Undersea Cables, Hyperscalers, and National Security

Richard Salgado

INTRODUCTION

The audacious and costly enterprise of connecting continents by cables that run beneath the oceans has yielded invaluable social and economic benefits. Improving their resilience and defense must be a national security priority.

The United States, simply put, lacks a comprehensive government-wide strategy to promote, protect, and secure undersea cables that land on American shores. The US government has taken an ad hoc approach, which relies heavily on a regulatory regime that is effective on paper but in practice creates disincentives to build state-of-the-art cables on new routes. This approach has created an environment that hinders cable development, is counter-productive to security, and squanders opportunities to strengthen cable resilience.

Today, as more cables originate and terminate outside the Americas, the nation's percentage of global cable expansion is shrinking.[1] All of this comes at a time when US influence in cyber-space generally seems to be waning and the People's Republic of China (PRC) and other autocratic nations have taken off the gloves.

This essay is based on conversations with practitioners in the private and public sectors and personal experience in government and the private sectors. It proposes ways to significantly improve our national security by taking steps that will help the US government, cable suppli-ers and operators, and the public at large.

- Make sure the federal process creates incentives for private investment in newer, more diverse and secure cable systems.

- Speed the Federal Communications Commission (FCC) licensing process and eliminate obstacles that block or impede development and repair of secure cables.

A Hoover Institution Essay

Aegis Series Paper No. 2304

- Integrate the FCC licensing process into the larger strategy by moving key agencies from Team Telecom advisory roles to full participants.

- Halt efforts by Team Telecom[2] to use the FCC process to pursue inquiries and impose conditions that are extraneous to the licensing of regulated submarine cables.

- Make the undersea networks more robust by supporting redundancy that will ensure service when natural disasters, accidents, or intentional attacks cause cable breaks and outages.

- Engage in a thoughtful and open decision-making process when developing policies about cables that link directly to nations that do not share our national security goals.

- Share much more information with cable builders and operators about risks and threats to their systems.

- Recognize that creating secure cable networks is a shared public-private goal, and approach the private sector, particularly the largest companies investing in undersea cables, as allies.

BACKGROUND

Initially used to replace steamships as the means to carry messages abroad, undersea cables now convey over 99 percent of international voice and electronic data.[3] The world communicates along cables of mind-boggling length that are the diameter of a garden hose and have covering layers of delicate glass strands, silicon gel, plastic insulation, copper sheathing, and steel wire, all wrapped in tar-coated nylon yarn. These cables lie in the cold, dark depths of the open sea, pass through territorial waters, and then make their way into beach manholes to cable landing stations near the shore, where terrestrial networks take over.

As data communications have transformed economies and society, cables and the companies that produce, lay, and operate them have become more important than ever. It is estimated that each day more than $10 trillion of financial transactions are made using undersea cables.[4] Enormous demand has led to the deployment of new, faster, and high-capacity infrastructure running on a variety of new routes. So-called hyperscalers, including Amazon, Google, Meta, and Microsoft, are financing and laying many next-generation cables. Those cables increasingly supplement cable capacity and routing choices once offered only by traditional telecom companies.

If hyperscalers that have spent hundreds of millions of dollars to lay cables are to continue to expand, they must be able to support top performance. Customers of the companies (including the government) expect instantaneous, reliable service and will not tolerate outages, latency, and security breaches. Cable on the ocean floor and infrastructure at the shore also

must be protected from natural disasters, fishing and mining operations, anchor drops, saboteurs, eavesdroppers, and sophisticated nation-states. Fighting these enemies must become core to the design and operation of cable networks.

US government agencies recognize the contribution that subsea cables make to the nation's communications and economy, and understand the need to maintain their viability, integrity, and security.[5] Every new state-of-the-art cable that originates or terminates in the United States adds to the nation's resilience to natural disaster, accidents, intentional attacks, and other threats. Cables that run new routes and land in places that are underserved also improve the network. National security demands that the US support investment in cable diversity and help cable operators maximize protection of infrastructure.

Key government officials have acknowledged that they must cooperate with business to ensure resilient and safe cable networks. Officials often call the private sector a "partner" in protecting communications infrastructure,[6] and President Biden has declared that "robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace."[7] The government must now encourage investment in new and existing cables and seriously engage companies, which are eager to advance national security and protect their costly infrastructure.

Unfortunately, government pledges fall short of their stated aims. The US lacks a comprehensive, whole-of-government strategy to encourage investment in secure cables and has not yet built the collaborative relationship with hyperscalers that is in the interest of us all. To date, in fact, Washington's approach has been largely ad hoc, dominated by regulators who take a cable-by-cable approach and apparently operate on the premise that every proposed cable, even the most benign, is a threat to national security.

The government relies mostly on the authority of the Federal Communications Commission (FCC) to license ownership and operation of submarine cables and associated cable landing stations located in the United States, with input from the Departments of Defense, Homeland Security, and Justice, the core members of "Team Telecom."[8] These officials have influence over everything from cable planning and design to routing and operations, including equipment and personnel.

Washington has recently tried to expand its power beyond the scope of the FCC's statutory jurisdiction. In addition, the government's tendency to maintain secrecy and approach cable developers and operators as adversaries has further alienated parties that should share common goals. Agencies more often than not are opaque, rarely share information, and fail to provide due process when the two sides disagree.

The current FCC regulatory regime is ill suited to achieve on its own the gains in security that a less coercive environment could generate. Increasing reliance on the FCC and Team Telecom and their tendency to expand their power to oversee the construction and protection of cables is both misplaced and dangerous. The system stifles cooperation between the

government and the private sector. At the same time, the licensing process remains slow and unpredictable, and the government's failure to adequately share threat information has weakened cable security. The system needs reforms.

HISTORY OF GLOBAL CABLE NETWORKS

Understanding the commercial players and the factors that drive cable operators is necessary to enhance security. Initiatives from the private sector are largely responsible for developing and maintaining the undersea global cables.[9] Companies have designed, built, and operated most of the 1.4 million kilometers (about 870,000 miles) of undersea cables currently in service.[10] This pattern holds true for most nations that have cables.[11]

For more than a century, large global telecom providers built and operated undersea cables. Their routes linked major population centers, focusing on developed nations with high trade volumes and GDPs. Because those cables were primarily used for telegrams and later voice calls, this pattern made sense for much of the twentieth century.

Then came the internet. Public, private, and nonprofit institutions quickly recognized its potential. The internet also spurred the growth of online services offered by hyperscalers including Amazon, Google, Meta (formerly Facebook), and Microsoft. By the early 2010s, hyperscalers had started building massive data centers around the world.[12] The companies require high-bandwidth cables to handle the huge volumes of data. The hyperscalers' customers and subscribers, both businesses and consumers, quickly became reliant on the availability and confidentiality of high-speed communications. Resilience to threats became essential.

To handle international traffic, hyperscalers until recently had no choice but to lease capacity from telecom companies, using routes designed in a different era and often carried via aging cables. For many reasons, hyperscalers quickly saw the need for more options to move vast quantities of data.

First, their options were limited to routes operated by major telecom companies. Cables followed the same paths at sea, and landing stations were highly concentrated in a few large cities. However, hyperscalers needed routes that linked their data centers, many of which are in sparsely populated areas. For example, the companies might serve their European customers from huge data centers located in relatively remote areas that have plenty of water for cooling and feature lower temperatures that help reduce energy consumption and minimize environmental impact.

In contrast, the closest cross-Atlantic route offered by a traditional telecom may connect to a major metropolitan area like London or Paris. This left hyperscalers facing complications and high costs of connecting across borders to distant data centers. These distances slow traffic and increase the possibility that cables will be blocked or compromised. Traditional cable systems were not designed for the new, connected world.[13]

Second, the hyperscalers needed more flexibility to increase capacity on the fly or shift traffic from one place to another. Companies must quickly reroute traffic from damaged cables or nonfunctioning landing stations, or shift traffic when data centers fail temporarily or require significant maintenance.[14] Hyperscalers also found that leasing increased capacity from a traditional provider could take months to negotiate and leave them open to price gouging.

Reliance on repair crews when cables fail is no substitute for building redundant, alternate routes. In some cases, identifying where cables are broken can take weeks and repairs cannot begin until governments approve permits.[15] The number of ships capable of repairing cables and sailing under the right national flag is very limited.[16] Travel time and repairs often take months. To reduce failure times and improve network durability, hyperscalers need alternative cable routes that would be available immediately.

Third, many of the cables run by telecoms had started to show their age.[17] Although state-of-the-art when laid, existing cables were too slow and lacked the capacity required by hyperscalers. Finally, traditional operators could not constantly monitor cable conditions. Hyperscalers needed the ability to anticipate latency and cable degradation, and remove obstacles before outages impacted speed-sensitive users.

In short, hyperscalers needed alternatives to supplement the offerings of telecom companies. And so they joined in the building of infrastructure, and today shoulder much of the cost and burden of the world's undersea cable network. This is no small matter. Cable systems are extremely expensive to design and build, requiring tremendous capital outlay; long spans often cost in the hundreds of millions of dollars. TeleGeography estimates that, as of 2021, hyperscalers had invested more than $20 billion in cable systems.[18] Constructing transcontinental cables takes as many as eight years, and rarely less than four years, from design to going live.

These hyperscalers are now perhaps the most important players in designing, building, operating, and securing undersea cables. Hyperscalers today are constantly trying to increase diversity in cable routes and maintain their infrastructure, while also paying to lease space from traditional cable providers.

SECURITY IMPERATIVES FOR OPERATORS

Because virtually every institution in the public, private, and nonprofit sectors relies on undersea cables for communication, the nation's security relies on ensuring they are available, dependable, and constantly increasing their capacity.[19] Loss of cable services, without reasonable alternate routes to carry vital government and commercial traffic, has the potential to seriously harm our economy, healthcare systems, the military, and other critical sectors. As a matter of national security, cables must remain available to transport data without sacrificing integrity or speed.[20]

There are, of course, many threats to cables. Outages are quite common.[21] Natural events like severe weather can take out cable landing stations and related infrastructure, or can strain undersea cables to the breaking point.[22] Earthquakes and aftershocks can have devastating outcomes.[23]

Historically, most instances of cable damage have come from inadvertent human activities including fishing.[24] Dropping an anchor on a cable can crush a cable; a dragging anchor can snap one. Seabed dredging and mining equipment can slice through cable. Intentional attacks are also a concern. An adversary may find landing stations to be tempting targets. And nation-states may consider disrupting submerged cables as part of naval warfare strategy.[25]

All modern communications equipment, whether located underwater, on the ground, or in space, faces network-based threats. Malware, eavesdropping, and denial-of-service attacks (both external and internal) threaten cable control systems.[26] Cable builders and operators, like those working on all sensitive networks, must secure their facilities and networks, and have procedures in place to deal with anomalies, disruption of supply chains, vendor failure, and other vectors of vulnerability.[27]

There are ways to reduce the chance of all of these threats occurring, and mitigate their impact on infrastructure. Perhaps the single best defense is to have alternative routes available to carry traffic that would otherwise depend on compromised or broken segments. Because uncontrollable phenomena such as earthquakes and hurricanes can take out cables, diverse routes and locations for landing stations are needed.

Having numerous routes and landings also serves to deter or mitigate intentional attacks; the more routes there are, the less impact a single successful attack can inflict.[28] Simply put, more cables and landing stations, and a greater variety of routes and end points, means faster recovery from outages and compromises, be they accidental, natural, or malicious.[29] Hyperscalers have helped reduce risks. Increasing needs for reliability, resilience, security, capacity, and speed led them to design custom systems. These companies have added nontraditional routes and new landing station locations to deal with security threats.

For example, hyperscalers have established routes that serve Southeast Asia with fast, reliable networks that detour around contested territory in the South China Sea.[30] The hyperscalers undertook this task to avoid significant obstacles, including the need to obtain permission from the Chinese government, which can be accompanied by (1) obligations to have a Chinese carrier as an owner, and branch landings in China or Hong Kong; and (2) Chinese restrictions on repair vessel activity.[31] In addition, the region is heavily trafficked with many vessels and full of physical hazards to cables. It is highly risky to rely solely on cables running through that region to service the enormous population across Asia. The US government, meanwhile, is unlikely to license cables running between the US and Hong Kong.[32] Limitations on cable length forced companies to run cables in the contested territories of the South China Sea. Serving the region from the US meant cables had to travel the Great Circle path from the

US to Japan, then to Hong Kong, and on to Singapore. Thanks to advances spurred in part by hyperscalers, cables can now stretch greater distances, reaching Southeast Asia through the Java Sea and bypassing the South China Sea. Today's cables, for example, can connect the US directly to Singapore and Indonesia.[33]

Hyperscaler experience in designing massive network infrastructure, procuring and updating secure equipment, and providing secure services to customers has transferred well to building and operating cables. As customers of their own cables, hyperscalers are very sensitive to signal degradation, latency, loss of data integrity, outages, and maintenance of confidentiality. As operators of enormous data centers, they understand the need for physical security for the equipment.[34] Finally, hyperscalers have proven to be innovative supporters of open standards and interoperability that create resilient ecosystems.[35] Their efforts have made cable networks far more secure.

ROLE OF THE US GOVERNMENT

The US government lacks a comprehensive strategy to ensure the safety and reliability of undersea cables. For decades the government has relied heavily on regulatory agencies that consider licensing cables case by case. A 1921 statute requires a would-be cable owner to obtain a license to allow it to land a submarine cable on US territory.[36] The president has delegated this power to the FCC, which uses the "public interest" standard when considering applications.[37]

Since the 1990s, the FCC has asked the Departments of Justice and Defense for guidance on the national security or law enforcement impacts of granting licenses. The Department of Homeland Security joined soon after its creation. In those years, a process developed that requires license applicants to engage with officials of these agencies, known colloquially as Team Telecom.[38]

In 2020, the Trump administration issued an Executive Order, and the FCC adopted rules, that aim to formalize and speed up the Team Telecom process.[39] The Executive Order states that "security, integrity, and availability of United States telecommunications networks are vital to United States national security and law enforcement interests."[40] The Order spells out Team Telecom's primary mission: to review new licenses for their impact on security and propose measures to mitigate any dangers associated with new cable routes or facilities.[41] The Order also regularizes much of Team Telecom's work and provides additional dedicated resources.[42] Finally, the Order officially renamed Team Telecom to the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, a titular change that has been largely ignored.[43]

THE TEAM TELECOM PROCESS

The procedures governing Team Telecom play an outsized role in how the US government addresses national security concerns with undersea cables. They influence not only how the

US government will handle a particular undersea cable license application, but the decision making by companies considering investments in new cables and routes.

As noted, Team Telecom's charge is to "review and assess" each application referred by the FCC and determine whether granting or transferring a license "poses a risk to national security or law enforcement interests of the United States."[44] Team Telecom may also initiate a review of existing licenses to make assessments and recommendations to the FCC.[45] Team Telecom is chaired by officials representing the attorney general, drawn from the National Security Division of the Justice Department, and includes representatives of the secretaries of defense and homeland security.[46] Officials from the US Departments of State and Commerce and the Office of the Trade Representative and other executive branch agencies have limited advisory roles.[47]

The process begins when the FCC notifies Team Telecom of a cable landing station license application. In turn, Team Telecom notifies the FCC whether it intends to review and assess the applications. If it does, the FCC suspends further action on the application until Team Telecom submits its recommendations.[48]

Under the Order and new FCC rules, Team Telecom starts such reviews by examining the applicant's answers to publicly available "Standard Questions."[49] If Team Telecom finds the answers insufficient, it has thirty days from the date the FCC refers the matter to it to submit so-called Tailored Questions to the applicant.

Once Team Telecom has the information it needs, it has an additional 120 days to complete its initial review. After the review, Team Telecom chooses among three options. It may do any one of the following:

1. Grant an application for a license or the transfer of a license that poses "*no current risk* to national security or law enforcement interests."
2. Recommend *standard mitigation measures* for risks to national security or law enforcement posed by the application.
3. Conduct a "*secondary assessment*" of an application if the Team finds that standard mitigation measures cannot mitigate the risks.[50]

If Team Telecom finds that an application poses no current risks (option 1), it notifies the FCC and the agency continues processing the application.

If Team Telecom chooses the second option, it identifies for the FCC based on a written analysis the standard mitigation measures needed to address the risks raised by the application.[51] The FCC will consider and may adopt the recommended mitigation measures as part of the license grant. Going forward, Team Telecom monitors compliance with the mitigation measures by the license holder using methods developed in consultation with the FCC; if it

determines a license holder is failing to comply with those conditions, Team Telecom can recommend that the FCC revoke the license.[52]

If Team Telecom selects the third option, concluding that standard mitigation measures are insufficient, it conducts a secondary assessment. Team Telecom can then recommend that the FCC deny the license or that it grant the license conditioned on nonstandard mitigation measures.[53] In either case, Team Telecom must then notify the advisory agencies, which triggers a three-week period in which those agencies can register disagreement.[54] The Executive Order outlines procedures to resolve disagreements within Team Telecom and with the advisory agencies.

The FCC defers to Team Telecom's recommendation, but the FCC has the ultimate responsibility to accept or reject license applications within its jurisdiction.[55]

THE TEAM TELECOM PROCESS IN PRACTICE

When the FCC adopted this process, officials in the public and private sectors hoped that Team Telecom's decision would be both more rapid and more predictable.[56] In practice, however, the licensing process for cable landing stations is an unpredictable ordeal for applicants.

Today, the private sector continues to confront a government process in which Team Telecom moves very slowly to gather information; demands that applicants answer questions that are not germane to security risks from the licensed activity; recommends mitigation measures that are vague, contradictory, or counterproductive; and gives applicants no realistic recourse. One thing that is predictable when it comes to a license application for a cable landing station: the FCC continues to refer applications to Team Telecom for its recommendations, even for domestic cable routes that have no apparent impact on national security.[57]

Excessive Delays in Gathering Information

Once in the hands of Team Telecom, the application process starts with information gathering.[58] The new rules governing this phase are intended to increase predictability, efficiency, and efficacy. Applicants can prepare answers to the Standard Questions in advance. Team Telecom has thirty days after the FCC refers the matter to submit tailored inquiries.[59] Despite these new provisions, however, the information-gathering phase remains extraordinarily slow.[60]

There are three primary reasons for these delays. First, despite the FCC's ostensible adoption of Standard Questions[61] in almost all cases, Team Telecom poses additional new and different "standard" questions that have not gone through the vetting process.[62] For whatever reason—perhaps the Standard Questions adopted by the FCC are already out of date—applicants confront a moving target and have no complete set of known "standard questions" before filing.

Second, after completing the different sets of Standard Questions, applicants are facing multiple rounds of Tailored Questions and document requests. This is anticipated in the rules, but was to be a phase limited to a thirty-day period that starts when the FCC refers the application to Team Telecom. That has not proven to be an effective constraint. The rules say that the government must provide the questions within those thirty days, but leaves it to the sole discretion of the attorney general, as chair of Team Telecom, to determine when the answers are complete.[63] In practice, this means that Team Telecom can ask vague and broad questions within the thirty-day period, and those questions serve as a wellspring from which a seemingly endless number of subquestions flow well beyond the thirty-day period. This drags the process on for several months.[64]

Third, even once the attorney general declares the answers are complete and starts the 120-day clock to conclude the assessment, officials will continue to request more information, and impose very short deadlines. An applicant may complain about this practice, and more particularly about the short amount of time within which Team Telecom wants the newly requested information. But that is met with an offer by Team Telecom to extend the due date, if the applicant agrees to toll the 120-day clock. With no other realistic choice, the applicant accedes and the delay piles on. As one participant has noted, "a 120-day review often takes closer to six to eight months."[65]

"Scope Creep" in Information Gathering

Applicants are reporting that Team Telecom's rounds of both Standard and Tailored Questions are detouring into matters wholly unrelated to the license. Such questions may skirt the edges of national security but are not germane to license grant or denial.[66] Applicants report, moreover, that agencies are not eager to explain the relevance of such questions, leaving companies wondering if agencies are conducting fishing expeditions or are refusing to be transparent about real security threats.

Applicants also lack any practical means to object to these delays or to challenge questions that exceed the statutory licensing jurisdiction. Even if they were to prevail in an objection, it would be a limited victory accompanied by further costly delays. To date, applicants are going along with the demands, but suspicions about the process are increasing while the desire to invest in new US cables recedes.[67]

Vague, Contradictory, and Counterproductive Mitigation Measures

In contrast to the detailed, if flawed, procedures and deadlines for information gathering spelled out by the Executive Order and FCC rules, there is little structure around mitigation measures.[68] Ideally, the government would start with a known set of "standard mitigation measures" agreed upon by Team Telecom and the advisory agencies.[69] In a situation where there were some national security concerns, but no secondary assessment is in order, Team Telecom would refer to that set and select those measures that address the incremental risk presented by a license grant. Discussion with the applicant would ensue, Team Telecom would relay its suggestions to the FCC, and agency commissioners would make the final decision.

In reality, there is no clear set of sanctioned "standard mitigation measures" that would-be investors or applicants can review in advance, much less measures that have undergone anything close to the so-called Notice of Proposed Rulemaking process used to generate the Standard Questions. To determine what measures might be required, applicants' best shot is examining conditions imposed in recent FCC license proceedings; even then, the conditions may represent the minimum required.[70]

The applicant will only find out what Team Telecom considers "standard mitigation measures" in any particular matter when it is presented with a draft agreement.[71] The document will look for all purposes like a contract, with the Team Telecom agencies and the applicant listed as parties and boilerplate contractual provisions. The draft will likely contain all the mitigation measures imposed in the most recent FCC license grant, possibly with some additions. After discussion between Team Telecom and the applicant, the parties eventually sign the agreement that obligates the company to abide by the stated mitigation measures. Regardless of whether Team Telecom's recommendation is to impose mitigation measures styled as "standard" or "nonstandard," or it is to deny the application, the FCC defers to Team Telecom.

From the hyperscaler's viewpoint, the current approach to identifying and imposing mitigation measures in practice is unpredictable, creates disincentives to build cables, can compromise cable security, and raises questions about the legitimacy of the process.

First, the lack of transparent "standard mitigation measures" creates unpredictability, which deters private sector investments. Current practice also means that changed components of one agreement can set a "standard" for all that follow. As time passes and different staff negotiate with applicants, Team Telecom changes definitions, adds new obligations, and expands its powers, all without meaningful scrutiny. Because the FCC defers to Team Telecom recommendations, the resulting mission creep faces no procedural check.

The lack of true standardization has other presumably unintended effects. Industry officials contend that companies holding licenses for two cable systems that are very similar from a risk perspective have faced two different sets of obligations for no discernible reason other than that Team Telecom had different staff in the respective negotiations.

It's not effective to rely on individual license applicants to check overreach or seemingly arbitrary requirements. Applicants have spent enormous sums of money prior to starting the process and need to secure a license timely. Applicants have great incentives to agree to virtually any Team Telecom demand in order to obtain a positive recommendation as quickly as possible. The applicant must either accept the terms or face even longer delays if it chooses to raise objections to the FCC or challenge the FCC's decision. Team Telecom also has the power to seek to impose new conditions on license holders that have been operating for years, even decades, under earlier agreements. Those companies must submit or risk losing their licenses. Team Telecom's leverage in these negotiations is tremendous.

Company representatives understand and expect that, over time, mitigation measures should change for new and existing cable operations. Technological advances may render some measures obsolete, and new threats will require new mitigation measures. The current approach to developing mitigation measures is a black box, however. Little wonder that companies want meaningful input into credible and predictable standards.

Second, companies are facing mission creep on Team Telecom's part. For example, Team Telecom has twice required license holders to assess and report on the risks to data *after* it flows beyond licensed infrastructure.[72] Provisions like this penalize companies that invest in building new cables compared to others that do not. When government agencies step outside their remit and impose questionable mitigation measures, they also discourage investments in new, secure cables.[73]

Hyperscalers and others that develop cable infrastructure outside the US can avoid the FCC process and escape mitigation measures,[74] as can those companies that merely lease capacity on cables and don't take on the risk and expense of investing in the infrastructure. The bottom line: when government agencies go beyond the scope of their legitimate authority, they disincentivize investments that can create more resilient and more secure cables.

Third, some of the new mitigation measures (again, intentionally or unintentionally) harm cable security. Mitigation agreements, for example, now require that operators get permission from Team Telecom before installing or changing "Principal Equipment."[75] Companies have learned to avoid certain vendors and equipment knowing that they won't be approved, and at least some agreements have a default approval if Team Telecom doesn't object in a given period of time.[76]

This component-by-component review has proven to be opaque, slow, and hard to scale. In some cases, the delays are so long that by the time the approval to install a piece of equipment comes in, there's an improved model or version available. Installing the latest, however, requires another round of approvals and more delay. Ultimately, the process hinders the kind of upgrades that would likely improve security.

Finally, the legitimacy of Team Telecom using its FCC advisory role to secure what look like contractual obligations from the applicants is questionable, and in any event is unnecessary. Styled variously as "Letters of Assurances," "Agreements," "Network Security Agreements," and, of late, "National Security Agreements," these accords have been used as long as Team Telecom has been around.[77] These agreements purport to give the government the contractual right to enforcement not just through the FCC, but through the court system.[78]

Nothing in the statute or the grant of authority to the FCC to issue licenses provides for this exercise of power by the Team Telecom agencies. The Executive Order makes clear that it doesn't preclude agencies and departments from entering into agreements pursuant to other authority, but nowhere does it say that it is one of those authorities.[79]

Moreover, these agreements are entirely unnecessary for the imposition or enforcement of mitigation measures. The FCC could simply include mitigation measures in licenses.[80]

RECOMMENDATIONS

To improve the security of undersea cables on which the United States relies, the government should design and execute a comprehensive strategy to expand diversified routes; share more threat information with cable operators, particularly hyperscalers; and reform the Team Telecom review process to maximize speed and regularize standards.

1. ADOPT A COMPREHENSIVE NATIONAL STRATEGY TO IMPROVE CABLE SECURITY

The US government, led by the president, should design and execute a government-wide strategy to improve cable security by encouraging investments in new cables and diversified routes. Protecting national security demands that multiple regional and hemispheric cable options be operable when nature, accidents, or enemies interrupt or corrupt service.

The current licensing process, particularly the role of Team Telecom, discourages investment in additional secure undersea cables landing in the US. Building a new cable takes many years and can cost hundreds of millions of dollars. Even a slight chance that Team Telecom will impose unreasonable conditions or that the FCC will deny a license plays a big role in decision making for the investors.

Based on their experience, companies perceive Team Telecom as undervaluing the long-term national security gains that come from cables serving new (even if vexing) jurisdictions or countries outside mature markets. Companies are heavily influenced by global economics, politics, and trade and must balance hundreds of factors before committing resources to new projects. Would-be investors will rationally try to reduce their risks, opting to deploy routes in existing crowded corridors or avoid US borders altogether. Having a comprehensive national strategy that encourages route diversity could encourage increased investments.

As a part of the strategy and to improve the licensing process, the president should make the State and Commerce Departments, as well as the Office of the United States Trade Representative (USTR), members of Team Telecom, promoting them from their current limited, advisory roles.[81] These agencies have expertise that could give the FCC a more comprehensive understanding of global economic and geopolitical forces and how a particular proposed cable may fit in the larger national security picture.[82] Team Telecom is currently under no obligation to even inform these agencies when it considers new applications; they get involved in this aspect of the licensing process only when Team Telecom intends to recommend that the FCC deny a new application, revoke an existing license, or add nonstandard measures to agreements.[83] Meanwhile, the Departments of Justice, Homeland Security, and

Defense dominate the process and have for the most part forfeited the strategic approach for one that is tactical.[84]

2. INCREASE GOVERNMENT SHARING OF THREAT INFORMATION

The companies applying for the licenses are very familiar with their systems, and are motivated to keep them reliable, secure, and fast.[85] The government should not, and in most cases does not, try to micromanage technical aspects of specific cable deployments.[86]

On the other hand, the government is in an excellent position to help companies understand current and future threats so the private sector can better defend its networks. Hyperscalers report, however, that the government's approach can be coy, and sometimes adversarial, when it comes to sharing information at key points in the licensing process. Mitigation agreements contemplate that the government will share information about threats and risks, but, in practice,[87] agencies rarely do. Perhaps unfairly, Team Telecom's reticence to share information gives the appearance that it has little concrete information to back up its security concerns and mitigation measures. Assuming that's not the case, it is hard to understand the reluctance to share information that could make systems more secure.

If the concern is that information sharing is better done outside the regulatory process, there are models from other contexts that could be effective. An Information Sharing and Analysis Center (ISAC) is one familiar approach, and can work well if carefully constructed. If not optimized for operational value, ISACs can be bureaucratic affairs, intensely focused on protocol, organization, and bylaws. Timely and actionable information sharing and real-time updates fall victim.

The government's best move would be to create a transparent system modeled on its procedures for sharing information on cyber threats with the private sector. Subject matter experts from agencies could meet with their counterparts individually and in groups, depending on the topic. Agendas for regular meetings could include nonurgent issues while ad hoc meetings deal with time-sensitive matters. Government representatives could use the meetings to warn companies about upcoming supply chain and equipment problems, for example; this could provide guidance so operators do not propose equipment upgrades the government will likely reject.[88] Done right, this arrangement could cut months off the time it takes companies to upgrade their systems.[89]

3. SPEED UP TEAM TELECOM REVIEWS

The government must streamline the Team Telecom license-review process and set real deadlines, a goal of the 2020 Executive Order that has not been achieved.[90] In practice, giving Team Telecom 30- and 120-day deadlines has made little difference. As noted, companies are also essentially forced to allow Team Telecom to toll the clock as it sees fit.

A 2020 Senate staff report on the Team Telecom process focused heavily on threats from China and suggested that Congress impose statutory deadlines on Team Telecom, similar to

those mandated for the Committee on Foreign Investment in the United States (CFIUS). On the one hand, companies would welcome guaranteed deadlines.[91] On the other hand, bringing Congress into the licensing process might also spook companies if it complicates legislation by introducing controversial geopolitical issues. Cable operators, however, would likely welcome laws to improve security, including new protections from fishing and mining operations; a larger fleet of repair vessels; incentives to diversify routes; and steps to smooth relations with foreign jurisdictions.

In addition to setting hard deadlines, the government should require Team Telecom to regularize, and be more disciplined and transparent in posing, the so-called Standard and Tailored Questions.[92] If there's a real issue identified that Team Telecom needs to explore, it should explain what the concern is and bring it to the table quickly for a genuine dialogue rather than leave the companies guessing what it is. The typical applicant is going to be very keen to understand what the threats are; it shares an interest in keeping its system secure and available. Not only would this allow the applicant to provide more pertinent information efficiently, but it may identify ways to deal with threats that the government could not.

4. ENSURE MITIGATION MEASURES STAY WITHIN BOUNDARIES

Deference by the FCC to recommendations from Team Telecom is entirely appropriate. The FCC must, however, ensure the Team does not exceed its jurisdiction to fish for information or try to regulate matters not germane to licenses. Cable developers and operators can push back against extraneous demands or if they believe Team Telecom is acting in bad faith. It is the FCC, however, that is in the best position to carefully guard against overreach.

Four changes to mitigation measures can begin to solve this problem. First, Team Telecom should have a far more transparent and disciplined process for identifying standard mitigation measures. Certainly its decisions about what measures should be standard can be informed by individual license applications, but Team Telecom should not rely on this ad hoc approach. Team Telecom should also regularly review the measures to eliminate those that are no longer appropriate.

Second, as part of its review and assessment, Team Telecom should be required to submit written risk analyses justifying, for each mitigation measure, why it is required. Team Telecom should share its analysis with the applicant, recognizing that in some situations classified information must be withheld.

Third, Team Telecom should apply the same criteria and similarly submit written analyses for nonstandard measures it seeks to impose. Those measures should be specifically flagged to the FCC and vetted for justification and to determine whether they go beyond the agency's statutory authority. In addition, nonstandard measures should not become standard merely because they have been adopted before.

Finally, Team Telecom should discontinue "contracts" and replace them with recommendations that the FCC can incorporate directly into licenses. The recommendations can, of course, be accompanied by submissions to the FCC, jointly filed by Team Telecom and the applicants, acknowledging that all have agreed on the adoption of the recommendations as a condition for the license grant.

5. ENSURE FAIR MITIGATION MEASURES

The government should also ensure that standard or secondary mitigation measures imposed by Team Telecom and then adopted by the FCC are nondiscriminatory and address the incremental risk to security that the license presents. While Team Telecom and the FCC are well within their mission to prevent risks to and improve security of the licensed cables, in recent years they have taken it upon themselves to regulate the way licensees use the cable and provide online services as customers of the cable. These actions violate the intent and scope of the agencies' authority.

Adding and supporting such restrictions is not only illogical, it's unfair.[93] In imposing obligations on activities outside the scope of the license, the government is currently disadvantaging the companies that build and upgrade cables, improve diversity, expand capacity, and enhance security.

6. ENCOURAGE FASTER EQUIPMENT AND SOFTWARE UPGRADES

Team Telecom should also be far more transparent and faster when it reviews new equipment and upgrades to cable systems. Scrapping the current piece-by-piece equipment review would remove delays but also build confidence between the government and companies. Team Telecom should, for example, work with operators to help them understand the risks the government sees from hardware and software vendors. By more openly sharing information with the operators about the perceived threats from a particular vendor, equipment, or software and its criteria for evaluation of change proposals, Team Telecom would be doing more to protect security than by invoking impenetrable fiat to strike a line through the item on a list of proposed equipment.

To be sure, having the government maintain a no-use list for vendors and equipment can add value and reduce delays. Team Telecom should, however, change its current piece-by-piece review process and, in so doing, remove another obstacle to keeping cables state-of-the-art. As Team Telecom takes on more of these agreements, it will be on the hook to review more and more equipment change proposals. Given the security downside to this slow process, it is worth considering whether this is the right approach in the first place.

7. ADOPT A NATIONAL STRATEGY ON ROUTING CABLES TO NONALLIED NATIONS

In an era of competition between the US and China and other authoritarian nations, the US government should willingly provide a rationale for its increasingly hard-line stance

preventing direct cable links to select nonallied nations. Recent FCC licenses involving China demonstrate that the government has adopted a policy that, in practice, bans new cables from connecting the US with potential adversaries. Team Telecom has (perhaps rightly) acted upon its fear that directly connecting cables to potential enemies could allow those nations to hijack data or disrupt service to the detriment of US security. No matter the reason, this policy is moving the world into what one commentator has called "the era of the undersea Iron Curtain."[94]

While this policy may be rational and necessary, such fundamental actions demand, at the very least, that the government get expert input and provide a sophisticated technical and geopolitical explanation of its policy. It appears that Team Telecom has not considered important factors related to securing information. Unredacted portions of Team Telecom's recommendations, for example, fail to take into account the strong and ubiquitous encryption of data, which effectively blocks most would-be eavesdroppers.

Team Telecom may be acting because of doubts that today's encryption sufficiently reduces future risks of data interception. Government officials are likely concerned that quantum computing technology will someday be able to break today's state-of-the-art encryption methods.[95] Any cable to a destination controlled by or heavily influenced by the Chinese government that runs on equipment manufactured under the control of the Chinese government is susceptible to wholesale interception by the PRC. With China's strong commitment to winning the race for quantum computing, fears that Beijing could store data for later decryption are reasonable.[96]

Data security transcends cable safety, of course, and the security community is acutely aware of the potential for a store-now-decrypt-later attack.[97] Government and company researchers are already developing quantum-resistant cryptography.[98] There is some reason to be optimistic about these efforts.[99]

There are other factors that will reduce the ability of US adversaries to wholesale capture data so it can be decrypted in the future. First, consider the immense amount of storage necessary to hold the never-ending data that traverses today's high-capacity cables. As a practical matter, the intercepting party would have to select what to keep and what to let drop on the floor, and do so without being able to see the plaintext. In addition, as some observers have noted, in the early years of quantum computing, decryption efforts would require message-by-message analysis.[100] Without some ability to select from among all those encrypted messages only those likely to be useful, the yield will be low.

Second, this future threat exists even when there is no direct cable connection between the US and China. Team Telecom has said in its recommendations, for example, that the PRC has many options for diverting data to networks under its control. Beijing, for example, could try to take advantage of so-called least-cost-routing rules (where traffic is sent based on cheapest cost, even if it is not the fastest or most direct route) or exploit vulnerabilities

in the internet routing infrastructure. As long as China is not completely decoupled, at least in theory it could cause traffic not destined for China to flow through networks under its control. Stopping the construction of new cables that connect directly to China will not solve such problems. Perhaps, however, forcing China to employ such tactics is a win since it makes signal acquisition harder. We don't know, but perhaps that's how Team Telecom sees it.

While neither Team Telecom nor private operators should downplay the risk of intercept-now-decrypt-later, China will rank high on the list of nations and groups with the power to do this.[101] Team Telecom's rationale is opaque, leaving cable operators to speculate about security concerns.[102] Prior to taking similar sweeping actions on instituting bans, Team Telecom should allow for debate and make sure such decisions fit into a comprehensive national cable security strategy.

There are, of course, many other ways to improve security for undersea cable networks. Among other steps, the government should take these:

- *Treat specific location information as confidential*. The FCC should no longer make available for public inspection maps submitted by applicants that show the street addresses and latitude/longitude coordinates for beach manholes and cable landing stations. The danger of including this kind of detail in the public record is real.[103] This practice makes it all too easy for an adversary with even limited funding to access vital information. Of course, it's possible to find the location of these facilities without resorting to the FCC files, but there's no reason to make it that easy. Keeping maps and facility locations confidential would increase security.[104] It requires a simple change in FCC practices.[105]

- *Remove legal impediments to cable repair*. The government should also take steps to negotiate with nations to loosen restrictions on cable-repair vessels operating in their territorial waters. As noted, a country's cabotage laws that restrict the operation of foreign repair ships within or into that country can severely hamper and delay cable repairs. In countries that have little or no cable-repair capacity, these restrictions also increase costs and sometimes force the use of ill-equipped ships with untrained crews.[106] In the most egregious cases, cabotage laws deter investments.[107] Cabotage laws have particularly bad effects in countries that lack backup cables.[108] Even in less remote areas of the world, the limited supply of repair ships often delays repairs.

The US government, specifically USTR, should seek selective removal of cable-repair cabotage laws from trade agreements.[109] This would allow foreign cable-repair ships to enter and operate in territorial waters, reduce approval requirements, and obligate participating nations to help protect cables in their waters.

CONCLUSION

To support more secure, resilient undersea cable networks, the US government should design and execute a comprehensive national strategy and reform the federal licensing process. While the regulatory process involving the FCC and Team Telecom has helped ensure the viability, integrity, and security of cables, the process needs to be changed. Ensuring that hyperscalers continue to invest in more diverse and secure cable systems requires the government to take concrete steps to shorten the licensing process; make it far more predictable; rein in mitigation measures; and engage the private sector in transparent, productive efforts to share information and improve cable security.

Failure to make progress will continue to deter necessary investments and block efforts to expand and modernize the global cable networks that carry vital data twenty-four hours each day. It is well past time for Washington to meet its obligations to change the complex licensing process, remove obstacles to growth, and demonstrate its commitment to making undersea cable systems far more secure, resilient, and efficient. US national security demands nothing less.

NOTES

1. Submarine Telecoms Forum, Industry Report 2022/2023, at 28 (2022), https://subtelforum.com/industry-report/ [https://perma.cc/B2ZP-E6XZ] [hereinafter Submarine Telecoms Forum 2022/2023 Industry Report].

2. As discussed below, Team Telecom plays a critical role in deciding which applications to build and operate cables will be approved. While Team Telecom is now formally known as the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, this paper will continue to refer to the committee as Team Telecom.

3. Douglas Main, *Undersea Cables Transport 99 Percent of International Data*, Newsweek (April 2, 2015), https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072 [https://perma.cc/5UTD-XYAV]. More precise statistics aren't available, though research shows that the alternative means to carry intercontinental traffic, such as the growing satellite capacity and some terrestrial networks between Europe and Asia, can handle only a very small percentage of international traffic. *See* Alan Mauldin, *Do Submarine Cables Account for over 99% of Intercontinental Data Traffic?*, TeleGeography Blog (May 4, 2023), https://blog.telegeography.com/2023-mythbusting-part-3 [https://perma.cc/EV5N-UURQ].

4. *See* Tim Stronge, *Do $10 Trillion of Financial Transactions Flow over Submarine Cables Each Day?*, TeleGeography Blog (April 6, 2023), https://blog.telegeography.com/2023-mythbusting-part-1 [https://perma.cc/Y7T7-JWXL].

5. *See* Jill C. Gallagher, Cong. Rsch. Serv., R47237, Undersea Telecommunication Cables: Technology Overview and Issues for Congress 1 (2022).

6. *See, e.g.*, Exec. Order No. 14,028, 86 Fed. Rec. 26633, 26633 (May 12, 2021) ("Protecting Our Nation from Malicious Cyber Actors Requires the Federal Government to Partner with the Private Sector").

7. Letter from President Joseph Biden (Mar. 1, 2023), *in* White House, National Cybersecurity Strategy (2023) (prefatory letter by President Biden).

8. *See* 42 U.S.C. §§34–39; *Submarine Cable Landing Licenses*, Fed. Commc'n Comm'n, https://www.fcc.gov/research-reports/guides/submarine-cable-landing-licenses [https://perma.cc/VW4L-LVLR];

Justin Sherman, Cybersecurity under the Ocean: Submarine Cables and US National Security 2–3 (2023). There are, of course, many other national security touch points with undersea cables, over some of which the FCC has no jurisdiction. *Id*. US government strategy is neither coordinated nor comprehensive.

9. In 1858, the Atlantic Telegraph Company laid the first undersea transcontinental cable, which connected Newfoundland to Ireland. *See* 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]. Queen Victoria and US president James Buchanan inaugurated its use by exchanging messages, which was completed at a rate of one letter every two minutes. *See id*.; Duncan Geere, *How the First Cable Was Laid across the Atlantic*, Wired (Jan. 18, 2011, 4:24 PM), https://www.wired.co.uk/article/transatlantic-cables [https://perma.cc/LYB3-Z4NH]. In a time when ocean liners took ten days to cross the Atlantic, the cable foreshadowed a revolution in long-distance communications technology and engineering. Little, *supra*. The cable failed within weeks but led to improvements and more successful efforts. *Id*. Decades passed before telegraph cables were laid from the US across the Pacific Ocean, with the first coming in 1902, linking the US mainland to Hawaii, and then in 1903 linking Hawaii and Midway, Midway and Guam, and then Guam and the Philippines. *See* Camille Morel, French Inst. Int'l Rels., The Pacific Caught in the World Wide Web? Geopolitics of Submarine Cables in Oceania 6 (2022), https://www.ifri.org/sites/default/files/atoms/files/morel_geopolitics_submarine_cables_oceania_2022.pdf [https://perma.cc/7E78-59CY]; *History of the Atlantic Cable & Undersea Communications, the Commercial Pacific Cable Company*, Atlantic-Cable.com, https://atlantic-cable.com/CableCos/ComPacCable/index.htm [https://perma.cc/GT3D-8KJG].

10. *Submarine Cable Frequently Asked Questions*, TeleGeography, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions [https://perma.cc/33MD-AXAC]. A specialized submarine cable industry, including suppliers and vendors, has evolved. There are a handful of submarine cable system suppliers that can lay long-haul cable across oceans, while others design and operate landing stations, run network operation centers, supply specialized networking equipment (e.g., line termination equipment), and provide repair services.

11. Government aid and subsidies to lay cables has a long history; the US and British governments, for example, helped finance the first transcontinental cable. *See* Geere, *supra* note 9. Although a few countries, including China and Russia, own or heavily subsidize domestic cable industries, most countries rely on private enterprise to lay and maintain undersea cables and operate landing stations. *See* Sherman, *supra* note 8, at 5, 7, 9.

12. A study by Synergy Research Group estimates that the "number of large data centers operated by hyperscale providers increased to 659 at the end of the second quarter [2021], having more than doubled since mid-2016." *Hyperscale Data Center Count Grows to 659—ByteDance Joins the Leading Group*, Synergy Rsch. Grp. (Sept. 13, 2021), https://www.srgresearch.com/articles/hyperscale-data-center-count-grows-to-659-bytedance-joins-the-leading-group [https://perma.cc/YP4B-WG66].

13. *See* Larry Schwartz, *Are OTTs from Mars, and Carriers from Venus?*, SubTel F. Mag., Jan. 2018, at 80–81, https://issuu.com/subtelforum/docs/stf-98v2 [https://perma.cc/8TZN-Y2RE].

14. *See* Study to Monitor Connectivity, at 34, CNECT/2020/LVP/0087 (2020), https://op.europa.eu/en/publication-detail/-/publication/a0b01654-9394-11ec-b4e4-01aa75ed71a1 [https://perma.cc/R453-WHD8] ("To increase network resilience, industry players seek to enhance geographic diversity of undersea cable routes."). Microsoft reportedly invested in the cable system MAREA in part to address the need for more cable routes to deal with events like Hurricane Sandy, which temporarily knocked out the TAT-14 transatlantic cable. *See* Rich Miller, *Cable to Cloud: New Data Flows Raise Hopes in Virginia Beach*, Data Ctr. Frontier (Mar. 6, 2018), https://www.datacenterfrontier.com/featured/article/11430309/cable-to-cloud-new-data-flows-raise-hopes-in-virginia-beach [https://perma.cc/UDD9-ABYP]. The earthquakes near Taiwan in 2006 and 2009 that damaged key cables also demonstrated the need for rerouting options and rapid repairs. *See* Winston Qiu, *Submarine Cables Cut after Taiwan Earthquake in Dec 2006*, Submarine Cable Networks (Mar. 19, 2011), https://www.submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006 [https://perma.cc/CT3M-Z6TG]; Michael Clare et al., *Climate Change Hotspots and Implications for the Global Subsea Telecommunications Network*, 237 Earth-Sci. Revs., Feb. 2023, at 2.

15. The massive volcanic explosion in Tonga in 2022 cut the only international cable to the island, and took more than a month to repair. *See* Simon Scarr et al., *The Race to Reconnect Tonga*, Reuters (Jan. 28, 2022), https://www.reuters.com/graphics/TONGA-VOLCANO/znpnejbjovl/ [https://perma.cc/2HP5-Q3QN].

16. A country's cabotage laws, which restrict the operation of sea, air, or other transport services within or into that country, may prohibit foreign vessels from performing cable repair in its territorial waters. *See* Rais Hussin Mohamed Ariff, Opinion, *Cabotage Policy—Let's Get Clever*, Malaysian Reserve (Apr. 9, 2021), https://themalaysianreserve.com/2021/04/09/cabotage-policy-lets-get-clever/ [https://perma.cc/33TY-W9WM].

17. The commonly cited industry standard for the minimum cable operational life is twenty-five years, though in practice the life span depends on a number of factors. Many last longer as a technical matter but lack the bandwidth and speed needed to satisfy current requirements. *See* Submarine Telecoms Forum 2022/2023 Industry Report, *supra* note 1, at 32; Alan Mauldin, *Is the Lifespan of a Submarine Cable Really 25 Years?*, TeleGeography Blog (Apr. 20, 2023), https://blog.telegeography.com/2023-mythbusting-part-2 [https://perma.cc/F4KU-XY3K].

18. Yevgeniy Sverdlik, *How Hyperscale Cloud Platforms Are Reshaping the Submarine Cable Industry*, Data Ctr. Knowledge (Feb. 17, 2021), https://www.datacenterknowledge.com/networks/how-hyperscale-cloud-platforms-are-reshaping-submarine-cable-industry#close-modal [https://perma.cc/MXD5-KGQH] (quoting Alan Mauldin, research director at TeleGeography).

19. *See* Gallagher, *supra* note 5, at 1.

20. *See* Improving Outage Reporting for Submarine Cables and Enhanced Submarine Cable Outage Data, 86 Fed. Reg. 22360, 22361 (Apr. 28, 2021) ("[T]he operation and maintenance of the undersea cables licensed in the United States are essential to the nation's economic stability, national security and other vital public interests.").

21. See Shu Zhuang, *Rise of Hyperscalers Places Greater Importance of Testing Subsea Optical Cables*, Submarine Telecoms F. (Sept. 27, 2022), https://subtelforum.com/stf-mag-feature-rise-of-hyperscalers-places-greater-importance-of-testing-subsea-optical-cables/ [https://perma.cc/ZRC8-MEAX]. Zhuang estimates that more than one hundred cables each year suffer a break. *See id*.

22. *See, e.g.*, Scarr et al., *supra* note 15. Aggression from wildlife, like a shark or barracuda attack on cables, attracts a lot of popular attention but is extremely rare; in any case, cables are now well protected against such attacks. In the wake of press attention driven by a viral YouTube video of a shark biting a cable, the International Cable Protection Committee (ICPC) noted in 2015 that "sharks and other fish were responsible for less than 1% of all cable faults up to 2006. Since then, no such cable faults have been recorded." Press Release, Int'l Cable Prot. Comm., Sharks Are Not the Nemesis of the Internet—ICPC Findings (July 1, 2015), https://iscpc.org/documents/?id=1959 [https://perma.cc/6DA9-AYSW].

23. *See, e.g.*, Qiu, *supra* note 14.

24. *See* Int'l Cable Prot. Comm., *Fish Aggregation Devices (FADs) Risks to Submarine Cable Deployment and Operations* (July 25, 2021), https://www.iscpc.org/documents/?id=3776 [https://perma.cc/9TYB-VR3H] (on fishing); Gallagher, *supra* note 5, at 10. Fishing aggregation devices pose particularly pernicious hazards for cable installation and operation, in part because they can cause abrasive or percussive damage that is hard to both detect and repair. Because of their relatively discrete nature, repair of breaks caused by careless fishing, though common, can be much faster than repair of extensive damage caused by a natural disaster. *See* Int'l Cable Prot. Comm., *supra*.

25. *See* James Kraska, *Submarine Cables in the Law of Naval Warfare*, Lawfare (July 10, 2020, 8:01 AM), https://www.lawfareblog.com/submarine-cables-law-naval-warfare [https://perma.cc/J5HE-822H]. Kraska concludes that the failure of international legal instruments to articulate clear rules means "that adversaries' plans to disrupt international submarine cables during naval warfare are limited only by their national laws and their imagination." *Id*.

26. Eavesdropping on cables on the bottom of the ocean has always been a technique limited to countries with sophisticated submarine vessels and highly specialized electronic equipment. Tapping into cables was relatively easy when cables were composed of copper wires, traffic was

unprotected, and encryption was more easily compromised. Fiber optics, introduced in commercial cables in the late 1980s, has made eavesdropping much more difficult. Today the resiliency and availability of cables are paramount concerns, because strong encryption has made data collection less useful, whether done in the ocean depths or by diverting traffic to convenient intercept points. *See* Matthew P. Goodman & Matthew Wayland, *Securing Asia's Subsea Network: US Interests and Strategic Options*, CSIS Brief (Apr. 2022), at 5, 8–9, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220405_Goodman_SecuringAsia_SubseaNetwork_0.pdf?SHc1AQZLEOcnz1yT9a8qnJbD489cJ0qb [https://perma.cc/TS5G-YT7G]. Cable operators also try to make espionage even harder by investing in sensor technology to detect suspicious contacts. Developments in quantum computing will simultaneously present challenges to existing encryption algorithms and opportunities for stronger security; ignoring the risks would be shortsighted.

27. Undersea cable operators use Network Management Systems (NMS) to ensure satisfactory technical performance. Their systems do not have access to the customer traffic being carried on the fiber, which is also protected by encryption. Disruption of the NMS, moreover, can threaten the availability or reliability of data flows but does not allow for their interception. System operators take care in how they connect NMS to the cable system and other equipment.

28. Some governments, including France and the UK, have also invested in deep-sea defensive measures intended to meet Russia's offensive capabilities. *See, e.g.*, *Les armées se dotent d'une stratégie ministérielle de maîtrise des fonds marins*, Ministère des Armées (Feb. 18, 2022), https://www.defense.gouv.fr/actualites/armees-se-dotent-dune-strategie-ministerielle-maitrise-fonds-marins [https://perma.cc/9CUR-25CS] (announcement by the French minister of the army outlining cooperative seabed strategy with the Ministry of the Armed Forces); HC Deb (Nov. 7, 2022) (722) col. 17, https://hansard.parliament.uk/Commons/2022-11-07/debates/6AFF1DF6-A757-4C9A-982C-FCBE2FEE0C9B/TopicalQuestions?highlight=multi-role%20ocean%20surveillance#contribution-D6AE6584-1B02-42C9-B932-43D89539A420 [https://perma.cc/NMM3-VSHT] (announcement of procurement of Multi-Role Ocean Surveillance Ship and future investments); Charlotte Le Breton & Hugo Decis, Int'l Inst. for Strategic Stud., *France's Deep Dive into Seabed Warfare* (Feb. 25, 2022), https://www.iiss.org/blogs/military-balance/2022/02/frances-deep-dive-into-seabed-warfare [https://perma.cc/8WFT-CLEJ].

29. Nations can also consider creating cable-specific protective corridors in territorial waters, aggregating cables and landing points. *See, e.g.*, Fisheries and Oceans Canada, *The Eastern Scotian Shelf Integrated Management (ESSIM) Initiative: A Strategic Planning Framework for the Eastern Scotian Shelf Ocean Management Plan*, at 30 (Jan. 2003); North American Submarine Cable Ass'n, *NASCA Submittal on the February 2005 Draft for Discussion Entitled "Eastern Scotian Shelf Integrated Ocean Management Plan (2006–2011)"* (Feb. 8, 2006). This strategy has superficial appeal. In theory, a corridor can exclude fishing, shipping, mining, and other activities that might pose a threat to cables, and enforcement is easier in confined areas. In practice, however, creating corridors that are sufficiently wide, numerous, and dispersed is extremely difficult and can lead to dangerous congestion of cables and landing stations. Designated narrow corridors also increase the odds that natural disasters will cause severe outages and invite targeted attacks by terrorist groups and others.

30. Sean Bergin & Tom Soja, 2023 Global Subsea Industry Headwinds and Opportunities, SubTel F. Mag., May 2023, at 31, https://issuu.com/subtelforum/docs/subtel_forum_130 [https://perma.cc/5P4C-F82P].

31. In addition, the Chinese government requires signals to transit a Chinese-controlled facility, empowering Chinese carriers to dictate system design. In a partial response to these Chinese rules, companies have developed newer cables that avoid sending data through Chinese-controlled facilities while crossing the South China Sea.

32. *See* Morel, *supra* note 9, at 15.

33. The Bifrost and Echo cables will connect North America to Singapore and Indonesia, avoiding the congested routes to the north. *See id*. Another proposed cable, Apricot, would use Echo to connect the Philippines, Japan, and Taiwan while purposely skirting Hong Kong. *See id*. The TPU cable will connect the mainland US to Guam, and then on to both Taiwan and the Philippines. Jonathan Kim, *Google's TPU Subsea Cable Revealed amid US-China Tensions*, Dgtl Infra (May 16, 2023), https://

dgtlinfra.com/tpu-subsea-cable/ [https://perma.cc/4MBZ-M3PD] (addressing geopolitical implications of this cable).

34. Hyperscalers pioneered open-architecture undersea cable systems that allow operators to place equipment necessary to control their fiber pairs, including Submarine Line Terminating Equipment, outside shared spaces such as landing stations. Individual owners now typically segregate their equipment into locations they control and secure.

35. Hyperscalers "are helping to push along new innovations inside of the cable systems themselves. New transmission technology to manage higher capacity wavelengths, increased fiber counts for more overall system capacity and streamlined network management, and the push for open systems leading to shared system architecture are just a small sampling of new technologies and ideas these providers are backing." Submarine Telecoms Forum 2022/2023 Industry Report, *supra* note 1, at 82.

36. Submarine Cable Landing License Act of 1921, 47 U.S.C. §34.

37. Executive Order 10,530, 19 Fed. Reg. 2709, 2711–12 (May 10, 1954) (delegates this authority to the FCC); Cable Landing Licenses, 47 C.F.R. §1.767 (FCC Rules). This requirement does not apply to cables entirely within US borders. It applies regardless of foreign control of the cable. *See* James X. Dempsey, Cyber Law Fundamentals ch. 16.4 (2021); *Updates to Chapter 16: National Security: Economic Controls, Trade Limits, Equipment Bans*, Cybersecurity L. Fundamentals, https://cybersecuritylawfundamentals.com/chapter-16 [https://perma.cc/EV43-G39J]. To provide common-carrier services, a submarine cable operator must also obtain an FCC license under Section 214 of the Communications Act of 1934. 47 U.S.C. §214; 47 C.F.R. §1.767(g)(4).

38. The work of Team Telecom is distinct from, but sometimes overlaps with, that of the Committee on Foreign Investment in the United States (CFIUS), which may review foreign investment in and acquisition of US companies in any industry, including those requiring an FCC license.

39. Exec. Order No. 13,913, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643 (Apr. 8, 2020) [hereinafter EO 13,913].

40. *Id*. at 19643.

41. *Id*.

42. The Administration issued the Order in anticipation of a June 2020 Senate subcommittee staff report that criticized the executive branch for its response to Chinese threats to US communications networks. Doug Olenick, *Senate Report: Chinese Telecoms Operated without Oversight*, Gov Info Sec. (June 9, 2020), https://www.govinfosecurity.com/senate-report-chinese-telecoms-operated-without-oversight-a-14409 [https://perma.cc/T8HL-K8XG]; Staff of S. Permanent Subcomm. on Investigations, Comm. on Homeland Sec. & Governmental Affs., Threats to US Networks: Oversight of Chinese Government-Owned Carriers (2020) [hereinafter Threats to US Networks]. In addition, a report from the working group tasked by the FCC to look into risks posed to undersea cables found that Team Telecom was the "principal source of delay" in licensing new routes and landings. Final Report—Interagency and Interjurisdictional Coordination, Commc'ns Sec., Reliability & Interoperability Council, Working Group 4A Submarine Cable Resiliency 12 (2016).

43. I was involved in the early days of Team Telecom, which for a (thankfully) brief time also went by "Team Global Mobile."

44. EO 13,913, *supra* note 39, at 19645; *see also* Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, Report and Order, 35 FCC Rcd. 10927, 10933 (2020) [hereinafter FCC 2020 First Report & Order], https://docs.fcc.gov/public/attachments/FCC-20-133A1_Rcd.pdf [https://perma.cc/TT4Y-3ADU] ("The primary objective of the Committee is to assist the Commission in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the U.S. telecommunications services sector.").

45. EO 13,913, *supra* note 39, at 19645 (Team Telecom may "review existing licenses to identify any additional or new risks to national security or law enforcement interests of the United States.").

46. Press Release, US Dep't of Just., Attorney General Will Chair Committee to Review Foreign Participation in the US Telecommunications Sector (Apr. 7, 2020), https://www.justice.gov/opa/pr/attorney-general-will-chair-committee-review-foreign-participation-us-telecommunications [https://perma.cc/9PYP-E8HE]; EO 13,913, *supra* note 39, at 19643–44. The president has the power to appoint the head of any executive department or agency, or any assistant to the president, as a member of Team Telecom. *Id*. at 19644.

47. Other advisors include officials representing the secretary of the treasury, the directors of National Intelligence and the Office of Management and Budget, the general services administrator, the assistants to the president for national security affairs and economic policy, the director of the Office of Science and Technology Policy, and the chair of the Council of Economic Advisers. *Id*. at 19643–44.

48. *See id*. at 19646–48.

49. Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, Second Report and Order, 36 FCC Rcd. 14848, 14873 (2021), https://docs.fcc.gov/public/attachments/FCC-21-104A1_Rcd.pdf [https://perma.cc/M68X-ZMSE] [hereinafter FCC 2021 Second Report & Order].

50. EO 13,913, *supra* note 39, at 19645 (italics added).

51. *Id*. at 19647–48.

52. *Id*. at 19648.

53. For example, Team Telecom found that a proposed route between the US and Cuba required a secondary assessment, ultimately leading to a denial. Team Telecom, ARCOS-1 USA, Inc., A.SURNET, INC., Application for a Modification to Cable Landing License, Recommendation of the Committee for the Assessment of Foreign Participation in the US Telecommunications Services Sector to Deny the Application (Nov. 29, 2022), https://www.justice.gov/opa/press-release/file/1554426/download [https://perma.cc/8JGX-ENKK]. Team Telecom took similar action in 2020 on a route that would have been the first direct link between the US and Hong Kong. Team Telecom determined that no mitigation measures would address its concerns.

54. EO 13,913, *supra* note 39, at 19647.

55. One caveat: in addition to its advisory role, the State Department has what is essentially veto power over an FCC grant or revocation of a license. Licenses to land or operate submarine cables on US territory "shall be granted or revoked by the Commission except after obtaining approval of the Secretary of State." Executive Order 10,530, *supra* note 37; *see* 47 C.F.R. §1.767(b). This second bite at the apple by the State Department does not seem to apply when the FCC denies a landing station license application.

56. Leading up to the more formalized Team Telecom process, the DOJ recognized the harm that Team Telecom delays can cause, and noted that "we must explore ways to make this process more efficient and expedient." Deputy Assistant Attorney General Adam S. Hickey of the National Security Division Delivers Remarks at the Fifth National Conference on CFIUS and Team Telecom (Apr. 24, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-adam-s-hickey-national-security-division-delivers-0 [https://perma.cc/5YGQ-7FZ4].

57. Regulations state that FCC referral criteria must be flexible and that the FCC exercise discretion when seeking input from Team Telecom. *See* FCC 2020 First Report & Order, *supra* note 44, at 10935–36. In practice, however, the FCC refers all US landing station applications to Team Telecom, which "has recently scrutinized even 100% American projects." Andrew D. Lipman, Ulises R. Pin & Leetal Weiss, *Protecting Submarine Cable Data: Team Telecom Expanding Its Toolkit to Include New Mitigation Measures*, SubTel F. Mag., Mar. 2022, at 25, https://subtelforum.com/stf-mag-feature-protecting-submarine-cable-data/ [https://perma.cc/A4LH-2J29]. For a thoughtful proposal that would improve this practice, *see* David Plotinsky & Morgan Lewis, Analysis: How Team Telecom Can Conduct Faster Reviews in No-Risk Cases at 5–7 (2023).

58. In practice, reviews continue even after the FCC grants a license. On the one hand, Team Telecom has the right to know about changes to licensed cable systems that impact security, and address

those concerns. On the other, these powers have resulted in Team Telecom imposing onerous conditions and led to mission creep.

59. The FCC characterized the changes as establishing "firm timeframes for Executive Branch review of applications." *Submarine Cable Landing Licenses*, *supra* note 8.

60. FCC 2020 First Report & Order, *supra* note 44, at 10942–43.

61. The Standard Questions are publicly available. FCC 2021 Second Report & Order, *supra* note 49, at attachment C, https://docs.fcc.gov/public/attachments/FCC-21-104A1.pdf [https://perma.cc/T9PZ-TXFW].

62. Even the Standard Questions adopted by the FCC remain in limbo. The FCC adopted the Standard Questions in the FCC 2021 Second Report and Order and directed its International Bureau to submit the Standard Questions to the Office of Management and Budget (OMB) for review under the Paperwork Reduction Act, and upon approval to issue a public notice with the effective date. FCC 2021 Second Report & Order, *supra* note 49, at 14873. It seems that has not been done yet.

63. EO 13,913, *supra* note 39, at 19645; FCC 2020 First Report & Order, *supra* note 44, at 10943, n. 112 ("The 120-day initial review period starts on the date the Chair determines that the applicant's responses to any questions and information requests from the Committee, including responses to the Tailored Questions where applicable, are complete.").

64. Threats to US Networks, *supra* note 42, at 47 ("[B]efore the clock begins to run, DOJ must determine that all of its questions have been satisfactorily answered. [citation omitted] This can take—and in some instances, such as those described below, has taken—months."); Lipman, Pin & Weiss, *supra* note 57 ("[I]n practice, it takes several weeks (if not months) for Team Telecom to start the clock, as Team Telecom generally asks multiple rounds of questions before it starts the review clock.").

65. Plotinsky, *supra* note 57, at 3.

66. Pursuant to the Executive Order, Team Telecom's review is to be confined to the national security implications arising from the license authority sought. EO 13,913, *supra* note 39, at 19647. Team Telecom is to make recommendations if "there is credible evidence that the application or license poses a risk to the national security or law enforcement interests of the United States." *Id*.

67. This leaves a vacuum to be eagerly filled by others. Team Telecom's block of the ARCOS-1 cable, which would have connected the US to Cuba, was followed a week later by the announcement of a French-Cuban system, which is now in place. Sebastian Moss, *Submarine Cable Connecting Cuba to Martinique Begins Tests*, Data Center Dynamics (May 4, 2023).

68. The underlying statutory authority, the Cable Landing License Act of 1921, not only is vague but also does not mention mitigation measures. *See* 47 U.S.C. §§34–39.

69. EO 13,913, *supra* note 39, at 19643.

70. One practitioner reviewed eleven license agreements adopted from January 2020 to December 2021 in an attempt to identify commonalities. Lipman, Pin & Weiss, *supra* note 57.

71. Veterans on the company side of the Team Telecom process express to me being routinely shocked to learn what has suddenly become "standard" since they went through the process only months before.

72. Team Telecom, National Security Agreement between Team Telecom and Google/GU, at art. 5(E)(1) (Dec. 17, 2021), https://www.justice.gov/opa/press-release/file/1457291/download [https://perma.cc/4KTP-W6RJ] [hereinafter Google NSA]; Team Telecom, National Security Agreement between Team Telecom and Edge/Meta, at art. 5(E)(1), https://www.justice.gov/opa/press-release/file/1457286/download [https://perma.cc/87SP-RGCY] [hereinafter Edge/Meta NSA].

73. *See* Plotinsky, *supra* note 57, at 7 (recommending that "Team Telecom mitigation be focused only on national security and law enforcement risk arising from the transaction itself.").

74. *See, e.g.*, Bikash Koley, *Introducing Topaz—The First Subsea Cable to Connect Canada and Asia*, Google Cloud Blog (April 6, 2022).

75. The term "Principal Equipment" appears to be expansive and includes software. *See, e.g.*, Google NSA, *supra* note 72, at art. 1(J); Edge/Meta NSA, *supra* note 72, at art. 1(J).

76. *See* Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (requiring that "the Commission shall clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(a))").

77. DOJ's National Security Division says there are currently 185 mitigation agreements stemming from Team Telecom and CFIUS reviews that it monitors. Nat'l Sec. Div., US Dep't of Just., FY 2023 Performance Budget Congressional Submission 10, https://www.justice.gov/jmd/page/file/1492206/download [https://perma.cc/7EC4-KLTR].

78. *See, e.g.*, Google NSA, *supra* note 72, at art. 6(J)(4); Edge/Meta NSA, *supra* note 72, at art. 6(J)(4).

79. EO 13,913, *supra* note 39, at 19648. It's not clear that these could be enforceable in their own right, in spite of the forum selection, specific performance, and other remedy-related clauses. These have all the bargained-for consideration of a shakedown. I've found no example of any effort by the government to enforce one of these instruments under a contract theory. Still, that possibility looms by the nature of the document and serves as yet another risk in investing.

80. The Executive Order provides for continued monitoring of compliance. *Id*. at 19648.

81. Team Telecom members and the advisory agencies can recommend that the president add these agencies to the core group. *See* EO 13,913, *supra* note 39, at 19649.

82. The FCC recognizes that foreign and trade policies can play an important role in the public interest evaluation, and says it relies on Team Telecom input for such information. FCC 2020 First Report & Order, *supra* note 44, at 10935–36.

83. EO 13,913, *supra* note 39, at 19644. Team Telecom advisory agencies may learn of a referral from an FCC courtesy notice. FCC 2020 First Report & Order, *supra* note 44, 10957–58 & n. 207. Team Telecom must also tell the advisors when it is going to conduct a review of an existing license. EO 13,913, *supra* note 39, at 19645.

84. Including more agencies as members of Team Telecom could slow the process down. It is important that the government take the steps described later to make the process efficient.

85. Companies have developed strong discipline and rules about the design, deployment, and operation of cables. The private/public International Cable Protection Committee was created in 1958 to help improve the security of undersea cables. Over time it has published "Best Practices" and other materials. *See ICPC Best Practices*, Int'l Cable Protection Comm. (Nov. 18, 2022), https://www.iscpc.org/publications/icpc-best-practices/ [https://perma.cc/LND3-29KS].

86. The preapproval process for "Principal Equipment" changes is an exception to this. Recent mitigation agreements urge licensees to comply with industry-created standards. As part of the Team Telecom compliance function, the agreements require license holders to disclose technical information and records and allow on-site inspection by US government representatives of domestic and foreign cable facilities. *See, e.g.*, Google NSA, *supra* note 72, at art. 4(A); Edge/Meta NSA, *supra* note 72, at art. 4(A).

87. Each of the December 2021 agreements in the Pacific Light Cable Network (PLCN) matter, for example, provides for annual risk assessments and sets out that "the Parties will use reasonable efforts to identify relevant risks in the assessments." Google NSA, *supra* note 72, at art. 5(E)(1); Edge/Meta NSA, *supra* note 72, at art. 5(E)(1). These agreements also contemplate a conversation between the government and the private parties about risks the government sees in changes to the network and Principal Equipment.

88. License conditions require companies to designate security personnel and a communications channel that is available 24/7 to address Team Telecom concerns. The designees must be US citizens and residents eligible for security clearances. *See, e.g.*, *National Telecommunications and Information Administration Petition to Adopt Conditions to Authorization and License, Letter of Assurances* sec. 1 (Apr. 12, 2021) [https://fcc.report/IBFS/SCL-LIC-20200807-00036/5747678]; FCC 2021 Second Report & Order, Attachment C, *supra* note 49.

89. For ideas on enhanced collaboration, *see* Joseph B. Keller, *The Disconnect on Undersea Cable Security*, Lawfare (May 7, 2023, 10:00 AM), https://www.lawfaremedia.org/article/the-disconnect-on-undersea-cable-security [https://perma.cc/BD4C-7D83].

90. Eliminating delays should be a common goal shared by government and business. Observers say, however, that Team Telecom uses the drawn-out process to let proposals die on the vine; inaction can help avoid tough decisions. True or not, this is a harmful perception.

91. More specific authorization could also help address the lurking question of whether the FCC's increasing licensing requirements exceed the agency's authority under the Cable Licensing Act. *Cf.* West Virginia v. E.P.A., 142 S. Ct. 2587 (2022).

92. Meaningful participation by State, Commerce, and USTR could discourage extraneous inquiries, untethered to the requested license authority.

93. An analogy may help. To design, build, and maintain a bridge over a river, a construction company must secure regulatory approvals designed for public safety. The regulator shouldn't attempt to wield its inherent bargaining power to regulate a contractor's ability to use that bridge or control other services it may offer.

94. Elisabeth Braw, *Decoupling Is Already Happening—Under the Sea*, Foreign Pol'y (May 24, 2023, 12:38 PM), https://foreignpolicy.com/2023/05/24/china-subsea-cables-internet-decoupling-biden/ [https://perma.cc/3TD8-GG8Q].

95. The White House warned recently that "a quantum computer of sufficient size and sophistication—also known as a cryptanalytically relevant quantum computer (CRQC)—will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions." Memorandum from the White House on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (May 4, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ [https://perma.cc/SUG8-FR98]; *see also* Herb Lin, *A Retrospective Post-Quantum Policy Problem*, Lawfare (Sept. 14, 2022, 9:34 AM), https://www.lawfaremedia.org/article/retrospective-post-quantum-policy-problem [https://perma.cc/3YU6-MSTP]; Michaela Lee, Harv. Belfer Ctr., Quantum Computing and Cybersecurity (July 2021), https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity [https://perma.cc/QTL5-S5T3]; *Quantum-Safe Cryptography (QSC)*, ETSI, https://www.etsi.org/technologies/quantum-safe-cryptography#:~:text=Quantum%2Dsafe%20cryptography%20refers%20to,quantum%20computer%20has%20been%20built [https://perma.cc/GH39-6YD3].

96. The Chinese government declared that it is all-in on quantum computing in its 13th and 14th Five-Year Plans (2016 and 2021). *See* Rogier Creemers et al., *Translation: 14th Five-Year Plan for National Informatization—Dec. 2021*, DigiChina (Jan. 24, 2022), https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/ [https://perma.cc/26A6-MY9B]; PRC State Council, *Translation: The National 13th Five-Year Plan for the Development of Strategic Emerging Industries* (Etcetera Language Group, Inc. trans., Ben Murphy ed., Dec. 9, 2019), https://cset.georgetown.edu/wp-content/uploads/Circular-of-the-State-Council-on-Issuing-the-National-13th-Five-Year-Plan-for-the-Development-of-Strategic-Emerging-Industries.pdf [https://perma.cc/BF9Q-KF55]; *see also* Glenn S. Gerstell, Opinion, *I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution*, N.Y. Times (Sept. 10, 2019), https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html [https://perma.cc/8S6M-34X5].

97. *See, e.g.*, Phil Venables, *How Google Is Preparing for a Post-Quantum World*, Google Cloud Blog (July 6, 2022), https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world/ [https://perma.cc/Z5EZ-LVA5].

98. *Post-Quantum Cryptography*, Nat'l Inst. Standards & Tech., https://csrc.nist.gov/Projects/post-quantum-cryptography [https://perma.cc/V5VA-2KYW]; Cybersecurity & Infrastructure Sec. Agency, Preparing Critical Infrastructure for Post-Quantum Cryptography (August 2022),

https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf [https://perma.cc/3MRA-TX2U].

99. Last year, Google announced it has already implemented quantum-resistant cryptography in addition to existing protections. ISE Crypto PQC working group, *Securing Tomorrow Today: Why Google Now Protects Its Internal Communications from Quantum Threats*, Google Cloud Blog (Nov. 18, 2022), https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms [https://perma.cc/2P86-82V3]. Microsoft is also working with the National Institute of Standards and Technology (NIST) project and has its own research effort. *Post-Quantum Cryptography*, Microsoft, https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/ [https://perma.cc/FKS5-66JM]. The same is true for Amazon, Matthew Campagna, *Preparing Today for a Post-Quantum Cryptographic Future*, Amazon Sci. (July 26, 2022), https://www.amazon.science/blog/preparing-today-for-a-post-quantum-cryptographic-future [https://perma.cc/D2N7-247X], and Meta, *Using AI to Find Post-Quantum Cryptography's Vulnerabilities*, Meta AI (July 13, 2022), https://ai.facebook.com/blog/using-ai-to-find-post-quantum-cryptographys-vulnerabilities/ [https://perma.cc/CR6T-EU8G], among many companies.

100. Chris Jay Hoofnagle & Simson Garfinkel, *Quantum Cryptanalysis: Hype and Reality*, Lawfare (Feb. 16, 2022, 8:01 AM), https://www.lawfaremedia.org/article/quantum-cryptanalysis-hype-and-reality [https://perma.cc/F4ZQ-WNG5].

101. *See* Booz Allen Hamilton, Chinese Threats in the Quantum Era 4 (2021). "Two Chinese telecommunications providers in particular, China Telecom (CT) and China Mobile International (CMI), have significantly expanded their networks in the past decade. Both are now significant players in the global non-Chinese Internet traffic transit market, with extraordinary access to—and ability to divert—routine network traffic of major and minor nations globally, especially in recent years." Yuval Shavitt & Chris C. Demchak, *Unlearned Lessons from the First Cybered Conflict Decade—BGP Hijacks Continue*, Cyber Def. Rev. (Winter 2022), at 198, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/20_Shavitt_Demchak_CDR_V7N1_WINTER 2022.pdf [https://perma.cc/6KKL-RMCC].

102. Team Telecom's denial of the US-Cuba cable raised eyebrows, coming as it did after the State Department recommended construction of a cable to Cuba. Bureau of Western Hemisphere Affs., Dep't State, Cuba Internet Task Force: Final Report (June 16, 2019), https://www.state.gov/cuba-internet-task-force-final-report/ [https://perma.cc/R4ZY-PUV2]. *See also* Doug Madory, *Cuba and the Geopolitics of Submarine Cables*, Kentik (Jan. 12, 2023), https://www.kentik.com/blog/cuba-and-the-geopolitics-of-submarine-cables/ [https://perma.cc/XR2Q-QZ9V]. Madory asserts that the rationale in the recommendation "reveal[s] a fundamental misunderstanding of how the logical internet and its underlying physical infrastructure work together." *Id*. Recent reports from a US government official about China using Cuba as a base for spying may add some color to the decision. Karoun Demirjian & Edward Wong, *China Has Had a Spy Base in Cuba for Years, US Official Says*, N.Y. Times (June 10, 2023), https://www.nytimes.com/2023/06/10/us/politics/china-spy-base-cuba.html#:~:text=A%20Chinese%20spy%20base%20or,to%20a%20Biden%20administration%20official [https://perma.cc/K9TN-U42Q].

103. 47 C.F.R. §1.767(a)(5).

104. In its rules, the FCC acknowledges that concealment of facilities could help protect them. 47 C.F.R. §1.767(g)(3).

105. The current rules already explicitly exclude these maps from the requirement that applications and materials be open to public inspection in the FCC offices. 47 C.F.R. §1.767(c).

106. "Cabotage and crewing restrictions in certain territorial waters can increase the cost of facilities and repairs and 'force' the use of vessels that lack proper equipment and are manned by inexperienced crews. These laws generally impair operations and economies of scale for maintenance companies. Restrictions can also delay critical repairs, as nations may require exemptions or waivers for vessels that are foreign-flagged or crewed. Cabotage and crewing restrictions can also harm connectivity in neighboring countries." *See* Int'l Cable Protection Comm., Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables 9, https://www.iscpc.org/documents/?id=3733 [https://perma.cc/CBE9-B7V2].

107. *See, e.g.*, Adrian Wong, *Malaysia Admits Losing Undersea Cable due to Cabotage!*, TECHARP (Oct. 9, 2021), https://www.techarp.com/business/malaysia-undersea-cable-cabotage/ [https://perma.cc/9MXX-XT5E].

108. When Tonga suffered an enormous volcanic eruption in 2022, seismic activity broke the only undersea cable to the island. This hindered attempts to bring in aid. Getting a repair ship to the area took over a week, and repairing the broken sections of cable took more than a month. Winston Qiu, *Tonga Cables Cut after Volcano Eruption, at Least Four Weeks to Restore*, SUBMARINE CABLE NETWORKS (Jan. 19, 2022), https://www.submarinenetworks.com/en/systems/australia-usa/tonga-cable/tonga-cable-cuts-after-volcano-eruption [https://perma.cc/3W5A-TRH4].

109. *See, e.g.*, Digital Economy Agreement, Austl.-Sing., Aug. 6, 2020, [2020] ATNIF 11, art. 22 (entered into force Dec. 8, 2020).

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

The preferred citation for this publication is Richard Salgado, *Undersea Cables, Hyperscalers, and National Security*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2304 (September 12, 2023), available at https://www.lawfaremedia.org/article/undersea-cables-hyperscalers-and-national-security.

ABOUT THE AUTHOR

RICHARD SALGADO

Richard Salgado was an early member of Team Telecom while a prosecutor with the US Department of Justice, Computer Crime and Intellectual Property Section. He later spent over a dozen years at Google, responsible for national security and law enforcement legal issues. He currently teaches at the law schools of Stanford and Harvard and is the principal of Salgado Strategies LLC.

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