CENTER FOR SPACE POLICY AND STRATEGY

FEBRUARY 2022

GLOBAL COMMUNICATIONS INFRASTRUCTURE: UNDERSEA AND BEYOND

LORI W. GORDON AND KAREN L. JONES
THE AEROSPACE CORPORATION

AEROSPACE

LORI W. GORDON

Lori W. Gordon leads space enterprise integration initiatives in the Corporate Chief Engineer's Office at The Aerospace Corporation. In this role, she serves as an expert in national and homeland security, cybersecurity, and infrastructure risk, and resilience, providing leadership across a range of critical infrastructure protection initiatives and internal technology strategy and investment. Gordon is also a partner with Aerospace's Center for Space Policy and Strategy (CSPS) and leads Aerospace's engagement with myriad collaborators, including the Space Information Sharing and Analysis Center and the National Security Institute (NSI). With more than 20 years of experience, Gordon has contributed to the development of national-level strategies, capabilities, and programs across homeland, intelligence, and civil agencies. Gordon has a bachelor's degree in geography from the University of Maryland, College Park, and a master's degree in public administration from the University of Massachusetts, Amherst.

KAREN L. JONES

Karen L. Jones is a senior project leader in the Center for Space Policy and Strategy at The Aerospace Corporation. In her role as a space economist and technology strategist, she has been responsible for performing and managing a variety of projects, including federal R&D, research grants, internal R&D projects, commercial space engagements, new space architectures for the Office of Director of National Intelligence, and R&D portfolio management for the Department of Homeland Security. Prior to joining Aerospace, Jones worked as a management consultant for IBM Global Services focusing on the telecommunications industry, and later e-business strategy for commercial companies and the federal sector. Prior to IBM, Jones worked as a management consultant with Arthur D. Little where she was focused on international privatization projects, technology commercialization, environmental consulting, and risk management. Jones has a bachelor's degree in geology from Louisiana State University and an M.B.A. from the Yale School of Management.

ABOUT THE CENTER FOR SPACE POLICY AND STRATEGY

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

Contact us at www.aerospace.org/policy or policy@aero.org

Summary

It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy. We have allowed this vital infrastructure to grow increasingly vulnerable and this should worry us all.

— Admiral James Stavridis, US Navy (Ret), 2017[1]

Today's high-speed data connectivity depends on a vast global network of infrastructure across space, air, land, and sea with undersea cable infrastructure (UCI) serving as the primary means for intercontinental and "long-haul" communications. National economies are dependent on undersea cable traffic and, increasingly, UCI acts as a conduit to ensure that global data traffic reaches data centers and end users. The UCI landscape is changing and includes an increasing variety of state actors—such as the growing economies of Brazil, Russia, India, China, and South Africa. Nonstate commercial actors (such as hyperscale content providers Google, Facebook, Microsoft, and Amazon) are also seeking to control their data and networks through huge investments in submarine cables. Active investments by both state and nonstate actors will invariably influence the growth, geopolitics, and security of this sector.

This paper focuses on policies to secure UCI and make it more resilient and less vulnerable. Understanding the role of submarine cables within the larger context of the global data commons (spanning space, terrestrial, air, and sea networks) will be critical. As network operators as well as commercial and government stakeholders plan for emerging technologies and architectures, hedging risks for future connectivity will ensure that our data backbone will be secure for years to come.

Introduction

Undersea cables, or submarine cables, link the continents of the world together and are the "backbone" for international data connectivity. The vast majority of the world's internet data traffic is routed through undersea cable infrastructure (UCI) which lies at the bottom of the ocean. These fiber optic cables, primarily owned and operated by commercial consortiums and privately owned social

media and cloud or "hyperscale" data providers, are vital for commerce, economic stability, and national security. Not surprisingly, much of the general UCI discourse has focused on evolving customer needs, including the increasing demand for transmission capacity. Yet despite ongoing market expansion and technology improvements, UCI remains at risk from a variety of unintentional and adversarial threats, including physical hacking to disrupt internet communications and data exfiltration to illegally target, copy, or transfer sensitive data.[2] (See Appendix A: Undersea Cable Faults, Disruptions, and Internet Blackouts). Although current technology and policy approaches are helping to mitigate submarine cable vulnerabilities, national-level coordination is needed to enhance UCI resiliency, including a future vision of the role that satellites can play to diversify and broaden the communications network architecture.

The world is more interconnected than ever, and UCI remains the long-haul carrier for the vast majority of the world's data traffic. Therefore, it seems reasonable and prudent to ask: Who is investing in UCI networks? Who owns the cables? What type of market and technical control do these UCI stakeholders have? Where are the vulnerabilities and why should we care?

UCI Networks: Key Elements and Trends

Submarine Cable Networks

The majority of the world's communications throughput resides in the "cloud," a vast global network of remote servers which are linked together through "long-haul" cable fibers lying on the seabed between land-based stations (see Figures 1 and 3). Public source estimates vary, but approximately 95 to 99 percent of intercontinental internet traffic is routed through UCI. Demand for UCI capacity is fueled by an exponential growth in web traffic, consumer expectations for increasing data speeds, and steady enterprise cloud adoption trends.[3*]

National economies of many countries are dependent on undersea cable traffic. The U.S. Clearing House Interbank Payment System (CHIPS), for example, serves a range of financial institutions and depends on UCI to transmit financial transactions to more than 22 countries. CHIPS accounts for approximately $1.8 trillion daily in domestic and international payments transactions.[4,5,6] Not surprisingly, the U.S. Department of Homeland Security (DHS) has identified UCI as "critical infrastructure," which means that its "incapacitation or destruction would have a debilitating effect on security, national economic security."[7] Despite the high consequences, UCI is increasingly at risk from a variety of unintentional and adversarial threats, ranging from environmental hazards to data exfiltration. These security challenges should spark a more inclusive dialogue between the government and commercial sector on future global communications and the steps the U.S. should take now to mitigate the risk of UCI disruption.

Satellites, terrestrial fiber, and mobile carrier networks often serve the first and last mile, with the middle mile connectivity relying on terrestrial fiber or undersea cables networks. Figure 1 provides an overview of the diverse connectivity options for middle and last mile connectivity.

[*]Lit fibers are actively deployed, and dark fiber is used as reserved capacity.

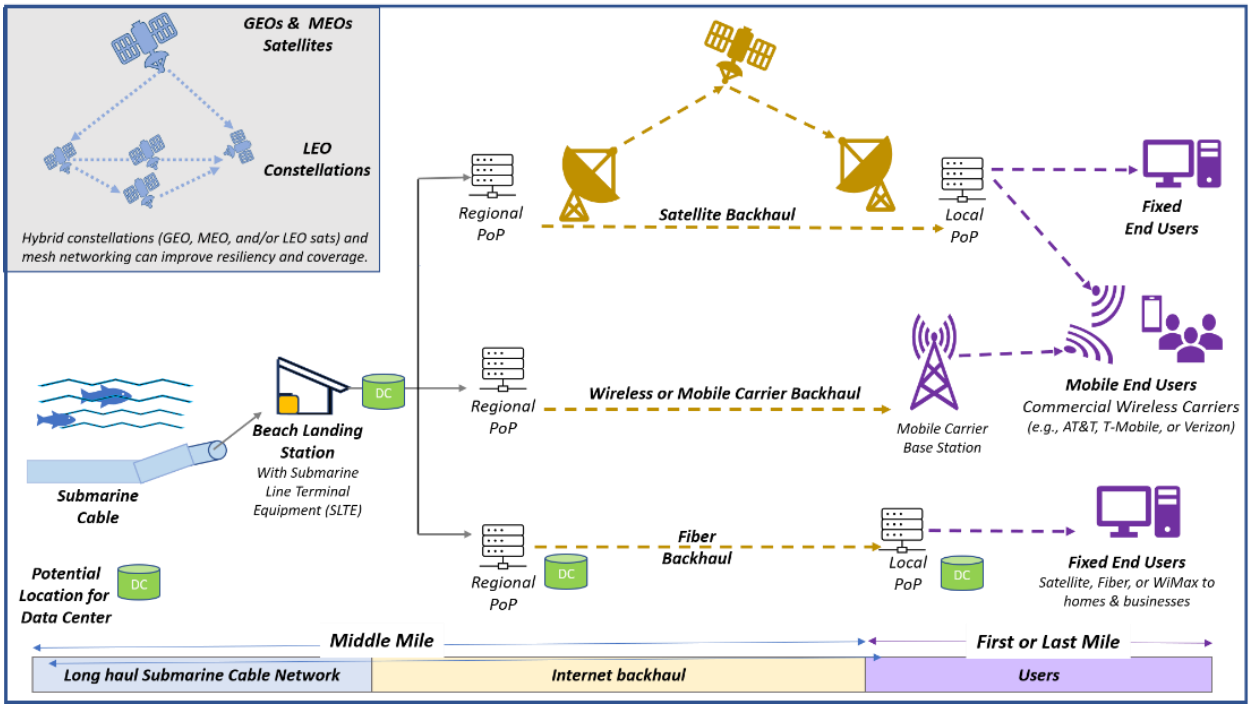

Figure 1: UCI networks – key elements: *UCI infrastructure provides the connectivity to data centers, terrestrial fiber and cables, mobile carrier networks, and satellites. Although submarine cable capacity dominates the long-haul transoceanic data transport market, in the future a range of connectivity platforms might capture a larger share, including HTS GEO satellites to large LEO constellations. Network operations centers and data centers can be strategically located at various locations depending upon performance criteria and business needs. (Acronyms: DC = Data Center; HTS = High Throughput Satellites; GEO = Geosynchronous Equatorial Orbit; MEO = Medium Earth Orbit; LEO = low Earth orbit; UCI = Undersea Cable Infrastructure)*

Internet Backhaul Networks

The submarine communications cable makes landfall near the landing station which houses the submarine line terminal equipment (SLTE). This is where the "wet plant" (submarine cable) meets the "dry plant" (SLTE) where the cable terminal box divides the communications cable into the optical fiber and the power supply line. Other key elements include the line terminal equipment; network protection equipment; and network management equipment, the latter of which acts as a traffic cop by directing data to backhaul networks that could include any combination of terrestrial fiber, wireless or mobile carriers, or satellite (see Beach Landing Station, Figure 1). In a more recent trend, cable operators are now choosing which vendors will supply their wet plant and which vendors are most suitable for the dry plant. This "open cable" approach is a shift away from closed turnkey systems and may help operators seek best-in-breed and encourage greater competition.[8]

Data Centers and Users

Data center operators are evolving their business models and seeking more efficient paths and new ways to move data around the world. Figure 1 shows a range of potential locations for data centers. Some data center providers are colocating their centers at UCI landing stations to take advantage of shared resources and economies of scale, while other centers choose to be closer to "the edge." These "edge" data centers are typically smaller and closer to customers.

Because data centers are power intensive and 80 percent of their costs are related to cooling, some

data centers are moving to cooler climates, such as Sweden, Norway, and Iceland. Other data operators are attracted to sites where they can tap into renewable energy, including solar and windfarms. Microsoft Azure, for instance, has been studying how to design an underwater data center that takes advantage of seawater currents for cooling and available renewable energy from offshore tides and waves. The underwater locations are considered "secure" and logistically practical, and they are close to coastal populations and customers.[9]

Latency Advantage for Free Space Optics

Optical intersatellite links (OISL) offer low latency point to point advantage, compared to submarine or terrestrial optical fiber networks because the light is not impeded by atmosphere or refractive materials. By contrast, a fiber optic communication fiber (index of refraction is approximately 1.5) can slow down the light beam due to the refractive properties of the fiber.† The speed of light in a vacuum is 50 percent higher than the speed of light in optical fiber. Future optical wireless satellite networks (e.g., LEO constellations including *Starlink*, TeleSat and *Kuiper*) may target higher profit margin applications—such as high-speed financial trades and gaming.[10]

Looking to the future, technical challenges remain as free space optic links require very precise pointing and beam steering capabilities to allow satellites to successfully link.

Satellites: Future Architectures

For the near term, UCI will continue to be the communications backbone to transport international data traffic. However, the world of connectivity is changing, with large commercial LEO constellation operators like SpaceX *Starlink*, TeleSat *Lightspeed*, and OneWeb already deploying their constellations. Additionally, another commercial provider, Amazon *Kuiper*, is well into the planning and licensing stage of its large LEO constellation. These LEO constellations aim to provide global broadband services.

Strategic partnerships between these satellite constellations and terrestrial wireless networks will allow mutual operational benefits. Terrestrial networks will extend coverage to remote and rural areas, and LEO satellite networks will provide backhaul internet capacity. Recent partnerships include:

- Verizon Communications and Amazon *Kuiper*
- AT&T and OneWeb[11]

These partnerships could enable future high-speed, high-capacity long-haul networks — potentially competing for global market share with UCI. How is this possible? Advances in free space optics using laser communications continue to mature amid a general trend toward hybrid networks. Over time, connectivity options will expand, as new satellite constellation architectures with optical intersatellite links (OISL) overcome technical challenges, such as precisely aligning optical lasers to link with other LEO satellites traveling at high speeds relative to each other. Assuming OISL capabilities continue to advance, satellites could operate as a global mesh network, with each satellite operating as a node. It is conceivable that satellite constellations could offer gigabit speed data networks, offering a competing high-speed path to undersea cable fiber data networks. Alternatively, data network owners and operators could view space-based long-haul networks as one more technology option to ensure overall network resilience (see Appendix B. Connectivity Platforms: Strengths, Weaknesses, and Market Maturity).

† There are terrestrial equivalents of guided free-space optics such as the use of hollow-core fiber, but they have significantly shorter reach and increased losses that are prohibitive for undersea use.

For now, satellite operators and UCI providers are connectivity partners who often depend upon each other to move data across the globe. See Appendix B for an overview of existing air and space connectivity platforms. The submarine cable industry and satellite sector will mutually influence each other due to a range of interdependencies, including market drivers, security concerns, and technology innovation.

Undersea Cable Industry: History, Market Trends, and Investments

UCI History and Evolution

The submarine cable industry, like many industries, has changed dramatically since the dawn of the digital age. Prior to the internet boom, undersea cable companies were generally built by telecommunication carriers to carry voice data which had relatively predictable traffic. As recently as 1988, microwave and satellites were the world's main data carriers. Yet in that year, the first fiber only cable, the Trans-Atlantic-8, became operational. Fewer than three years later, in July 1991, fiber-optic cables surpassed satellites as the dominant media supporting global digital networks.[12] During the 1990's dot-com boom, the telecommunications industry spent more than $20 billion USD laying undersea fiber-optic cables from New York to London and through the Mediterranean to prepare for the internet explosion.

The sudden growth in submarine cable data traffic surprised many market analysts. UCI is now the primary means of delivering international communications due to the significant expansion of fiber-optic communications capacity, often providing high speed capacity at lower costs compared to satellites.[13]

Global Internet Usage and Market Momentum for UCI Development

The graph in Figure 2 suggests a strong correlation exists between high international internet traffic growth (compounded annual growth rate or CAGR over five years) and internet usage as a percent of market penetration. More mature markets (right side of x-axis) experience less international market growth, as they have already established their international networks. The size of each bubble is proportional to the internet user population in each region. For example, Asia has 2,762 million internet users and USA/Canada has 348 million users.[14]

Mature internet markets, such as North America and Europe, demonstrate lower rates of growth in international data traffic. This is not surprising since these countries have already established many of their needed international routes and have arrived at a more advanced stage of market growth where they are keeping up with *current* demand. By contrast, less mature and emerging internet markets, such as Africa and Asia, are experiencing faster growth in international internet traffic growth and are striving to meet *pent up* demand for international connectivity. Note that Africa and Asia are also the same regions that are experiencing significant investments and activity for subsea cable connections and buildouts. Of course, this does not tell the whole story. In addition to increased internet adoption (new users), existing internet users expect increased bandwidth. Between 2018 and 2023, users will see their average broadband speeds increase from 45.0 Mbps to 110.4 Mbps. New UCI routes and capacity expansion for existing cables are striving to meet customer expectations for increased capacity and speeds. In brief, rapidly maturing internet markets in Asia and Africa, along with increasing global expectations for increased broadband speeds, are driving investments and growth.

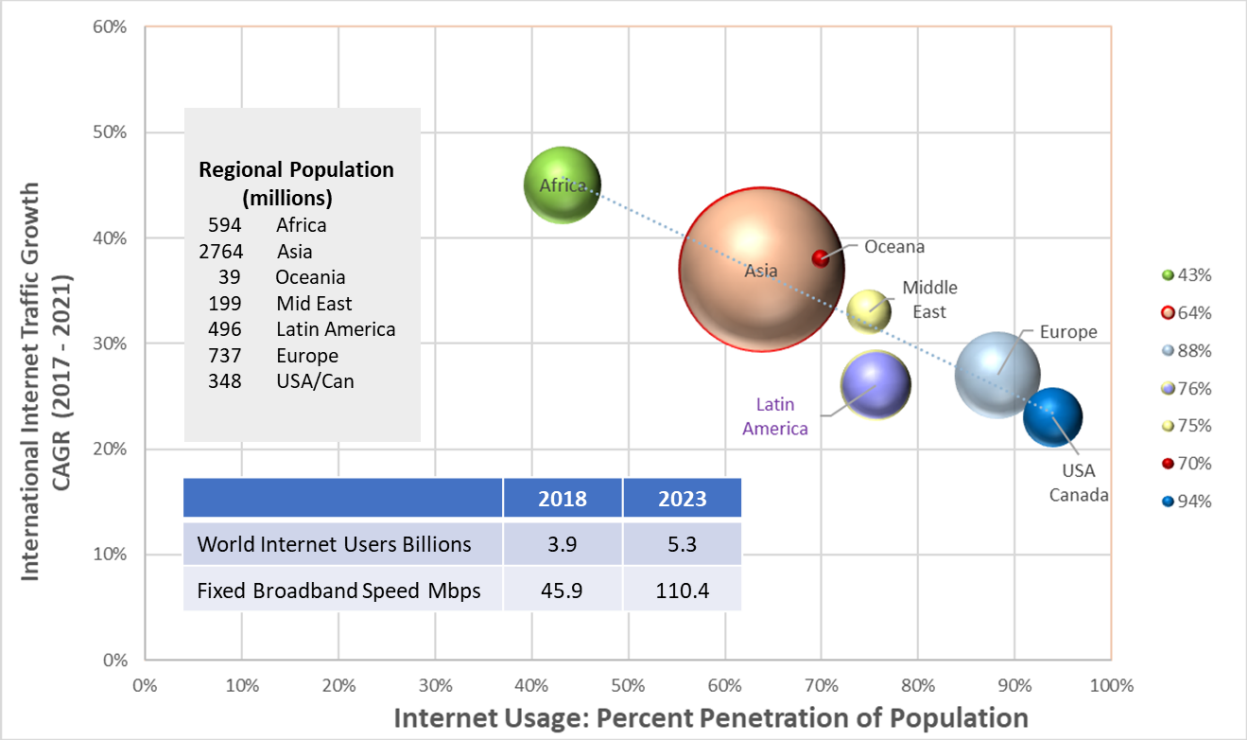

Figure 2: International internet traffic growth and market momentum for UCI development. *Size of each sphere is proportional to each region's internet user population. Source: statistics provided by TeleGeography for International Traffic Growth and Internet World Stats for internet usage. (https://www2.telegeography.com,https://www.internetworldstats.com/stats.htm)*

Cable Ownership

Since the first transatlantic telegraph cable in 1858, undersea cables have generally been owned and installed by private companies. Figure 3 shows global cables and landing site nodes.[15] There are approximately 436 operating submarine cables owned by a collaboration of private investors, tech companies, or governments. These cables transport almost all transoceanic traffic around the world, of which 50 cables serve the Unites States, entering about 20 zones.[16] On the East Coast, they are grouped together in New York, New Jersey, Virginia Beach, and Miami, and on the West Coast, near Los Angeles, San Francisco, central California, and Oregon.

The three most commonly registered types of cable ownership include:

1. **Single owner.** Typically, nation-state-backed entities or cloud/media service providers, including "hyperscale" content providers (e.g., Google and Microsoft).

2. **Consortium**. Ownership model composed of multiple commercial entities.

3. **Public-private partnership (PPP)**. An agreement that involves public and private sector stakeholders. Both parties share equity and risk to deliver a public good, such as increased

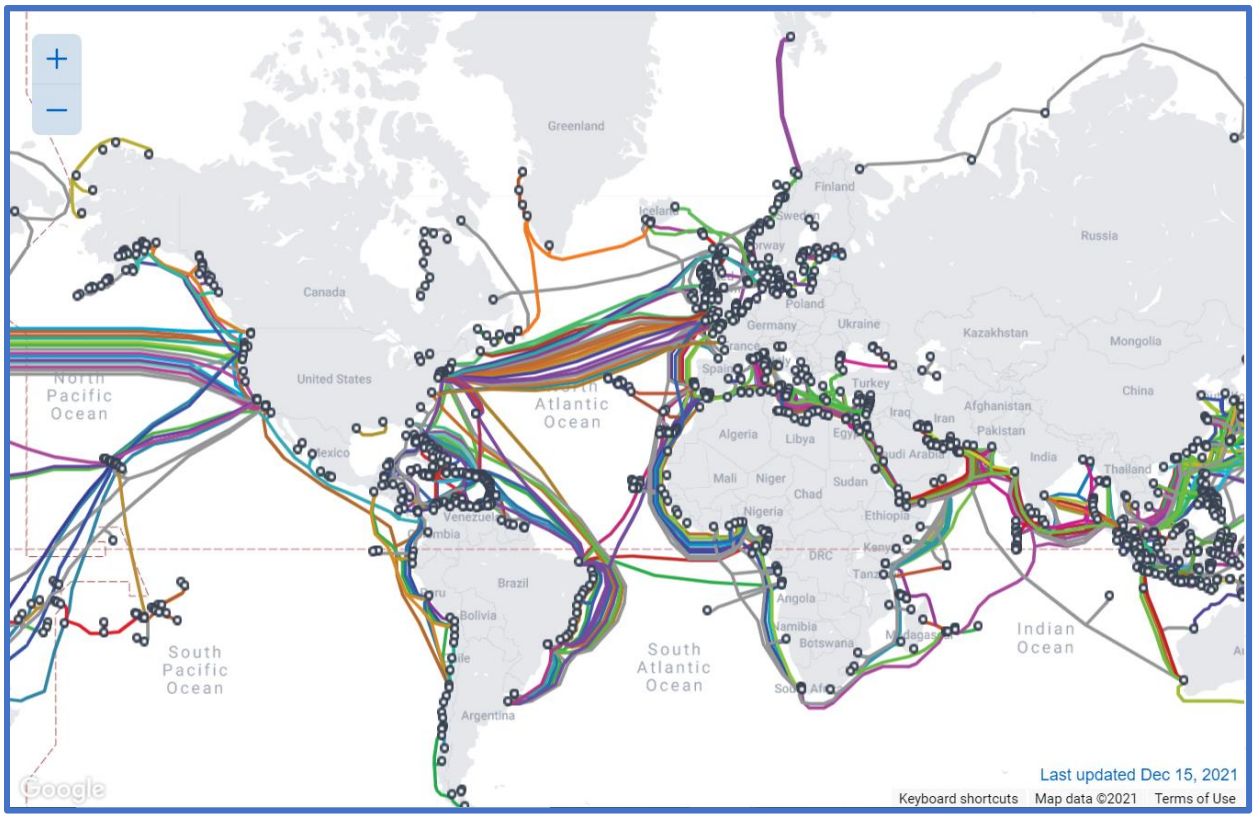

Figure 3: Global submarine cables including landing sites. Approximately 436 cables operating around the world, with approximately 50 serving the U.S. *Source: TeleGeography. December 15, 2021 (https://www.submarinecablemap).*

> connectivity and the resultant social and economic benefits that the UCI provides. An example is Telecom Namibia and Paratus Telecom, which funded the Namibian link to Google's new undersea cable between South Africa and Portugal to bring faster and reliable broadband to the Namibian people.[17]

Note that all three cable ownership types (single owner, consortium, and public-private partnership) might lease their capacity to telecom carriers who, in turn, may sublease to their customers. This can introduce transparency challenges in who owns the cables.

The Rise of Commercial Hyperscale Content Providers

Non-state or market actors are responding to the global need for internet access and the world's apparently unquenchable thirst for data. According to Cisco, nearly two-thirds of the global population will have Internet access by 2023. There will be 5.3 billion total Internet users (66 percent of global population) by 2023, up from 3.9 billion (51 percent of global population) in 2018. Fixed broadband speeds will more than double by 2023, reaching 110.4 Mbps, up from 45.9 Mbps in 2018.[18] Over the past decade, Brazil, Russia, India, and China — the four fast-growing market countries — have accelerated in the number of Internet users and is forecast to grow exponentially in the next few years. Given their large populations, China and India are leaders, with China, for example, forecast to increase from 700 million users in 2016 to 950 million in 2021.[19]

Internet content providers (e.g., Internet services and infrastructure; data centers; cloud computing,

networking and storage; and web hosting) started as significant purchasers of capacity on submarine networks. During 2010, major content providers realized that they could influence networks and lower the cost per bit by owning their data transport. Google, for instance, became a partial owner in the "Unity" cable stretching 9,620 km from Chikura, Japan to Redondo Beach, California.[20] Fast forward to 2022, data demand has incentivized "hyperscale" content providers—such as Google, Facebook, Amazon, and Microsoft—to own and operate their own cables.‡ U.S.-based internet content providers have transformed the submarine cable industry and now account for 80 percent of 2018–2020 transatlantic cable investment, up from 20 percent in 2015-2017.[21] In fact, Google has become by far the biggest investor in submarine cables, owning six active cables with plans to have eight more ready by 2022.[22] Today, Google and Facebook own about 29 percent[23] of all cables. Some they own exclusively—for example, Google owns the entirety of the Curie cable, which runs from Chile to Los Angeles.[24] An executive from Facebook noted that "over the years we have advanced from leasing cables, to becoming anchor tenants. And more recently we have made longer term commitments as investors. We own the connecting infrastructure to our datacenters."[25]

According to Tim Stronge, VP Research with TeleGeography, "Hyperscale companies often provide a healthy stimulus to the industry. They don't mind taking a hit on undersea cable investment because these expenses are capital investments and internal to their business models. It would have been impossible to finance some of the cables we use today without direct investment from hyperscale providers." Stronge added that these hyperscale content cable investors often work under consortium business models, allowing smaller investors to participate.

Hyperscale content providers now dominate international capacity. In 2020, hyperscale content providers used 66 percent of total international capacity, up from less than 10 percent in 2012.[26]

More Commercial Submarine Cable Expansion

More cable is being laid each year to meet the growing demand for bandwidth and to replace aging cables, as well as to prioritize route diversity and underserved markets.

Facebook's initiative "2Africa" will extend over Africa, Europe, and Asia, stretching over 45,000 kilometers (27,962 miles) with the recent addition of nine landings referred to as the "2 Africa Pearls." The undersea cable will directly connect three continents—Africa, Europe, and Asia—and will bring high speed internet to 3 billion people across 33 countries, representing 36 percent of the world's population.[27] Google also announced a cable to connect the U.S. to Britain and Spain to upgrade its aging infrastructure and to accommodate increased bandwidth demands for data-intensive services such as Netflix and Zoom.[28,29]

For policymakers who want to ensure that U.S. industry maintains a dominant undersea cable market position, the expansion of hyperscale content providers as cable owner/operators has supported American interests to dominate the global internet. However, U.S. ownership is a far cry from hegemonic control. In order to ensure that United States UCI players can continue to successfully own and operate undersea cable systems in an intensely competitive and dynamic business environment, regulators must work to ensure that competition is

‡ Other terms for "content providers" include hyperscalers, web-scale companies, OTTs (over-the-top providers), ICPs (internet content providers), or CSPs (cloud service providers).

fair and that ownership is transparent. Although the U.S. appears to be in a good position, gross margins and operating results can fluctuate significantly, and the market composition could shift again.

UCI Competitive Landscape and Geopolitics

Beyond American hyperscale data companies' investment in cables, China's interest in UCI development and ownership has also grown beyond its own shores and those of its protectorates. China is now engaged in cable projects in more than 80 countries as part of its $79 billion Digital Silk Road (DSR) strategy to become a world leader in providing physical infrastructure in the digital space, including UCI and data centers.[30,31] And as the DSR continues to expand, worries about its influence on recipient states will likely grow. According to the Council on Foreign Relations, Chinese firms are bringing technology and additional benefits to developing countries. But concerns have been raised that "China [could also] use the DSR, a component of its larger Belt Road Initiative[§], to enable recipient countries to adopt its model of technology-enabled authoritarianism, which would be detrimental to personal freedoms and sovereignty in those countries."[32] Additionally, China's influence is growing in developing countries. As of 2019, more than 70 percent of African nations and the African Union signed memoranda of understanding (MOU) with Beijing on the BRI (Belt Road Initiative).[33]

An example of how Chinese tech companies are serving to expand China's influence across global data networks, Huawei Marine (recently rebranded as HMN Technologies Co., Ltd. or "HMN Tech"), has partnered in joint ventures with British company Global Marine Systems to become the fourth largest player in an industry long dominated by IT and fiber optic cable manufacturers. By 2020, the company built or repaired almost a quarter of the world's underwater cables.[34**] One of the more recent Chinese-owned projects, part owned and built by Huawei, is the Peace Cable, which will travel undersea from China around the Horn of Africa and terminate in France, providing faster service for Chinese companies doing business in Europe and Africa. Although Google and Facebook do not plan to use the Peace Cable, as they have sufficient network capacity, the installation of the cable has signaled potential security risks, particularly because Huawei will supply the equipment for the Peace Cable landing stations and its underwater transmission gear.[35]

Maintaining the Integrity of a Rapidly Expanding UCI Landscape

The U.S. Senate Permanent Subcommittee on Investigations or "Subcommittee" has warned that Chinese companies subject to the influence and control of the Chinese government have established relationships with major U.S. commercial companies, including AT&T, Verizon, and Lumen Technologies (previously known as CenturyLink).[36,37] To address security concerns and protect against potential anticompetitive behavior by a carrier with market power in a foreign country, the Subcommittee recommended in 2020 that the Federal Communications Commission (FCC) establish a clearer standard and process for a foreign carrier's authorization. This was motivated in part because the prevailing requirements, FCC's

[§] The Chinese government's global infrastructure development strategy to invest in nearly 70 countries.
[**] The other companies include U.S.-based SubCom, Finnish-owned Alcatel Submarine Networks, and Japan's NEC Corp.

Section 214 application, was lengthy and protracted.[††] The Subcommittee also recommended a periodic review and renewal of foreign carrier's authorizations to provide international telecommunications services.[38] On April 4, 2020, Executive Order 13913 established "Team Telecom,"[‡‡] an interagency team responsible for making permitting recommendations to the FCC. One early recommendation was to partially deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the U.S., citing national security concerns.[39]

To further fine-tune and accelerate the permitting process, rules promulgated since the Executive Order of 2020 now clarify when and how the "Team Telecom" process will apply, set timeframes for review, and facilitate the submission of more information and certifications at the beginning of the process. Applicants must provide specific information—including corporate structure and shareholder information; relationships with foreign entities; financial condition; legal and regulatory compliance; and business and operational information, including network infrastructure. A foreign owner of 10 percent or more of the licensee will automatically trigger Team Telecom review, as will applications to assign, transfer, control, or modify licenses.[40] Team Telecom can also review—and potentially recommend revocation of—existing FCC authorizations.[41]

Team Telecom – United States' Oversight of Foreign Telecommunication Interests

A federal government interagency committee, Team Telecom's primary objective is to provide permitting oversight and assist the FCC in its review of foreign participation in the U.S. telecommunications services sector and to identify national security and law enforcement concerns. The Committee, which includes voting members DHS, DOD, and DOJ, reviews applications and licenses and responds to any risks by recommending to the FCC that it dismiss, deny, or grant an application or license. It may also grant an application or license conditionally upon compliance with mitigation measures.

UCI Threats

"A successful attack on the UK's undersea cable infrastructure would be an existential threat to our security. Yet the exact locations of these cables are both isolated and publicly available – jugulars of the world economy which are a singularly attractive target for our enemies."

— Rishi Sunak
Member of Parliament United Kingdom[42]

[††] In some cases, Team Telecom's review and recommendation process to the FCC took several years. In May 2019, for instance, it denied China Mobile USA's international Section 214 application following an eight-year review period which involved extensive consultation with the intelligence community—marking the first instance in which Team Telecom denied a Section 214 application based on national security concerns. ("FCC Streamlining & Formalizing Team Telecom," National Law Review, October 20, 2020.)

[‡‡] Despite Team Telecom's formal name, established in subsequent guidance as the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector, the committee is still referred to as Team Telecom.

In addition to transparency and ownership concerns, UCI is subject to a spectrum of natural, accidental, and malicious threats (see Figure 4).

Threats from natural forces include earthquakes and plate tectonic movement, as well as human activity from trawling, dredging, and anchors. Another natural risk to UCI landing station sites is from the global impacts of climate change and rising seas, with encroachment at approximately one-eighth of an inch per year.[43,44]

Fortunately, cable operators often have excess network capacity. By automatically rerouting global information traffic via excess network capacity, or "dark fiber" that can be illuminated, operators can quickly respond to customer demand. Meanwhile, operators can direct cable repair ships to locate and

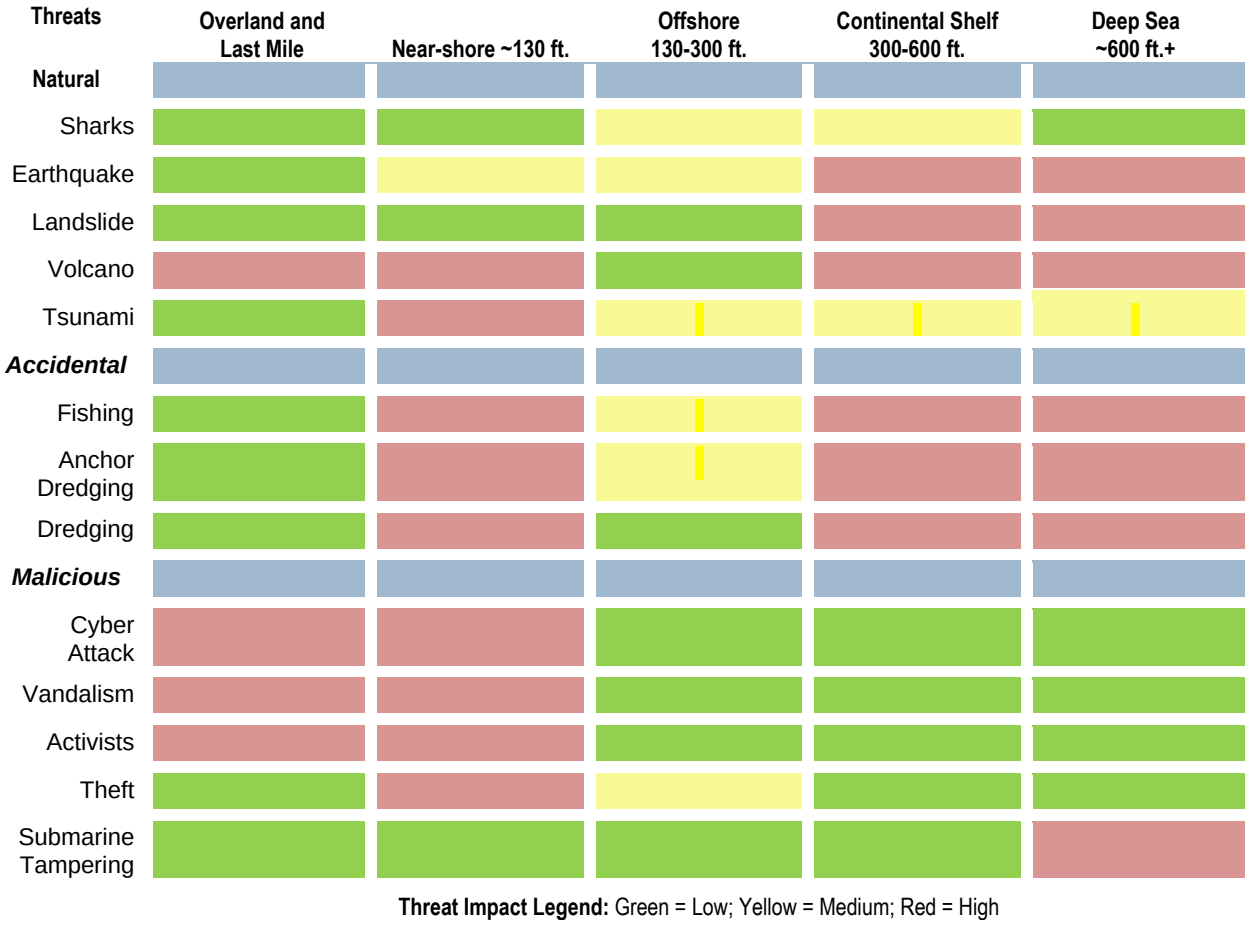

Figure 4: UCI Threats. *Source: Adapted from The Public-Private Analytic Exchange Program (AEP), sponsored by the Department of Homeland Security's Office of Intelligence and Analysis (DHS/I&A), on behalf of the Office of the Director of National Intelligence (ODNI). Colors indicate UCI threats, which vary depending upon depth and location (https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf, September 2017).*

repair a break with the help of submarine robotics or remotely operated vehicles (ROVs).[45§§] On a longer-term basis, many operators plan alternate subsea routes to offer paths for improved resiliency.

On the customer side, many use a "safety in numbers" approach, spreading their networks' capacity over multiple cables and often across diverse routes so that if one goes down, their network will run smoothly over other cables while service is restored to the damaged cable.

Undersea Data Security

Data security is a challenge for undersea cables due to the risk of a data release to malicious actor(s) or loss of functionality which creates national security and privacy risks. Areas of concern include data infiltration, exfiltration, malware, data corruption, timing, tapping/eavesdropping, denial of service, metadata analysis, fiber jamming, spoofing, and crypto. Current protections include software and hardware mitigations, monitoring, tamper detection and alerting, key management, network operations center monitoring, and intrusion detection systems (IDS) and intrusion prevention systems (IPS) analysis.

Malicious threats are generally at the last mile where infrastructure is accessible for data exfiltration, espionage, and sabotage.[46,47,48] However, cable tampering and sabotage are occurring at great depths and outside of territorial waters where countries often patrol and have legal protections. For example, the Russian "research" vessel known as the *Yantar* acts as the mothership to minisubs. It is quite feasible that a minisub armed with hydraulic cutters can cut through submarine cables.[49] Figure 4 (last row) was adapted to reflect the threat from subsea cable tampering and sabotage. The U.S. Navy has observed suspicious activity from Russian vessels along several undersea cable routes. It is difficult to confirm deep-sea sabotage of cables, compared to natural or accidental faults which are widely observed and reported. Regardless, this threat appears to be increasing as the former head of the Royal Navy warned of a "phenomenal increase in Russian submarine and underwater activity."[50]

Given the diversity of natural and accidental threats and the looming threats from malicious actors, physical security protections will become a priority for access control policies, monitoring (patrols), repair, power backups (batteries), redundant connections, adherence to quality/design standards, and supply chain risk management. Cybersecurity protections will also become more imperative in network operations center monitoring, tamper detection/alerting, and encryption.

Maritime Law, UCI Policies, and Regulatory Oversight

Numerous U.S. and international policies address legal and regulatory oversight for physical and cyber communications infrastructure (see Figure 5 for legal maritime territorial zones); however, they may not fully address the scale of the UCI threat. Although UCI policy was initially focused on ensuring fair competition, more recent attention has focused on policies which address national security concerns related to foreign UCI ownership and related concerns over unauthorized access and control. Governments and commercial UCI providers are increasingly aware of hacking and intelligence gathering conducted through submarine cables, and think tank studies and media coverage on communications infrastructure security are now examining how a complex and evolving patchwork

§§ Coherent Optical Time Delay Refractometers (COTDRs) are used for searching for submarine cable faults or to detect tapping of cables. The method involves detecting signal disruption to fibers by sending test pulses to measure backscattering through the repeaters. This option is proven and effective, but requires available fiber capacity, as a dedicated fiber for each direction is used for fault detection.

of data privacy laws could be just one more lever to discourage unauthorized submarine cable data exfiltration. As this policy landscape shifts, evolving international norms may have greater potential to reduce hacking.

Maritime Zones

The United States Coast Pilot®, published by NOAA, is intended to be used as a supplement to NOAA nautical charts and describes the offshore extent of maritime zones (see Figure 5). Submarine cables can cross any of the maritime zones listed below, and according to the Coast Pilot, the cables may not be charted. For inshore areas, cables are buried beneath the seabed; for outer maritime zones, the cables often lie on the ocean floor.[51] Maritime zones recognized under international law include:

- **Territorial waters.** Each coastal state has the jurisdictional authority to implement cable hacking laws. It is largely up to each coastal state to enforce these regulations to punish both domestic and foreign violators.

- **EEZ and continental shelf up to 200 miles.** Coastal states' regulations in the EEZ do not apply to foreign nationals who intentionally damage cables. In other words, in hacking instances, "this would mean coastal states could only address domestic hackers, which, while potentially useful for private actors, does not likely apply to the majority of hacking incidents, which are largely committed by foreign governments."[52] U.S. policymakers should encourage UNCLOS to reconsider its cable protections for EEZs.

- **High seas or international waters.** Although most challenges with undersea cables occur closer to shore, international maritime law does not extend regulations for the protection of

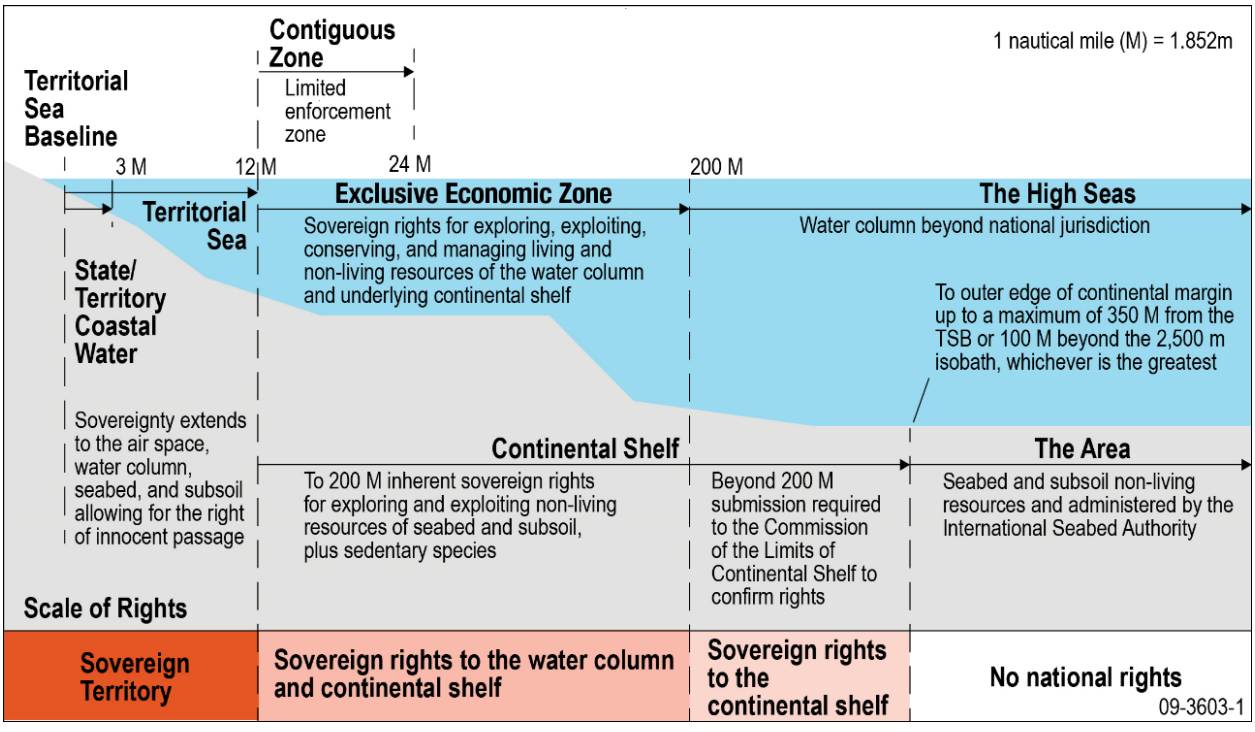

Figure 5: Maritime zones and rights under the 1982 United Nations Convention on the Law of the Sea (UNCLOS).
Source: Reproduced from the United States Coast Pilot, published by the National Oceanic and Atmospheric Administration (NOAA).

submarine cables outside territorial seas, including cyber threats or threats from unmanned and autonomous systems, and it has no authority to identify a hacker. Beyond the scope of this paper is a complex array of international laws that might provide some data protection and legal recourse. A recent paper in the *Chicago Journal of International Law* suggests that states can pursue two options:

1. Establish liability through an intergovernmental organization known as International Tribunal for the Law of the Sea (ITLOS), which was established by UNCLOS, for damage to cables.

2. Seek legal recourse for international right to privacy violations.

State actors should continue to monitor legal options as norms and conventions for addressing hacking and submarine cables continue to develop.[53]

"Few places on the planet are as lawless as the high seas, where egregious crimes are routinely committed with impunity."[54]

UCI Policies, Regulations, and Evolving Norms

A number of other U.S. government agencies with oversight for homeland security, telecommunications, the space and satellite sector, and cybersecurity have established guidance, regulations, and standards that can help manage risk to UCI. Figure 6 illustrates the value chain of UCI infrastructure. Appendix C, "U.S. Government Regulatory Oversight and Partner Information Sharing and Risk Assessments," describes this environment in more detail.

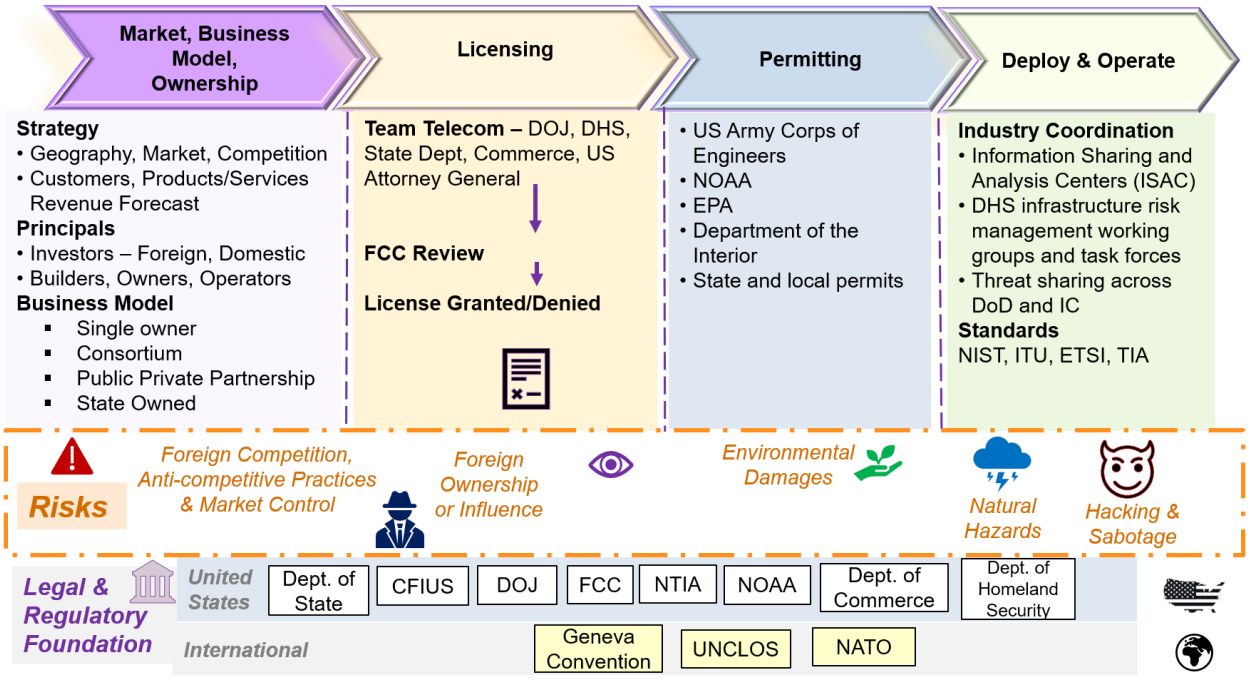

Figure 6: UCI infrastructure value chain with associated risks and regulatory foundation.

Interagency and industry partner coordination across the UCI value chain will be critical for the protection of communications infrastructure that spans satellites, undersea cables, landing stations, data centers, and their supply chains. Historically, UCI regulations were addressed by two statutes that vest authority and requirements in licensing:

- **Cable Landing License Act of 1921.** Provides FCC the authority to authorize cable landing licenses, including the ability to grant, withhold, revoke, or condition cable landing licenses if it determines "that such action[s] will assist in securing rights for the landing or operation of cables in foreign countries, or in maintaining the rights or interests of the United States…or will promote the security of the U.S."[55]

- **Communications Act of 1934: Section 214.** Requires telecom carriers to obtain authorization from the FCC before engaging in international telecom services. FCC must consider whether telecom service providers will serve the "public interest, convenience and necessity." The international Section 214 process ensures that the U.S. market is protected against potential anticompetitive behavior by a carrier with market power in a foreign country.[56]

Subsequently, a range of laws, orders, and principles have been established to provide further oversight and structure to address UCI risks related to foreign control of UCI, criminalizing damage to cables, and establishing nonbinding guidance and exercises to enhance protective practices:

- **United Nations Convention on the Law of the Sea (UNCLOS).** Provides for the freedom to lay cables and pipelines in international waters, and requires that UCI companies possess permits, licenses, and environmental agreements according to local laws and international treaties. While UNCLOS focuses on Exclusive Economic Zones (EEZ) to require states to enact domestic legislation penalizing damage to cables by ships or persons subject to their jurisdiction,[57,58,59] it does not extend regulations for the protection of submarine cables outside territorial sea, including from cyber threats or threats from unmanned and autonomous systems, and it has no authority to identify a hacker.[***]

- **Executive Order 10530.[†††] Providing for the Performance of Certain Functions Vested in or Subject to the Approval of the President** – Takes steps beyond the *Communications Act of 1934* to assess foreign control of communications infrastructure. Provides FCC the authority to work with the Secretary of State and other agencies before granting or revoking a communications infrastructure license, which includes assessment of foreign inclusion or ownership of cables that end in the U.S.[60]

NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). CCDCOE publishes the Tallinn Manual, which establishes principles for how cables should be managed in the same fashion as cyber infrastructure on land. CCDOE

[***] "UNCLOS establishes rules governing uses of the oceans and seas and their resources. Specific to submarine cables, UNCLOS Article 113 requires every State to adopt laws and regulations making it a punishable offense for ships or persons subject to its jurisdiction to break or injure a submarine cable beneath the high seas, either willfully or through culpable negligence. UNCLOS Article 114 requires every State to adopt laws and regulations to provide for reimbursement of persons whose cable is broken or injured by someone subject to that State's jurisdiction. The United States is not a party to UNCLOS." From "Submarine Cables – International Framework," NOAA Office of General Counsel, updated March 1, 2019.

[†††] Exec. Order No. 10530 § 5(a), 19 Fed. Reg. 2709 (May 10, 1954).

also conducts cyber exercises through its annual *Locked Shields* experiment, which in 2020 extended beyond terrestrial communications to include space infrastructure as part of the broader communications network.[61,62‡‡‡] As critical infrastructure resilience is increasingly a priority of government and industry partnerships, it is both practical and logical to include UCI as part of CCDCOE future exercises.

- **Organisation for Economic Cooperation and Development (OECD).** *OECD* publishes the Oslo Manual and other internationally agreed guidelines and proposals for the collection, reporting, and use of data indicators on science, technology, and innovation (STI)**,** including rules for applying the law of neutrality in cyberspace.

Securing Space Infrastructure

Legislation to secure space infrastructure, *The Space Infrastructure Act* (June 2021), would direct the Secretary of Homeland Security to designate space systems, services, and technology as critical infrastructure. The House bill, sponsored by Congressman Ted W. Lieu (D-Los Angeles County) and Congressman Ken Calvert (R-CA) was introduced to strengthen efforts to secure space-based assets, particularly as "…recent hacking incidents [have] underscore[d] that we have to be forward-thinking about how to safeguard critical infrastructure… The collaboration between federal security agencies and industry partners directly and indirectly involved with space-based assets and technologies is essential to America's future as we confront evolving threats."[63]

Emerging Satellite Architectures as an Operational Risk Hedge

Emerging satellite architectures could, over time, begin to offer fiber-like capacity and throughput to provide increased resilience and redundancy. For example, although today's orbiting satellites communicate by radio frequency (RF) electromagnetic waves, new proliferated low Earth orbit (pLEO) operators realize the potential of free space optical communications. Elon Musk, CEO of SpaceX, for instance tweeted in January 2021 that "all sats launched next year will have laser links."[64] Starlink has already equipped and launched some of their satellites with optical inter-satellite links (OISL). In addition to Starlink, OneWeb (UK) and Telesat (Canada) LEO constellations are looking at future OISL implementations.

Commercial companies are not the only ones focusing on OISL. The Space Development Agency (SDA) plans to leverage space-based laser optics not only for the high data throughput rates but also for security. Specifically, narrow optical beams are more difficult to intercept than RF links. SDA plans to build a "transport layer" as a mesh network of communications/data relay satellites. Derek Tournear, SDA Director, noted that this mesh network or "transport layer" of satellites will have "something on the order of three to five optical cross links per satellite." Tournear also added that the cross links will "not only be satellite-to-satellite, but satellite-to-air, satellite-to-ground and satellite-to-maritime assets."[65]

From a risk management standpoint, according to Frank Rose of the Brookings Institution, "We

‡‡‡ The Aerospace Corporation provided threat scenarios on behalf of the Space Information Sharing and Analysis Center (Space ISAC).

should not look at space, cyber, and undersea cables independently of one another, as these areas are becoming increasingly intertwined. If a determined adversary wants to cut off U.S. and allied access to communications infrastructure, they are likely to deploy capabilities to attack space, cyberspace, and undersea cables at the same time, in a coordinated manner, and across a broad spectrum of means. There is limited historical precedent for conflict in these domains, unlike conflict on the land or the sea. As a result, it is helpful to look at these vulnerabilities holistically to ensure our responses are coordinated."[66]

Mesh Networks Provide Greater Resilience

Traditional communications infrastructure relies upon centralized systems (such as fiber optic backbones, cell towers, and satellite "bent-pipe" architecture) where the satellite primarily operates to retransmit the signals back to Earth. By contrast, mesh networking involves peer-to-peer communication between multiple "nodes" instead of relying on a centralized and potentially vulnerable node. Modern mesh optical or radio networks also use algorithms which allow the network to constantly reconfigure itself to provide the fastest path to the destination and self-heal in the event of failure. Mesh networks support traffic at different quality of service (QoS) levels, bandwidth, and data rate requirements.

Key Questions to Ensure Network Capabilities, Security, and Resilience

Short-term, critical programs and missions should strive to achieve some level of platform diversity to address UCI failure events. As satellite and airborne networks begin to offer new long-haul data transport options, government and private sector communications owners and operators should ask:

- **Capacity**. Under what circumstances are satellites capable of offering acceptable throughput (e.g., Gigabits per second) as a feasible option to ensure additional capacity? How much backup capacity could satellites provide?

- **Availability**. Is the satellite network always on? Always connected? Where are the coverage gaps?

- **Latency**. How does a satellite network compare with today's fiber networks in terms of the delay between start and end point or latency? And how critical is latency as a factor for specific communications applications?[§§§]

- **Security and Resiliency.** What physical and cyber vulnerabilities and threats would lead to heightened risk through greater use of satellites? Are there hardening protocols and practices in place? During failure events, what is the plan to reduce recovery time and means to support degraded operations?

- **Emerging Satellite Networks.** As telecommunications firms, like Verizon, ink deals with commercial satellite companies, like Kuiper, to leverage low Earth orbit mesh networks for connectivity[67] how might this begin to divert data traffic to satellite constellations? What are the market implications? National security implications?

- **Connectivity Markets.** As non-state commercial actors continue to increase their stakes in UCI, what are the business, policy, and technological advantages of the winners and losers? And how can policymakers ensure an even playing field for U.S. commercial actors?

[§§§] For example, autonomous car applications and electronic trading may require minimal delay while other applications can tolerate longer delays without any noticeable disadvantage.

Conclusion

Fiberoptic submarine cables are a relatively recent technology development. After 30 years of evolution and growth, data connectivity and UCI have become critical to our economy, society, and national security. As a result, geopolitical interests will be reflected in the competition for control of the undersea cable market. With future efforts to secure UCI and enhance resiliency, the United States government should work toward:

- "Whole of network" transparency and security to improve situational awareness across the communications enterprise — to include undersea, terrestrial, air, and satellite segments.
- Forecasting and planning for emerging technologies and architectures.

As network operators and commercial and government stakeholders plan and hedge risks for future connectivity, the following recommendations should be considered.

Continue Efforts to Improve Transparency and Security

Legal and regulatory frameworks combined with key institutions are focused on protecting UCI from unfair competition, hostile foreign influences, hacking and data exfiltration, and damages from unintentional natural forces. Government and industry should continue to secure the communications enterprise—including undersea, terrestrial, air, and satellite segments. Additionally, organizations such as Team Telecom should continue to improve ownership and investment transparency by incorporating routine and proactive monitoring of permits and licenses. Given expanding UCI routes and increasing commercial activity, the U.S. government should ensure sufficient resources to monitor, respond, and enforce National Security Agreements pursuant to CFIUS and Team Telecom findings.[68] Moving toward increased regulatory agility and predictability will allow commercial UCI players to better manage their significant investment risks.

Beyond U.S. shores and territorial waters, it is difficult to prevent bad actors from taking advantage of gaping holes in ocean governance to hack or damage cables. Realistically instituting legal protections in international waters is complicated as governments from one country may not recognize the legal authority of another. A U.S. State Department official noted that broad, inclusive multilateral processes may have the best chance of being adopted by those whose behavior we seek to influence. In the meantime, it is perhaps more productive to work with allies and partners, bilaterally or multilaterally, to provide best practices to secure facilities and enhance resilience, and to share information as appropriate on specific threats.

Keep an Eye to Emerging and Future Technologies and Architectures

Industry and government can now build upon their existing institutional and regulatory frameworks to ensure that the global data commons offer alternate pathways. Strategic diversification of technology investments across connectivity platforms can "future proof" our nation's long-haul international data connectivity infrastructure. This includes the adoption of new and hybrid network architectures across space, airborne, terrestrial, and maritime platforms.

Although UCI will continue to offer unrivaled backbone capacity for years to come, space-based solutions, such as existing HTS GEO satellites and future LEO constellations with inter-satellite laser link mesh networks, will offer alternate secure data paths. The world of long-haul global communications continues to evolve and

policymakers must stay ahead of the game to ensure that the U.S. and its allies are well-positioned across a range of global communication pathways, undersea and space, to offer overall network and operational reliability and resilience.

Acknowledgments

The authors would like to thank Richard Grubb, Department of State; Frank Rose, Brookings Institution; David Feith, Center for North American Security (CNAS); Tim Stronge, TeleGeography; Dr. Megan Ammirati, TextOre Inc. and the National Security Institute (NSI); and Joseph Touch, Ramin Sadr, Robert Schoenberg, and John Mills of The Aerospace Corporation for their insight. We are also grateful for colleague reviews by Mick Gleason, David Eccles, and Angie Bukley as well as helpful edits by Mary Mills.

Appendix A.
Undersea Cable Faults, Disruptions, and Internet Blackouts

Many undersea cables in use today were built in the early 2000s, and with a 25-year life, many are aging beyond their useful life. There is a continuing effort to "refresh and replace the cables," which also provides the ability to increase capacity. For example, although optical cable technology once only accommodated four to eight fiber pairs in each cable, there are now 20 pairs per cable,[69] which will allow operators to have a massive amount of capacity on the cables and at reduced cost per bit.

It is preferable to have redundant cables for backup. Lack of back up infrastructure can result in reduced or disrupted service availability through single point failures. Unfortunately, internet blackouts due to undersea cable faults are not uncommon (see examples below) and the impact can be tremendous. Yet it is important to note that most undersea cables are built and owned by private companies; the security and repair of undersea cables remains, for the most part, a commercial responsibility.

Current reports of cable faults and repairs are listed on the Submarine Telcoms Forums website at https://subtelforum.com/. A few examples are noted below:

- **2008 – Middle East and India.** Up to 75 million people left with very limited internet access for days. Cause: Ship mooring accident due to bad weather.[70]
- **2011 – Japan.** At least eight submarine cables were disabled. Cause: 8.9 magnitude earthquake, aftershocks severed four cables and tsunamis damaged four more landing stations.[71]
- **2019 - Tonga**. This small island nation depended upon a single cable which experienced a fault reverting it to satellite backup (Satellite Kacific) and creating significant disruption, plunging its 170 islands and 100,000 residents into digital darkness, knocking out overseas phone calls and hampering money transfers and airline bookings. Cause: Unknown, suspect a boat anchor severed the cable.
- **2020 – Yemen.** 20 million citizens were without internet for almost one week due to a break in a subsea cable in the Red Sea. Neighboring countries including Kuwait, Saudi Arabi, Sudan, and Ethiopia all suffered partial outages. Cause: Suspected sabotage.[72]
- **2022 – Svalbard**. Space Norway located a disruption where the seabed goes from 300 meters down to 2700 meters in the Greenland Sea. Cause: Suspected sabotage.[73]
- **2022 – Tonga.** The entire population of Tonga was impacted by a cable fault; scientists estimated it would take weeks to restore internet connection. Cause: Underwater volcano.

Appendix B.
Connectivity Platforms: Strengths, Weaknesses, and Market Maturity.

Includes Geostationary (GEO), high throughput satellite (HTS) GEO, low Earth orbit (LEO) mega-constellations, and high-altitude platforms (HAPS). These communication platforms vary in terms of coverage, capacity, availability, latency, expected lifetime and are in various lifecycle stages ranging from research and development (R&D), demonstration or "demo," high growth, and mature.

Platform	Advantages/Disadvantages
Traditional GEO ◆ Operational since 1964 ◆ Market Phase: Mature ◆ Lifetime: 15–20 years	***Advantages:*** Broad coverage (~42% of the Earth's surface). Ground station tracking is not required. Fewer satellites are needed than in LEO or MEO to cover entire Earth. Strong heritage. Life expectancy can exceed 20 years. ***Disadvantages:*** Bigger and expensive to build and launch. Due to line of sight limitations, a GEO satellite cannot reach above 81 degrees latitude north or south. Due to its high altitude, a GEO satellite experiences relatively high signal latency. High CAPEX GEOs are expensive to build and launch. Current capacities are limited due to use of RF.
HTS GEO ◆ Operational since 2004 ◆ 31 satellites available today ◆ Market Phase: Mature ◆ Lifetime: 15–20 years	***Advantages:*** Significant increase in capacity is achieved by a high-level frequency reuse and spot beam technology. Provides more throughput than a classic fixed GEO satellite for the same amount of allocated orbital spectrum. Despite higher costs associated with spot beam technology, the overall cost per circuit is considerably lower compared to shaped beam. ***Disadvantages:*** Same as GEOs (see above).
LEO Mega-Constellations – Global Broadband ◆ Market Phase: High Growth ◆ Lifetime: 3–10 years	***Advantages***: Smaller and less expensive rockets needed to place into orbit. Multiple nodes in a mesh network enhances resiliency. Compared to MEO or GEO, has the lowest latency. ***Disadvantages:*** Many LEOs are needed to cover even a limited a geographical area. Network complexity requires many ground stations. Need different frequencies or optical inks (see below) to avoid interfering with each other's communication. High OPEX due to satellite replacement, typically every 5 years. ***Note:*** SpaceX Starlink has 1,468 satellites in orbit; Amazon Project Kuiper received FCC approval for 3,236 satellites; OneWeb has 394 satellites in orbit. Both Starlink and OneWeb started service during 2021.
High Altitude Platforms (HAPS) ◆ Market Phase: Demo ◆ Lifetime: Up to one year	***Advantages:*** Could provide cellular connectivity to remote areas where a traditional mobile network would be too difficult and costly. Could work with unmodified cellular devices as a last mile connection. Lower latency than LEO satellites. ***Disadvantages:*** Large mesh radio networks have not been deployed with global coverage across continents. Frequent replacements increase lifetime system costs. Many countries will apply additional regulatory scrutiny to address security and radio frequency interference concerns. ***Note:*** After more than a decade of research, in January 2021, Alphabet shut down *Google Loon* due to unsustainable costs.
Satellite with Optical Links ◆ Market Phase: R&D ◆ Active DOD/DARPA program in ISLL between GEO and LEO constellations	***Advantages:*** Linking LEO satellites with optical inter-satellite laser links (OISLs) will lower latency and reduce need for terrestrial ground stations. ***Disadvantages:*** Cost and complexity may preclude some companies from investment in OISLs, including OneWeb. Also, clouds and precipitation can block optical signals for space to ground links (not applicable for OISL constellations with RF ground links, though they have limited ground bandwidth). ***Note:*** SpaceX and Amazon Kuiper and Telesat are pursuing OISL technology and the future may see OISLs between LEO, MEO, and GEO sats.

Appendix C.
U.S. Government Regulatory Oversight and Partner Information Sharing and Risk Assessments

U.S. Government

- **Federal Communications Commission (FCC).** Per Executive Order No. 10530, the FCC regulates interstate and international communications, conducts investigations, and can require companies to file legal responses and provide a listing of their subscribers for domestic and international services.

- **Department of Commerce**

  - **National Telecommunications and Information Administration (NTIA).** NTIA can make requests to the FCC to revoke *Section 214* authorizations that may pose unacceptable national security and law enforcement risks related to malicious cyber activities and a company's failure to comply with cybersecurity and privacy laws.

  - **National Institute of Standards and Technology (NIST).** NIST supports U.S. competitiveness in communications technology and cybersecurity by developing new tools to measure critical attributes, providing authoritative data, and bringing stakeholders together to find the way forward.

  - **National Oceanic and Atmospheric Administration (NOAA).** NOAA regulates whether and how proposed submarine cables may be installed in National Marine Sanctuaries in accordance with international agreements to which the U.S. is a party and generally accepted principles of international law.

  - **Bureau of Industry and Security (BIS).** The Export Administration Regulations (EAR) contain a list of foreign businesses, research institutions, government and private organizations, individuals, and others subject to license requirements for the export, re-export, and/or transfer (in-country) of specified items. These persons comprise the Entity List, which is within the EAR.

- **Department of State.** The department works with allied partners to address UCI and discourage allies from collaborating with untrusted firms across the digital economy. David Feith, of the Indo-Pacific Security Program at the Center for North American Security (CNAS) and former U.S. State Department official, noted that clean network standards "can provide a solid foundation" for improved accountability and can help investors better understand risk prior to investment and hold operators responsible throughout the life of the cable.[74]

- **Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA).** CISA is the designated lead risk management agency responsible for coordinating efforts to help protect and improve the security and resilience of the communications sector, which includes broadcast, cable, satellite, wireless, and wireline services as National Critical Functions (NCF). CISA is responsible for development of the *Communications Sector-Specific Plan* (CSSP) that is designed to guide the sector's voluntary, collaborative efforts to advance a national unity

of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure relative to Presidential Policy Directive 21 *Critical Infrastructure Security and Resilience*. As part of its partnership and information sharing mission, CISA's activities bridge the government and private sector in multiple forums including:

- **Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force**. The Task Force works to develop common frameworks for the bidirectional sharing of threat information between government and industry, and to identify processes and criteria for threat-based evaluation of ICT products and services, among other ICT-related guidance.[75]

- **Cross-Sector Space Systems Critical Infrastructure Working Group.** This group (with members representing communications, defense industrial base, IT, and space asset infrastructure sectors) makes recommendations to manage risk to space-based assets and national critical functions.[76]

- **Committee on Foreign Investment in the United States (CFIUS).** An interagency committee that reviews and evaluates the national security implications of foreign investments in U.S. companies or operations. CFIUS determines if a transaction could pose a risk to national security and can recommend to the president to block or unwind the investment. The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) strengthened and modernized CFIUS to address national security concerns arising from noncontrolling investments—an ownership position wherein a shareholder owns less than 50 percent of outstanding shares and has no control over decisions—involving foreign persons. Covered investments include critical technologies, critical infrastructure (including telecommunications), and sensitive personal data.[77]

- **U.S. Department of Defense (DOD).** The DOD is a significant user and customer of commercial communications infrastructure, including combatant commands responsible for specific defense communications domains (*USSTRATCOM*, *USSPACECOM*, and *CYBERCOM)*. The U.S. Army Corps of Engineers can regulate artificial islands, installations, and "devices" (which can include cables) on the seabed of the U.S.' outer continental shelf. Additionally, the U.S. Navy could potentially recapitalize deep undersea capabilities to match the swift growth of Chinese and Russian deep undersea capabilities.

- **Intelligence Agencies**. Collect and analyze information in support of law enforcement and national security; protect against terrorist and foreign intelligence; and protect cyberspace and critical infrastructure.

Nonprofit and Other Partners

- **International Cable Protection Committee (ICPC).** The ICPC works to improve the security of undersea cables through elevating awareness of submarine cables as critical infrastructure; establishing international recommendations for cable installation, protection, and maintenance; monitoring the evolution of international treaties and national legislation; and liaising with United Nations bodies.

  Information Sharing and Analysis Centers (ISAC). As coordinating bodies designed to maximize information flow across private sector critical infrastructures and with government, the Space ISAC and Communications ISAC have

the opportunity to examine the communications enterprise described in this paper, which includes satellites, undersea cables, landing stations, data centers, and their supply chains. This would facilitate a shared understanding of data connectivity security concerns and enhance mitigation opportunities.

- **International Telecommunications Union.** Facilitates international connectivity in communications networks, allocates global radio spectrum and satellite orbits, develops standards to ensure networks and technologies interconnect, and improves access to ICTs to underserved communities.

- **European Telecommunications Standards Institute (ETSI).** Standards body for telecommunications, broadcasting, and other electronic communications networks and services.

- **Telecommunications Industry Association (TIA)** and **Alliance for Telecommunications Industry Solutions (ATIS)**. TIA develops U.S. national standards for the equipment that connects to the telecommunications network and ATIS develops U.S. national telecommunications standards for the network to which the equipment attaches. Work from both these organizations is passed via the U.S. State Department to the ITU where worldwide telecommunications standards are defined.

References

[1] Rishi Sunak, "Undersea Cables Indispensable, Insecure," Policy Exchange, 2017. (https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/).

[2] Justin Sherman, "Cyber defense across the ocean floor: The geopolitics of submarine cable security," Atlantic Council, September 13, 2021. (https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/#primer).

[3] United Nations Environment Program World Conservation Monitoring Centre (UNEP-WCMC) International Cable Protection Committee, "Submarine Cables and the Oceans: Connecting the World," 2009. (https://www.unep-wcmc.org/system/dataset_file_fields/files/000/000/118/original/ICPC_UNEP_Cables.pdf?1398680911).

[4] Chris Frakes, "CHIPS," Modern Treasury. (https://www.moderntreasury.com/learn/chips).

[5] Klint Finley, "How Google Is Cramming More Data Into Its New Atlantic Cable," Wired, April 15, 2019. (https://www.wired.com/story/google-cramming-more-data-new-atlantic-cable/).

[6] Statement of the U.S. Chamber of Commerce at a Hearing on the United Nations Law of the Sea Convention, US Chamber of Commerce, 2012. (https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf).

[7] Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors," (www.cisa.gov/critical-infrastructure-sectors).

[8] Ian Clarke, "Smart Submarine Infrastructure - The Future of Global Connectivity," Capacity Media, May 28, 2021.

[9] Mark Haranas, "Microsoft's Underwater Data Center A Success; Azure Ahead," CRN.com, September 22, 2020.

[10] Aizaz Chaudhy and Halim Yanikomeroglu, "Optical Wireless Satellite Networks versus Optical Fiber Terrestrial Networks: The Latency Perspective," Arxiv, June 14, 2021. (Optical Wireless Satellite Networks versus Optical Fiber Terrestrial Networks: The Latency Perspective (arxiv.org).

[11] Jason Rainbow, "Verizon announces intent to use Amazon's planned Project Kuiper constellation," Space News, October 26, 2021.

[12] Barton Crockett, "Fiber Takes the Lead Over Satellite in Int'l Digital Nets," *International Networks,* July 1, 1991.

[13] Richard Aldrich and Athina Karatzogianni, "Postdigital War Beneath the Sea? The Stack's underwater cable Insecurity. Digital War," *Springer Nature Limited*, 2020. (https://doi.org/10.1057/s42984-020-00014-x).

[14] Internet World Stats: Usage and Population Statistics, (www.internetworldstats.com)

[15] Submarine Cable Map 2020, *TeleGeography*, January 27, 2021. (https://submarine-cable-map-2020.telegeography.com/).

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

[17] "Telecom Namibia and Paratus announce major public private partnership to connect Namibia to Google's New Undersea Cable", *Extensia*, February 17, 2021. (https://extensia-ltd.com/2021/02/17/telecom-namibia-and-paratus-announce-major-public-private-partnership-to-connect-namibia-to-googles-new-undersea-cable/).

[18] "Cisco Annual Internet Report (2018–2023)," *Cisco*, March 9, 2020. (https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html).

[19] "Internet usage in BRIC," *Statista*, April 29, 2021. (https://www.statista.com/topics/3116/internet-usage-in-bric/).

[20] "How Google is building its huge subsea cable infrastructure," *VentureBeat*, April 24, 2019. (https://venturebeat.com/2019/04/24/how-google-is-building-its-huge-subsea-cable-infrastructure/).

[21] Thomas Seal, "The Undersea Cable Market Is Booming Again, This Time Funded by Big Tech," *Bloomberg BusinessWeek*, March 14, 2019. (https://www.bloomberg.com/news/articles/2019-03-14/undersea-cables-are-no-longer-underwater-as-fiber- booms-again).

[22] Solana Larsen, ed., "The New Investors in Underwater Sea Cables," *Mozilla Internet Health Report*, April 2019. (https://internethealthreport.org/2019/the-new-investors-in-underwater-sea-cables/).

[23] Helen Martin, "Undersea Espionage: Who Owns Underwater Internet Cables?" *The McGill International Review,* Sep 29, 2019. (https://www.mironline.ca/undersea-espionage-ownership-of-underwater-internet-cables/).

[24] "How Google is building its huge subsea cable infrastructure," *VentureBeat,* April 24, 2019.

(https://venturebeat.com/2019/04/24/how-google-is-building-its-huge-subsea-cable-infrastructure/).

[25] Interview with Facebook investment team executive, January 21, 2022.

[26] Alan Maudlin, "A Complete List of Content Providers' Submarine Cable Holdings," *TeleGeography Blog* at *Telegeography.com*, November 2017.

[27] Tage Kene-Okafor, "Facebook-backed 2Africa set to be the longest subsea cable upon completion,' *Tech Crunch*, September 29, 2021.

[28] Michael Thompson, "Facebook Building a 23,000-Mile Undersea Cable to Bring High Speed Internet to 23 Poorly Served Countries in Africa and the Middle East," *UK Daily Mail*, May 15, 2020. (https://www.dailymail.co.uk/sciencetech/article-8323973/Facebook- building-23-000-mile-undersea-cable-bring-internet-Africa-Middle-East.html).

[29] Sam Shead, "Google is Building a Huge Undersea Fiber-optic Cable to Connect the U.S. to Britain and Spain," *MSN*, July 27, 2020. (https:/www.msn.com/en-us/finance/other/google-is-building-a-huge-undersea-fiber-optic-cable-to-connect-the-us-to-britain-and-spain/ar-BB17gf8z).

[30] Sally Adee, "The Global Internet is Disintegrating – What Comes Next?," *BBC*, May 15, 2019. (http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-next).

[31] Sheridan Prasso, "China's Digital Silk Road is Looking More Like an Iron Curtain," *Bloomberg*, January 10, 2019. (https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain).

[32] Joshua Kurlantzick, "Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms?" *Council on Foreign Relations*, December 18, 2020.

[33] Abdi Latif Dahir, "These Are the African Countries Not Signed to China's Belt and Road Project," *Quartz Africa*, September 30, 2019. (https://qz.com/africa/1718826/the-african-countries-not-signed-to-chinas-belt-and-road-plan/).

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

[35]Helene Fouquet, "China's 7,500-Mile Undersea Cable to Europe Fuels Internet Feud," *Bloomberg Business Week*, March 5, 2021.

[36] Frank Jüris, "Handing Over Infrastructure for China's Strategic Objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic," *National Intelligence Law of the PRC, Ministry of Justice*, 2017. (http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf).

[37] Senators Rob Portman and Tom Carper, "Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers." *U.S. Senate Permanent Subcommittee on Investigations*, June 9, 2020. (https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf).

[38] Senators Rob Portman and Tom Carper, "Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers," *U.S. Senate Permanent Subcommittee on Investigations*, June 9, 2020. (https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf).

[39] "Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States," *Department of* Justice *Federal Communications Commission*, June 17, 2020. (https://www.justice.gov/opa/pr/teamtelecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-underseadirect).

[40] "FCC Formalizes Foreign Investment Review Process," *Covington & Burling LLP*, October 1, 2020. (https://www.cov.com/en/news-and-insights/insights/2020/10/fcc-formalizes-foreign-investment-review-process).

[41] "FCC Streamlining & Formalizing Team Telecom," N*ational Law Review*, October 20, 2020. (https://www.natlawreview.com/article/formalizing-team-telecom).

[42] Rishi Sunak, "Undersea Cables Indispensable, Insecure," *Policy Exchange*, 2007. (https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf).

[43] National Oceanic and Atmospheric Administration, , "Is the Sea Level Rising," *Ocean Facts.* (https://oceanservice.noaa.gov/facts/sealevel.html).

[44] Nitish Pahwa, "Biden and the Underseas Cable Underworld," *Slate*, December 28, 2020.

[45] Nicole Starosielski, "In our Wi-Fi World, the Internet Still Depends on Undersea Cables," *The Conversation*, January 25, 2019.

(https://theconversation.com/in-our-wi-fi-world-the-internet-still-depends-on-undersea-cables-49936).

[46] John Fritz, "Threats from Below: Undersea Fiber-Optic Cable Criticality," *Stable Seas, March 2019.* (https://www.stableseas.org/sites/default/files/fiber_optic_cables.pdf).

[47] Garrett Hinke, Cutting the Cord: The Legal Regime Protecting Undersea Cables," *Lawfare Blog,* November 2017. (https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables).

[48] H.I. Sutton, "How Russian Spy Submarines Can Interfere With Undersea Internet Cables." *Forbes,* August 19, 2020. (https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/?sh=41c93263b04a).

[49] David Wilkes, "How Putin could black out Britain: Top military man warns Russian sabotage could wreck undersea cables that supply our internet and $10 trillion of financial deals a day", January 10, 2022.

[50] PA Media, "UK military chief warns of Russian threat to vital undersea cables," January 8, 2022

[51] National Oceanic and Atmospheric Administration, *The United States Coast Pilot 2*, Chapter 1, November 28, 2021. (https://nauticalcharts.noaa.gov/publications/coast-pilot/files/cp2/CPB2_C01_WEB.pdf).

[52] Cybersecurity and Infrastructure Security Agency (CISA), "ICT SCRM Task Force." (https://www.cisa.gov/ict-scrm-task-force).

[53] Jason Petty, "How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea" *Chicago Journal of International Law,* Volume 22, Number 1, June 22, 2021.

[54] Ian Urbina, "Lawless Ocean", *New York Times,* July 19, 2019.

[55] 47 U.S.C. §§ 34-39

[56] Federal Communications Commission (FCC), "International Section 214." (https://www.fcc.gov/general/international-section-214).

[57] United Nations. United Nations Convention on the Law of the Sea of 10 December 1982. (http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf).

[58] Jeremy Page, Kate O'Keeffe, and Rob Taylor, "America's Undersea Battle With China For Control of the Global Internet Grid." *Wall Street Journal*, March 12, 2019. (https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466).

[59] Garrett Hinck, "Cutting the Cord: The Legal Regime Protecting Undersea Cables," *Lawfareblog,* November 21, 2017. (https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables).

[60] "Executive Branch Recommendation for a Partial Denial and Partial Grant of the Application for a Submarine Cable Landing License for the Pacific Light Cable Network (PLCN)," Federal Communications Commission, 2020. (https://licensing.fcc.gov/myibfs/download.do?attachment_key=2448548).

[61] "Tallinn Manual," NATO Cooperative Cyber Defence Centre of Excellence. (https://ccdcoe.org/research/tallinn-manual/).

[62] "Locked Shields," NATO Cooperative Cyber Defence Centre of Excellence. (https://ccdcoe.org/exercises/locked-shields/).

[63] Congressman Ted Lieu, "Representatives Lieu and Calvert Introduce Bill to Designate Space as Critical Infrastructure," June 4, 2021. (https://lieu.house.gov/media-center/press-releases/reps-lieu-and-calvert-introduce-bill-designate-space-critical).

[64] Rachel Jewett, "Latest Starlink Satellites Equipped with Laser Communications, Musk Confirms",*ViaSatellite,* January 25, 2021. (https://www.satellitetoday.com/broadband/2021/01/25/latest-starlink-satellites-equipped-with-laser-communications-musk-confirms/).

[65] Theresa Hitchens, "JADC2: SDA To Upgrade Satellite Laser Links", *Breaking Defense,* April 23, 2021. (https://breakingdefense.com/2021/04/jadc2-sda-to-upgrade-satellite-laser-links/).

[66] Interview with Frank Rose, while serving as Senior Fellow and Co-director of the Security and Strategy team in the Foreign Policy program at the Brookings Institution, August 2020.

[67] Jason Rainbow, "Verizon Announces Intent to Use Amazon's Planned Project Kuiper Installation," *Space News,* October 21, 2021. (https://spacenews.com/verizon-announces-intent-to-use-amazons-planned-project-kuiper-constellation/).

[68] Wiley, *Law Alert*, "Department of Justice Announces Increased Monitoring and Enforcement of National Security Agreements Under Team Telecom and CFIUS", July 21, 2020.

[69] Yevgeniy Sverdlik, "NEC Reaches Record 20 Fiber Pairs In New Submarine Cable Design," Data Center Knowledge, January 16, 2020. (https://www.datacenterknowledge.com/networks/nec-reaches-record-20-fiber-pairs-new-submarine-cable-design).

[70] Bobbie Johnson, *The Guardian*, "How One Clumsy Ship Cut Off the Web for 75 Million People," February 1, 2008. (https://www.theguardian.com/business/2008/feb/01/internationalpersonalfinancebusiness.internet#:~:text=According%20to%20reports%2C%20the%20internet,in%20bad%20weather%20on%20Wednesday)

[71] Winston Qiu, "Submarine Cables Cut after Magnitude-9.0 Earthquake and Tsunami in Japan," *Submarine Cable Networks*, March 12, 2011. (https://www.submarinenetworks.com/news/cables-cut-after-magnitude-89-earthquake-in-japan).

[72] The Data Center Podcast February 2021, interview with Alan Mauldin who tracks the submarine cable market at TeleGeography.

[73] Thomas Nilsen, "Disruption at one of two undersea cables to Svalbard," *Barents Observer*, January 9, 2022.

[74] Interview with David Feith, Adjunct Senior Fellow, Indo-Pacific Security Program at the Center for North American Security (CNAS), June 2021.

[75] "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force." Cybersecurity & Infrastructure Security Agency. Accessed January 31, 2022. https://www.cisa.gov/ict-scrm-task-force.

[76] Cybersecurity and Infrastructure Security Agency (CISA), "CISA Launches a Space Systems Critical Infrastructure Working Group," May 13, 2021. (https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group#:~:text=WASHINGTON%20%E2%80%93%20The%20Cybersecurity%20and%20Infrastructure,that%20support%20the%20nation%27s%20critical).

[77] Latham & Watkins, "Committee on Foreign Investment in the United States: Key Questions Answered," 2020. (https://www.lw.com/thoughtLeadership/committee-foreign-investment-united-states-key-questions-answered-CFIUS).