council, Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security 4 (2021), https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf [https://perma.cc/U6AJ-32X5].

2. *Submarine Cables*, Nat'l Oceanic & Atmospheric Admin., https://www.noaa.gov/submarine-cables [https://perma.cc/UWN6-29NU]; *Submarine Cable Frequently Asked Questions*, TeleGeography, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions [https://perma.cc/8QGQ-XAYR].

3. *See, e.g.*, Paul Lipscombe, *Google officially launches Equiano subsea cable*, Data Ctr. Dynamics (Sept. 5, 2022), https://www.datacenterdynamics.com/en/news/google-officially-launches-equiano-subsea-cable/?referral=www.penta-code.com [https://perma.cc/5W2N-46VD]; Mike Schuler, *SubCom Awarded $600 Million Contract to Build Fiber-Optic Subsea Cable from Singapore to France*, gCaptain (June 27, 2022), https://gcaptain.com/subcom-awarded-600-million-contract-to-build-fiber-optic-subsea-cable-from-singapore-to-france/ [https://perma.cc/NE7D-A3MY]; Amit Chowdhry, *Google Invests in $300 Million Underwater Internet Cable System* to *Japan*, Forbes (Aug. 12, 2014, 11:37 AM), https://www.forbes.com/sites/amitchowdhry/2014/08/12/google-invests-in-300-million-underwater-internet-cable-system-to-japan/ [https://perma.cc/3W2S-HJSU].

4. Lionel Carter et al., U.N. Env't Programme, Submarine Cables and the Oceans: Connecting the World 11 (2009), https://digitallibrary.un.org/record/681380/files/ICPC_UNEP_Cables.pdf [https://perma.cc/XC8C-EBRL].

5. Geoff Huston, *At the Bottom of the Sea: A Short History of Submarine Cables*, Asia Pacific Network Info. Ctr. (Feb. 12, 2020), https://blog.apnic.net/2020/02/12/at-the-bottom-of-the-sea-a-short-history-of-submarine-cables [https://perma.cc/B9C6-PWVD].

6. Becky Little, *The First Transatlantic Telegraph Cable Was a Bold, Short-Lived Success*, Hist. (Oct. 28, 2021), https://www.history.com/news/first-transatlantic-telegraph-cable [https://perma.cc/5CEN-ZAKK].

7. *See Submarine Cable Map*, TeleGeography, https://www.submarinecablemap.com [https://perma.cc/RF7E-XBQ9]; *Submarine Cable Frequently Asked Questions*, *supra* note 2.

8. Justin Sherman, Atl. Council, Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security 4 (2021), https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf [https://perma.cc/U6AJ-32X5].

9. *See, e.g.*, Steve Scott, *Subsea Cable Sector Needs a New Financing Model*, Submarine Telecoms F., Mar. 2020, at 34, 34–37, https://issuu.com/subtelforum/docs/subtel_forum_111 [https://perma.cc/AM7N-5CLE]; U.S. Off. of the Dir. of Nat'l Intel., Threats to Undersea Cable Communications 11 (2017), https://permanent.fdlp.gov/gpo149138/12017AEPThreatstoUnderseaCableCommunications.pdf [https://perma.cc/6CAM-LMM3].

10. *Submarine Cable Landing Licenses*, U.S. Fed. Commc'ns Comm'n, https://www.fcc.gov/research-reports/guides/submarine-cable-landing-licenses [https://perma.cc/A64H-M7ZY].

11. *International Section 214 Application Filing Guidelines*, U.S. Fed. Commc'ns Comm'n, https://www.fcc.gov/research-reports/guides/international-section-214-application-filing-guidelines [https://perma.cc/M9NM-GBDM]; Patricia Moloney Figliola et al., Cong. Rsch. Serv., R47192, The Federal Communications Commission: Selected Issues Under Consideration 10–12 (2022), https://crsreports.congress.gov/product/pdf/R/R47192/2 [https://perma.cc/F6JD-KQJM].

12. Exec. Order No. 13913, 85 Fed. Reg. 19643, 19643–44 (Apr. 4, 2020).

13. Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, 35 FCC Rcd. 10927, 10930 ¶ 7 (2020) [hereinafter Process Reform for Executive Branch Review], https://docs.fcc.gov/public/attachments/FCC-20-133A1.pdf [https://perma.cc/KM66-K7T8].

14. *CFIUS Laws and Guidance*, U.S. Dep't Treasury, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-laws-and-guidance [https://perma.cc/G9V6-A86S].

15. Larry G. Franceski, Stephen M. McNabb & Kim Caine, *President Obama Blocks Proposed Chinese Acquisition of Controlling Interest in German Chip Maker*, Norton Rose Fulbright (Dec. 2016), https://www.nortonrosefulbright.com/en-us/knowledge/publications/4a3ee7bd/president-obama-blocks-proposed-chinese-acquisition-of-controlling-interest-in-german-chip-maker [https://perma.cc/5TU3-FQ7W].

16. *See* National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 53202, 133 Stat. 1198, 1989-90 (codified at 46 U.S.C. § 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.").

17. *NSCPO Background*, Naval Facilities Eng'g Sys. Command, https://www.navfac.navy.mil/Business-Lines/Design-and-Construction/Products-and-Services/NAVFAC-Ocean-Facilities-Office/Naval-Sea-Floor-Cable-Protection-Office/NSCPO-Background/ [https://perma.cc/T5WR-RKGD]; *see also* Bob Fredrickson & Catherine Creese, *Navy Undersea Cable Systems*, 35 Submarine Telecoms F., Nov. 2007, at 39, https://www.navfac.navy.mil/Portals/68/Documents/Business-Lines/Design-and-Construction/nscpo%20article%202.pdf [https://perma.cc/A4WV-F88R].

18. *See, e.g., Team Telecom Recommends the FCC Deny Application to Directly Connect the United States to Cuba Through Subsea Cable*, U.S. Dep't of Just. (Nov. 30, 2022), https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through [https://perma.cc/ZKK3-YMK7].

19. *See, e.g., Joint Statement on Improving East Micronesia Telecommunications Connectivity*, U.S. Dep't of State (Dec. 11, 2021), https://www.state.gov/joint-statement-on-improving-east-micronesia-telecommunications-connectivity/ [https://perma.cc/LM64-NS8X].

20. *See* Safety Zone, 33 C.F.R. pt. 165, https://public-inspection.federalregister.gov/2022-12058.pdf [https://perma.cc/P3AZ-BZYP].

21. *See* 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/ [https://perma.cc/2LJW-7AKG].

22. Ben Buchanan, The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics 16–17 (2020).

23. Matthew Carle, *The Mission Behind Operation Ivy Bells and How It Was Discovered*, Mil., https://www.military.com/history/operation-ivy-bells.html [https://perma.cc/H4XC-8QZP]; Khazan, *supra* note 21.

24. *See, e.g.*, Richard Chirgwin, *Snowden Doc Leak Lists Submarine'd Cables Tapped by Spooks*, Register (Nov. 26, 2014, 5:02 UTC), https://www.theregister.com/2014/11/26/snowden_doc_leak_lists_all_the_compromised_cables/ [https://perma.cc/BAP9-7ASR].

25. Philip Dorling, *Australian Spies in Global Deal to Tap Undersea Cables*, Sydney Morning Herald (Aug. 29, 2013, 3:00 AM), https://www.smh.com.au/technology/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html [https://perma.cc/2A9R-KJNM].

26. David Brennan & John Feng, *Taiwan Says China Wants to Spy on Nations, Steal Data Through Undersea Cable Networks*, Newsweek (Dec. 18, 2020, 5:30 AM), https://www.newsweek.com/taiwan-china-spy-nations-steal-data-undersea-cable-networks-kiribati-connectivity-project-1555849 [https://perma.cc/33PL-GPMW].

27. Bobbie Johnson, *How One Clumsy Ship Cut off the Web for 75 Million People*, Guardian (Feb. 1, 2008, 6:47 AM), https://www.theguardian.com/business/2008/feb/01/internationalpersonalfinancebusiness.internet [https://perma.cc/RHY7-BTVV].

28. Matt Burgess, *The Most Vulnerable Place on the Internet*, WIRED (Nov. 2, 2022, 7:00 AM), https://www.wired.com/story/submarine-internet-cables-egypt [https://perma.cc/Z398-SUGH].

29. Ian M. Ralby & Justin Sherman, *Tonga's Devastating Volcanic Eruption Has Left the Island Without Internet*, SLATE (Jan. 21, 2022, 5:11 PM), https://slate.com/technology/2022/01/tonga-volcano-internet-underseas-cables.html [https://perma.cc/2CVH-AHY8]; Jane Wakefield, *How will Tonga's broken internet cable be mended?*, BBC NEWS (Jan. 24, 2022), https://www.bbc.com/news/technology-60069066 [https://perma.cc/CTK5-BEF3].

30. *Damaged Cable Leaves Shetland Cut Off from Mainland*, BBC NEWS (Oct. 20, 2022), https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102 [https://perma.cc/DFW5-ADT9]; Derrick Bryson Taylor & Christine Chung, *Shetland Cut Off from the World After Undersea Cable Breaks*, N.Y. TIMES (Oct. 21, 2022), https://www.nytimes.com/2022/10/20/world/europe/shetland-scotland-outage.html [https://perma.cc/AEX8-2UQA].

31. U.S. OFF. DIR. NAT'L INTEL., *supra* note 9, at 7.

32. U.S. OFF. DIR. NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 10 (2021), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf [https://perma.cc/9FQK-U3Z2].

33. NATO COOP. CYBER DEF. CTR. EXCELLENCE, STRATEGIC IMPORTANCE OF, AND DEPENDENCE ON, UNDERSEA CABLES 3 (2019), https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf [https://perma.cc/8Y3K-VE5U].

34. *See, e.g.*, Philip Heijmans, Cindy Wang & Samson Ellis, *Taiwan Tensions Raise Alarms Over Risks to World's Subsea Cables*, BLOOMBERG (Oct. 27, 2022, 5:00 AM), https://www.bloomberg.com/news/articles/2022-10-27/us-china-tensions-over-taiwan-puts-focus-on-underwater-internet-cables?leadSource=uverify wall [https://perma.cc/85KP-K9VW]; Mark Magnier, *Undersea internet cables a major vulnerability in any potential Taiwan attack, report finds*, S. CHINA MORNING POST (Sept. 1, 2022, 12:41 AM), https://www.scmp.com/news/china/military/article/3190898/report-about-potential-attack-taiwan-focuses-vulnerability [https://perma.cc/5WBJ-XGL3]; Mark Scott, *Will Russia attack undersea internet cables next?*, POLITICO (Sept. 29, 2022, 6:28 PM), https://www.politico.eu/article/everything-you-need-to-know-about-the-threat-to-undersea-internet-cables/ [https://perma.cc/S8RQ-AUYK].

35. U.S. OFF. DIR. NAT'L INTEL., *supra* note 9, at 11–12.

36. *Id*.

37. SHERMAN, *supra* note 8, at 7.

38. *Id*. at 12–13.

39. *Id*.

40. *Id*.

41. *Id*. at 13.

42. *Id*.

43. *Id*.

44. *Id*. at 14.

45. For example, Facebook has made investments in internet infrastructure in Africa alongside, and as part of, company efforts to expand market share across the continent. *See, e.g.*, Nesrine Malik, *How Facebook took over the internet in Africa – and changed everything*, GUARDIAN (Jan. 20, 2022, 5:00 EST), https://www.theguardian.com/technology/2022/jan/20/facebook-second-life-the-unstoppable-rise-of-the-tech-company-in-africa [https://perma.cc/SG8E-BD56]; Ryan Browne, *Facebook is building a huge undersea cable around Africa to boost internet access in the continent*, CNBC (June 2, 2020, 4:03 AM), https://www.cnbc.com/2020/05/14/facebook-building-undersea-cable-in-africa-to-boost-internet-access.html [https://perma.cc/R9SL-7ENB]; Robert Pepper, *Facebook Connectivity Investments to Deliver Over $200 Billion in Economic Benefits*, FACEBOOK (July 6, 2020), https://about.fb.com/news/2020/07/facebook-connectivity-economic-benefits [https://perma.cc/5ZUH-8MQR]; Maeve Shearlaw, *Facebook lures Africa with free internet – but what is the hidden cost?*, GUARDIAN (Aug. 1, 2016, 11:25 AM),

https://www.theguardian.com/world/2016/aug/01/facebook-free-basics-internet-africa-mark-zuckerberg [https://perma.cc/R4H5-3BLZ].

46. For a discussion of the Border Gateway Protocol (BGP), the internet's "GPS" for traffic, see, for example, Owen Lystrup, *BGP and the System of Trust that Runs the Internet Pt. 1*, Cisco Umbrella (Sept. 21, 2021), https://umbrella.cisco.com/blog/bgp-and-the-system-of-trust-that-runs-the-internet-pt-1 [https://perma.cc/CB8U-2UN7]; *BGP Best Path Selection Algorithm*, Cisco (June 22, 2022), https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html [https://perma.cc/47MG-3BJA]; *What Is Routing?*, Amazon Web Servs., https://aws.amazon.com/what-is/routing [https://perma.cc/2DWD-D2YE].

47. *Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States*, U.S. Dep't of Just. (June 17, 2020), https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea [https://perma.cc/4A8T-ADEZ].

48. *Id*.

49. *Team Telecom Recommends FCC Grant Google and Meta Licenses for Undersea Cable*, U.S. Dep't of Just. (Dec. 17, 2021), https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable [https://perma.cc/QNH4-8ZH3].

50. Alan Burkitt-Gray, *Chinese investor sells stake in Hong Kong-US cable for $160m*, Capacity (Mar. 9, 2022, 4:38 PM), https://www.capacitymedia.com/article/29u7jsv7079dqvsxz7if4/news/chinese-investor-sells-stake-in-hong-kong-us-cable-for-160m [https://perma.cc/22MB-9GU5].

51. Process Reform for Executive Branch Review, *supra* note 13, at 82 (statement of Comm'r Geoffrey Starks).

52. *FCC Bans Authorizations for Devices That Pose National Security Threat*, U.S. Fed. Commc'ns Comm'n (Nov. 25, 2022), https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat [https://perma.cc/R59L-5CFA].

53. Jack Hasler, *Huawei Marine is being sold. That's unlikely to change the threat it poses*, Wash. Post (June 5, 2019, 7:45 AM), https://www.washingtonpost.com/politics/2019/06/05/huawei-marine-is-being-sold-thats-unlikely-change-threat-it-poses [https://perma.cc/ZX3Z-F3UE].

54. Chris Gill, *Huawei submarine cable unit changes name, identity*, Asia Fin. (Nov. 10, 2020), https://www.asiafinancial.com/huawei-submarine-cable-unit-changes-name-identity [https://perma.cc/2XTL-AMZ4]; *Huawei's Marine Submarine Cable Business Changes Name to Huahai Communications and Launches New Corporate Identity*, HHT Grp. (Nov. 4, 2020), https://www.hhtgroup.com.cn/huaweis-marine-submarine-cable-business-changes-name-to-huahai-communications-and-launches-new-corporate-identity [https://perma.cc/J789-PJRE].

55. Keir Giles, NATO Strategic Commc'ns Ctr. Excellence, The Next Phase of Russian Information Warfare 12 (2016), https://stratcomcoe.org/publications/download/keir_giles_public_20-05-2016.pdf [https://perma.cc/2Y73-TQTV].

56. Michael Birnbaum, *Russian submarines are prowling around vital undersea cables. It's making NATO nervous*, Wash. Post (Dec. 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 [https://perma.cc/SBH3-PCW8].

57. *Id*.

58. *UK Military chief warns of Russian threat to vital undersea cables*, Guardian (Jan. 8, 2022, 4:59 EST), https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables [https://perma.cc/QM9U-SMSG].

59. For discussions of Russian military and security service thinking around information and the internet, see generally Joe Cheravitch, The Role of Russia's Military in Information Confrontation (2021), https://www.cna.org/reports/2021/06/The-Role-of-Russia%27s-Military-in-Information-Confrontation.pdf [https://perma.cc/Q3M5-8CHV]; Blagovest Tashev et al., *Russia's Information Warfare: Exploring the Cognitive Dimension*, 10 MCU J., no. 2, 2019, at

129–47, https://www.usmcu.edu/Portals/218/MCUJ_Fall2019_10_2_web_1.pdf [https://perma.cc/5BKR-PNN4]; Roger McDermott, *Russian Military Thought on the Changing Character of War: Harnessing Technology in the Information Age*, Jamestown Found. (Oct. 29, 2021, 4:10 PM), https://jamestown.org/program/russian-military-thought-on-the-changing-character-of-war-harnessing-technology-in-the-information-age/ [https://perma.cc/LJD9-FDVM]; Justin Sherman, Atl. Council, Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior (2021), https://www.atlanticcouncil.org/wp-content/uploads/2021/07/RuNet-Issue-Brief-2021.pdf [https://perma.cc/LD5B-55H5].

60. *See* Nomura Kenichi & Takeda Takaaki, *Optical Submarine Cable Network Monitoring Equipment*, 5 NEC Tech. J., no. 1, 2010, at 33, https://www.nec.com/en/global/techrep/journal/g10/n01/pdf/100108.pdf [https://perma.cc/3FAD-2FE3]; Michael Sechrist, *New Threats, Old Technology: Vulnerabilities in Undersea Communications Cable Network Management Systems* 12–14, 18 (Expl. in Cyber Int'l Rel. Project, Sci., Tech., & Pub. Pol'y Program, Discussion Paper Series Paper No. 2012-03, 2012), https://www.belfercenter.org/sites/default/files/files/publication/sechrist-dp-2012-03-march-5-2012-final.pdf [https://perma.cc/ZD5C-XF7W].

61. Nomura & Takeda, *supra* note 60, at 33.

62. Sechrist, *supra* note 60, at 14 (finding that, in 2012, only Huawei's Network Management System claimed to offer encrypted communication between network controllers and submarine cable terminals).

63. *See* Daniel Voelsen, *Cracks in the Internet's Foundation: The Future of the Internet's Infrastructure and Global Internet Governance* 18–21 (German Inst. Int'l & Sec. Affs., SWP Research Paper 14, 2019), https://www.swp-berlin.org/publications/products/research_papers/2019RP14_job_Web.pdf [https://perma.cc/7SVJ-UQYE].

64. *See* NATO Coop. Cyber Def. Ctr. Excellence, *supra* note 33, at 2–3.

65. AJ Vicens, *DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii*, CyberScoop (Apr. 13, 2022), https://www.cyberscoop.com/undersea-cable-operator-hacked-hawaii/ [https://perma.cc/VQ8A-CYU9].

66. *Id*.

67. *Attachment C: Standard Questions for Submarine Cable Landing License Application*, U.S. Fed. Commc'ns Comm'n, https://docs.fcc.gov/public/attachments/DA-20-1545A4.pdf [https://perma.cc/T9PZ-TXFW].

68. Tianjiu Zuo & Justin Sherman, Atl. Council, Cloud as Critical Infrastructure (forthcoming) (manuscript at 3–15) (on file with author).

69. *See, e.g.*, Brian Lavallée, *5G wireless needs fiber, and lots of it*, Ciena, https://www.ciena.com/insights/articles/5G-wireless-needs-fiber-and-lots-of-it_prx.html [https://perma.cc/9ZAC-5T8U].

70. Submarine Telecoms F., Submarine Telecoms Industry Report 31 (2021/2022), https://issuu.com/subtelforum/docs/submarine_telecoms_industry_report_issue_10 [https://perma.cc/6MKU-2VSN].

71. Sherman, *supra* note 8, at 24.

72. *Id*. at 23.

73. Sherman, *supra* note 8, at 25.

74. Staff of Permanent Subcomm. on Investigations of the S. Comm. on Homeland Sec. and Governmental Affs., Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers 44 (2020), https://www.hsgac.senate.gov/download/threats-to-us-networks-oversight-of-chinese-government-owned-carriers [https://perma.cc/AL9B-HRLV].

75. *Id*. at 42–46.

76. Sherman, *supra* note 8, at 26.

77. *Id*. at 27.

78. *Id*.

79. *Id*. at 27–28.

80. Justin Sherman, *Seizing on US-Japan Opportunities for Submarine Cable Security*, *in* US-Japan Cybersecurity Cooperation: Beyond the Tokyo 2020 Olympics 25, 28 (Mark Bryan Manantan & Crystal Pryor eds., 2021), https://pacforum.org/wp-content/uploads/2021/11/PacForum_Report_Final_Single_Page.pdf [https://perma.cc/NNT3-7XWS].

81. Matteo Colombo et al., Eur. Council on Foreign Rels., Network Effects: Europe's Digital Sovereignty in the Mediterranean 4 (2021), https://ecfr.eu/wp-content/uploads/Network-effects-Europes-digital-sovereignty-in-the-Mediterranean.pdf [https://perma.cc/BF47-Z53R].

82. *See* Justin Sherman, *Internet Security Under the Ocean: EU-US Must Cooperate on Submarine Cable Security*, Italian Inst. for Int'l Pol. Stud. (June 17, 2022), https://www.ispionline.it/en/pubblicazione/internet-security-under-ocean-eu-us-must-cooperate-submarine-cable-security-35471 [https://perma.cc/F7S6-GUC2].

83. Sherman, *supra* note 8, at 19.

29 28 27 26 25 24 23 7 6 5 4 3 2 1

The preferred citation for this publication is Justin Sherman, *Cybersecurity under the Ocean: Submarine Cables and US National Security*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2301 (January 18, 2023), available at https://www.lawfareblog.com/cybersecurity-under-ocean-submarine-cables-and-us-national-security.

ABOUT THE AUTHOR

JUSTIN SHERMAN

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, a senior fellow at Duke University's Sanford School of Public Policy, and the founder and CEO of Global Cyber Strategies, a Washington, DC–based research and advisory firm focused on technology, policy, and geopolitics.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION