Title:
Localizing Conceptualizations of Submarine Cable Security

Author and affiliation:
First Author: Lane Burdette, George H.W. Bush School of Government and Public Service at Texas A&M

Second Author: Jesse H. Sowell, George H.W. Bush School of Government and Public Service at Texas A&M
ORCID: 0000-0002-1970-920X

Correspondence details:
Jesse H. Sowell (jsowell@tamu.edu)

Abstract:
Contrary to characterizations of the submarine cable network as broadly insecure, the overall network is resilient and faces localized security threats. Local and regional variance is evaluated in six cases. Topologies are assessed based on redundancy and diversity, stratifying cases into three groups: traffic chokepoints (the Red Sea and South China Sea), island networks (the Caribbean and South Pacific), and developing markets (Brazil and the Arctic). State and private actors in each region pursue interests related to cost, local data markets, existing connectivity dynamics, incidental damage mitigation, intentional damage mitigation, diplomatic and cultural ties, and information security. The evaluative framework presented bridges the gap between nuanced topological characteristics and geopolitical factors affecting local, regional, and global network security. Analyses highlight the trade-offs facing emerging markets looking to build resilient networks that avoid the risk and security vulnerabilities evident in some established markets.

4-6 keywords:
Submarine cables, security governance, Internet infrastructure, risk, maritime security

Acknowledgments:

Funding information:

Disclosure statement:
No conflicts of interests.

Biographical note:
Lane Burdette is a Master of International Affairs candidate at the George H.W. Bush School of Government and Public Service at Texas A&M. Burdette's research focuses on the geopolitics of telecommunications security, particularly as related to submarine cables.

Jesse H. Sowell is an Assistant Professor of International Affairs at the George H.W. Bush School of Government and Public Service at Texas A&M. Dr. Sowell's interdisciplinary research focuses on the governance of Internet infrastructure and security, with a special focus on the role of epistemic authorities managing infrastructures that mediate our social, economic, and political lives.

Introduction

Submarine cables, essential for global Internet connectivity, are often overlooked by policymakers. Uncertainty in the governance of this digital infrastructure prompts concerns for communications security. These challenges are often characterized in general terms (Morel, 2016; Bueger & Liebetrau, 2021; Martinage, 2015). Case studies presented in this work operationalize these challenges in terms of the real geography of connectivity. In contrast to typical framings of a "borderless" Internet, this article highlights the distinct geographies of submarine cables. This tangible element of the Internet's infrastructure, both affecting and affected by security politics, is shaped by private and state interests alike. By focusing on regional case studies, this work characterizes the diversity in these relationships, identifying common and regional factors.

Research on this hidden infrastructure has emphasized that submarine cables are largely invisible, with their study relegated as a niche topic despite the network's criticality (Bueger & Liebetrau, 2021). Military analyses perceive cables as assets which, under insufficient international protection, are broadly threatened by aggressors (Chapman, 2021; Kono, 2019; Sunak, 2017). Many news articles contain factual errors that mischaracterize cable security and perpetuate internalization of knowledge within the cable industry. For example, damage by sharks to submarine cable systems is intermittently sensationalized by media and is even reported in U.S. government documents (Public-Private Analytic Exchange Program, 2017), despite a statement from the International Cable Protection Committee that sharks no longer threaten the cable network (2015). A 2015 article in the New York Times also notoriously inflates the Russian threat to submarine cables (Sanger & Schmitt, 2015), better summarized by Matsakis (2018) and Hinck (2018). Starosielski argues for literature to move beyond narratives of connection or disruption (2015, Chapter 2), and Bueger and Liebetrau (2021) call for broader analyses of cable networks that bring together security, legal, and regulatory frameworks.

This article adds nuance to submarine cable security analysis by comparing local conditions in six regional cases. Cases were selected by their topology and to highlight geopolitical dynamics that unequally affect *parts* of the cable network. These are grouped into traffic chokepoints, island networks, and developing markets. Cases in the traffic chokepoints group, the Red Sea and South China Sea cases, examine implications of critical corridors that concentrate cable segments in small but economically efficient areas. The Caribbean case and the South Pacific case represent island networks which lack sufficient cable connections for secure connectivity. Finally, in the developing markets group, the Brazilian and Arctic cases investigate areas of change within the global cable network. Unlike previous groups, cases in the developing markets group target emerging, not established, topologies. Comparative analysis of these cases provides a framework for understanding relationships between topological conditions like diversity and redundancy to regional security and economies.

This article first offers a primer on the cable network, presenting both the business and practice of communications security. Cases then examine regional conditions. Across cases, industry actors consider region-specific relationships between cost, local data markets, existing connectivity dynamics, potential for incidental damage, potential for sabotage, diplomatic and cultural ties, and intelligence gathering opportunities. These are known factors (Carter et al., 2009; Kono, 2019; Starosielski, 2015; Thorat, 2019), evaluated here within their geographic contexts. Region-specific analysis highlights that the conditions for secure connectivity are not uniformly distributed. Rather, network security varies, with cascading local, regional and global effects. Emerging topologies may learn from vulnerabilities in established markets and seize opportunities for resilient development.

Evaluating cable network resilience

Submarine cables are critical communications infrastructure that traverse the seafloor and carry approximately 97% of international internet and voice traffic (TeleGeography, 2022). This includes virtually all financial transactions. The deployment of submarine cable links across the globe is not homogenous but instead exhibits different patterns across regions. Initial growth was driven by states and large multinational telecommunications carriers, but the submarine industry is now almost entirely in private hands (Burnett et al., 2013). This and the transnational nature of cabling complicates governance.

There are currently 436 in-service submarine cables (TeleGeography, 2022). These can cost hundreds of millions of dollars to lay, and operational costs range from $100 to $1,000 per kilometer annually (Starosielski, 2015, p. 122). Between 2017-2021, $9.7 billion was invested in submarine cables, 14% of which came from Multilateral Development Banks (Submarine Telecoms Forum, 2021, p. 43). Submarine routes are preferable over terrestrial links because they insulate communications infrastructure from human interaction (Starosielski, 2015, p. 29). They are also cheaper and faster than satellites, whose capacity is insufficient to meet global demand (Kono, 2019). Satellite communications nonetheless complement fiber capacity in remote areas and provide *limited* support if submarine connectivity is unavailable.

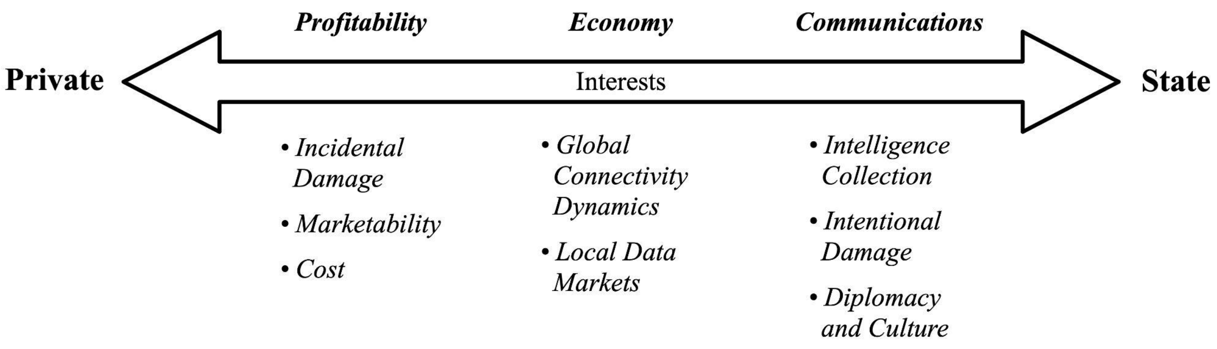
Cable breaks are common. Over 100 occur annually, most of which are the result of accidental human activity like fishing. Others result from natural disasters or component failure (TeleGeography, 2022). When a break occurs, traffic is automatically rerouted along alternative routes. Global repair systems exist to re-establish connectivity, though this is an expensive and time-consuming process (Kono, 2019, sec. 2e; Submarine Telecoms Forum, 2021, sec. 4). Despite costs, the overall network is resilient and faces localized, not broad, security threats.

Security conditions vary and can be understood through the framework of redundancy and diversity. Redundancy references the number of cables serving a region. Without redundancy, states rely on a single cable for their connectivity and a break can result in catastrophic connectivity loss. Diversity describes the distribution of landing points and cable paths within a region. For instance, connectivity to a high redundancy state may still be impacted by a single natural disaster if all cables have segments in the affected area, called a chokepoint.

Perhaps the most significant economic trend of modern telecommunications is the rise of predominantly American content providers like Facebook, Google, Amazon Web Services, and Microsoft Azure. Platforms have become the primary driver of online traffic, with total bandwidth demand by content providers rising from 10 to 66% between 2012-2020 (Lairson et al., 2021). These companies, recognizing the value of ensuring connectivity to global markets, have begun making capital-intensive submarine cable investments. This viable and profitable method to ensure platform performance has led to a period of accelerated development in the industry, which can be differentiated from previous development booms. Investment in the early 2000s featured "speculative builds along duplicative routes" by companies intending to resell capacity. Contemporary efforts are driven "by large web-based companies that understand their demand curve" and are less likely to overbuild existing routes (Brake, 2019, p. 3).

The contemporary cable network, like the telegraph network before it, was developed by diverse and often uncoordinated actors with variable means and interests. These can be broadly grouped into state and private actors. States prioritize communications security and economic development. Private entities are also interested in economic development but emphasize profitability over other factors (see Figure 1). Although fiber-optic cables are new, their topologies frequently mirror those of colonial telegraph networks (Thorat, 2019, p. 253). As demand for connectivity in a given area increases, companies seek out well-trod paths for deploying cable systems which are cheaper and less risky. This increases profitability but may stagnate diversity and decrease communications security. Per Starosielski in her book *The Undersea Network*: "New cables will continue to follow the old routes until governments or other organizations are willing to spend the money it takes to develop new pathways of exchange: global network diversity is a problem that cannot be fixed by market forces alone" (2015, p. 62).

Figure 1: Interests of actors in submarine cable development



The construction of cable networks is frequently described as a link binding together states and peoples (Starosielski, 2015, pp. 69–72, 194). In this way, cable construction can be perceived diplomatically. Note, however, that a technical assessment of a state's international bandwidth or connectivity must be understood separately from internet access within that state. Cable networks rely on terrestrial infrastructure which may be insufficiently developed to reach end-users. Some cable landings are little more than "relay stations," where international traffic is transmitted but does not penetrate into local networks (Thorat, 2019, p. 260). This is common in the Global South, which is also disadvantaged in cable deployment due to early colonial influences on network topology, the distance between countries, and the perception that links to new states will be expensive and/or insecure (Starosielski, 2015, Chapter 1).

Cables are incorporated into international agreements. The 1884 Convention on the Protection of Submarine Telegraph Cables increased protections and permitted navies to board offending vessels. The treaty was invoked in 1959, when the U.S. boarded a Soviet trawler that cut five cables off the coast of Newfoundland (Hinck 2017). The 1982 United Nations Convention on the Law of the Sea (UNCLOS) defined maritime boundaries extending from the coastline and outlined permissions within a state's territorial sea and their exclusive economic zone. Today's security regime is characterized by lax enforcement and an "implementation gap." There are no international provisions for responding to a terror attack against the cable network (Matley, 2019, pts. 1, 3c).

Intentional damage poses an unlikely but potential risk. Most malicious actors like vandals, thieves, and others pose the greatest threat at the shoreline. State actors primarily threaten submarine cables off-shore, on the continental shelf, and in the deep sea (Public-Private Analytic Exchange Program, 2017, pp. 7–8). Intentional attacks are rare but documented; one famous example is Britain's sabotage of telegraph cables in WWI. In his 1924 book, *Cables and Wireless*, Schreiner wrote that "naval men are still wondering why the German submarines did not [retaliate by cutting] every cable connecting Europe and America" (1924, pp. 199–200). We know now that these attempts were made, with limited success (Navy Lookout, 2021). In the modern era, sabotage may be conducted using both high- and low-tech means including specialized submarines or grappling hooks. Where cables come ashore, a hacksaw and manhole lifter might suffice (FitzGerald, 2015).

It would be impossible for an actor to take down all internet, everywhere, using physical means. This is true in peace or wartime. Even if communications between nodes are limited, signal transmission would remain possible inside isolated areas (Matsakis, 2018). However, at cable chokepoints, well-targeted attacks could cause substantial disruption. Cables therefore pose an attractive, low risk target in asymmetric conflict which could achieve "enormous impact" using a relatively modest investment (Navy Lookout, 2021). For example, in 2013, three divers were arrested off the Egyptian coast after cutting the SE-ME-WE-4 cable, leading to a 60% reduction in Egypt's international bandwidth (Cochrane, 2021).

Fiber links also represent intelligence assets. Capabilities are highly classified, but it is reasonable to assume technologically advanced states might conduct bulk collection (Dorling, 2013; *Wikimedia Foundation v. National Security Agency/Central Security Service*, 2021, pp. 14–16). This is easiest at cable landing stations, where states have direct access to cables and regulatory control over service providers. Despite historical examples like U.S. operation Ivy Bells, it is uncertain whether high capacity, contemporary cables may be tapped underseas. One potential area to watch is underwater data center development (Judge, 2021) in conjunction with submarine abilities to manipulate seabed infrastructure. Close relationships between governments and telecommunications firms may also facilitate espionage, like the National Security Agency's (NSA) "partnership" with AT&T and China's tight control over state-owned carriers (Angwin et al., 2015; Portman & Carper, 2020, sec. 3).

Examining conditions across regions

The Red Sea and South China Sea cases highlight implications of traffic chokepoints, where segments of many cables are geographically concentrated in well-known corridors. This creates a security risk by physically grouping paths for regional and global data. These two maritime cases were chosen because of their centrality and vulnerability to geopolitical tensions. Island cases illustrate regions where terrestrial alternatives are simply not available. Islands' typically small populations and/or economies makes financing cable networks difficult and poses barriers to state engagement in global information and knowledge economies. The Caribbean and South Pacific represent two significant island communities seeking to improve connectivity and reduce interstate dependencies. Developing markets on the Brazilian coast and in the Arctic are seeing significant investment. Analyses of these topologies illustrate development strategies intending to alleviate pressure on global chokepoints and increase network diversity. Developing markets also provide an opportunity to highlight the trade-offs involved in strategies of vulnerability mitigation.

Table 1: Introduction to cases

	Diversity	**Redundancy**	**Case**	**Primary Weakness**	**Primary Strength**
Cable Chokepoints	Lower	Higher	Red Sea	Intentional or incidental catastrophic connectivity loss	Carries most Europe to Asia bandwidth
			South China Sea	Intentional or incidental catastrophic connectivity loss	New route development increases regional diversity
Island States	Lower	Lower	Caribbean	Dependence on U.S. and inability to fund alternatives	Island closeness cheapens connections; many states with two or more cables
			South Pacific	Incidental catastrophic connectivity loss	Competitive funding increases total foreign investment
Developing Markets	Higher	Lower	Brazil	Catastrophic connectivity loss at landing station	Most diverse topology in South America
			The Arctic	Challenging financing for expensive construction	Alleviates global chokepoints; availability of cooling

Traffic Chokepoints

New cable connections typically lay fiber along the shortest or most favorable paths. Inevitably, common or favorable routes accrue the highest number of cables. Incidents at high concentration chokepoints—where many cable segments pass through geographic corridors—are more likely to affect several cables and cause significant disruptions, with potential cascading effects for extraregional endpoints. This section examines two major chokepoints, the Red Sea and South China Sea. Both are historically significant cable routes, densely cabled, that are now experiencing modern diversification efforts (Schreiner, 1924, fig. "Chart of the World's Principal International Cables"). Chokepoints are insecure, but should be recognized for their large role in intercontinental connection.

The Red Sea

The Red Sea is a frequently traveled maritime area pinched-off in the North by the Suez Canal and in the South by Bab al-Mandab, a strait less than 10 nautical miles wide between Yemen, Djibouti, and Eritrea. Despite significant redundancy, the low geographic diversity of these chokepoints creates risks. Cables traversing the Red Sea carry between 17-30% of all global bandwidth and most Europe to Asia traffic (Cochrane, 2021).

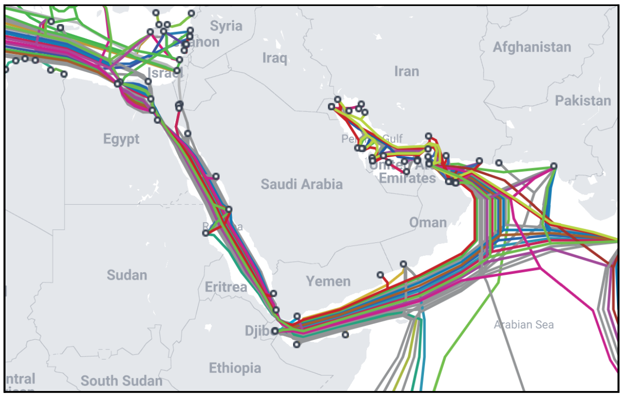


Figure 2: In-service and planned Red Sea cables (TeleGeography, 2022)

Submarine cables do not pass through the Suez Canal. Instead, "all cables crossing Egypt are connected to terrestrial cables in ducts buried underground, without touching the Suez Canal," affording Egypt the highest redundancy in Africa (TeleGeography, 2022). Egypt also leverages its local monopoly to increase local transit costs (Starosielski, 2018). The potential for intelligence gathering at this central node is unlikely to escape the eye of Egyptian President Abdel Fatteh el-Sisi, former Director of Military Intelligence, or that of his son, current Deputy Director of the General Intelligence Directorate (Cochrane, 2021). Well-targeted attacks on Egyptian facilities could significantly impact global communications; in 2010, 80% of all traffic between Europe and the Middle East passed through a single building in Alexandria (Sechrist, 2010, p. 43).

Cables do pass through Bab-al-Mandab. The strait is crucial to global military strategies and its closure would have widespread effects in a major conflict. Nonstate actors in this area are of particular concern, as "a well-financed terrorist group could easily get its hands on [a semi-autonomous or remote undersea vehicle] in order to target key cables and junction points. It could also opt for brute force, using fishing trawlers equipped with deep-sea grappling hooks to maul cables in shallower waters" (Martinage, 2015).

Nearby Djibouti is home to significant foreign influence. Multiple states have local military bases, including the U.S., China, and France. Djibouti was also found to be at high risk of "debt distress from BRI-related financing" (Hurley et al., 2018, sec. 3.4). The BRI, or Belt and Road Initiative, is a program for global infrastructure development hosted by the People's Republic of China (PRC). The project provides competitive loans, largely to developing countries, but is associated with security concerns. An examination of 100 BRI contracts found that, in all instances, severing diplomatic ties with the PRC could trigger default clauses requiring immediate loan repayment (Gelpern et al., 2021, p. 7). Debt relief is typically handled on an ad-hoc basis and has resulted in territorial asset transfers (Hurley et al., 2018). Djibouti's status as a relay station parallels this dynamic of foreign influence in the submarine cable network (Thorat, 2019, pp. 260–261).

Regional cable alternatives to the Red Sea are sparse, requiring either a high-latency lap around Africa or long terrestrial links through geopolitically risky states. The Blue and Raman cable systems stand out as diversification efforts in a corridor physically unsuited to topological change. The two are owned by the same consortia—Google, Omantel, and Telecom Italia Sparkle—and would connect in Aqaba, Jordan. Together, they would stretch from France to India through Saudi Arabia and Israel (TeleGeography, 2022). They are essentially one cable, divided for geopolitical reasons. The cables nonetheless represent improved relations. Per telecommunications researcher Karatzogianni, "If Saudi Arabia signs up to the deal with the Israelis, it will be a significant moment in geopolitics, where tech infrastructure - the fibre optic cable - becomes a facilitator for strategic collaboration between regional historical enemies" (Cochrane 2021). Note that the link will still route through Bab al-Mandab.

The South China Sea

The South China Sea (SCS) is a major international waterway which facilitates $3.37 trillion in trade annually (Blackwill et al., 2021). Concentrated cable segments pass through the Strait of Malacca near Singapore and Luzon Strait between Taiwan and the Philippines. The SCS is susceptible to natural disasters including earthquakes which may increase the frequency of unintentional breaks (Gerlach & Seitz, 2013, p. 32). This was highlighted after the 2006 Hengchung earthquakes off of Southwest Taiwan broke nine submarine cables. Subsequent repairs required 11 ships and lasted 49 days. Because Taiwan is difficult to avoid in local data transit (Faidherbe et al., 2021, p. 60), connectivity loss also impacted surrounding areas, with significant disruption to Hong Kong and South Korea (Chapman, 2021, p. 9). One-third of global cableship activity reportedly occurs in East Asia, South East Asia, or the China Coast. These are also the top three regions for activity globally (Submarine Telecoms Forum, 2021, p. 75).

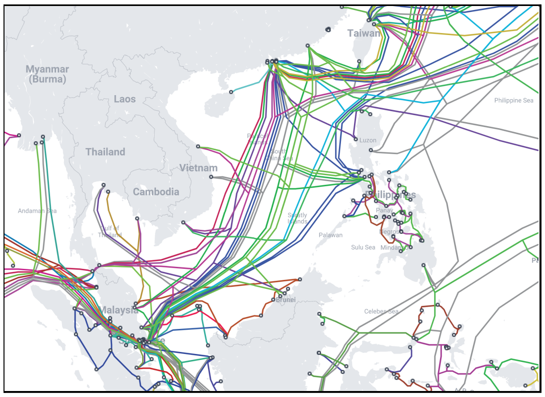


Figure 3: In-service and planned South China Sea cables (TeleGeography, 2022)

The SCS is a pressure point for international conflict. The sea is disputed by China, Brunei, Indonesia, Malaysia, the Philippines, Taiwan and Vietnam. China's claim overlaps all others to encompass most of the sea. A unanimous 2016 ruling in favor of the Philippines found China to be in violation of UNCLOS. China does not accept this ruling and has artificially constructed or enlarged islands in the SCS to reinforce its claim (Blackwill et al., 2021). Chinese cableships have been documented in the sea and may be laying clandestine networks between artificial islands (Long, 2020). Chinese military action in the SCS prompted responses from local states in 2021 and a Chinese invasion of Taiwan is increasingly likely (*2021 Annual Report to Congress*, 2021, pp. 316–318, Chap. 4). Taiwan relies on submarine cables for nearly all external communications.

Worsening U.S.-China relations shape cable topologies in the SCS. Under the 2020 Clean Network program and in the context of tightening Chinese control over Hong Kong, the U.S. has systematically denied licenses for cables landing near China or those owned, operated, or supplied by Chinese state-owned companies. This strategic disconnection has led to the cancellation or significant alteration of several projects. The first was the Hong Kong stretch of the Pacific Light Cable Network, which was denied a license for operation by the U.S. Federal Communications Commission (FCC) in 2020 (U.S. DOJ, 2020). Shortly after, The Bay to Bay Express system, which would have connected the U.S., Hong Kong, and other states, withdrew their request for a cable license from the FCC. The project was then reconfigured, under the same consortium of Amazon, Facebook, and China Mobile, into the CAP-1 cable between the Philippines and California (TeleGeography, 2020). China Mobile was eventually forced out altogether (Clarke, 2021).

Several content providers have planned cables along new routes as U.S. policies incentivize eastward diversification. However, every planned cable still passes through the Strait of Malacca (TeleGeography, 2022). This critical passage remains a weakness of the overall network (Faidherbe et al., 2021, p. 60). However, restrictions on the saturated Singaporean data industry—implemented in 2019 and now slowly relaxing (Swimhoe, 2022)—may incent the development of alternate hubs. Meanwhile, China has begun to invest significantly in global submarine cable projects through the BRI Digital Silk Road. Chinese involvement in submarine cable investment grew from seven percent of new cable projects in 2012 to 20% in 2019 (Chapman, 2021, p. 21). Though this has increased redundancy of global infrastructure, Western entities disparage Chinese telecommunications equipment as a vehicle for state espionage (Gorman, 2020).

Island Networks

Island networks are examined here through the Caribbean and South Pacific cases. These networks are unique, both in the center of submarine networks, providing a hub for exchange of en-route maritime traffic, and at its edge, representing poorly connected states forced to rely on satellite alternatives. Island states are at particular risk for natural disasters, extreme weather events, and the effects of climate change. The potential for incidental damage increases the need for "reliable, redundant, and robust communications systems that are able to withstand unpredictable trauma" (Jensen & Minges, 2017, p. 23). However, low populations decrease demand for Internet services and disincentivize private companies from building redundancy.

The Caribbean

The Caribbean is an island region whose cable networks connect exclusively to the U.S. and South America; there are no transatlantic connections (TeleGeography, 2022). It is better connected than the South Pacific and had a robust telegraph network (Schreiner, 1924, fig. "Chart of the World's Principal International Cables"). Perhaps as a result of this, or generally due to higher incomes than other island states, many Caribbean nations have higher levels of broadband penetration (Jensen & Minges, 2017, p. 24).

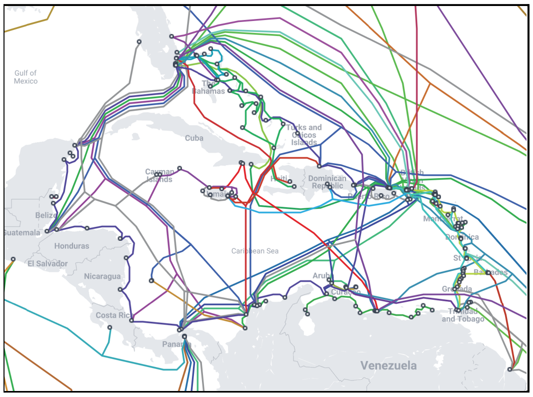


Figure 4: In-service and planned Caribbean cables (TeleGeography, 2022)

Financing Caribbean cable projects is difficult. Most local cables are owned by a consortia of private owners as "very few governments have the available finances to participate" (Fonseca-Hoeve et al., 2017, p. 24). U.S. backing could explain heightened connectivity to Puerto Rico and the U.S. Virgin islands. The Caribbean cable market is duopolized (Jensen & Minges, 2017, p. 20; Quarless, 2015); the two significant players in the region are Cable & Wireless and Digicel. This raises concerns over limited competition (Fonseca-Hoeve et al., 2017, p. 25), which is crucial to improving connectivity (Jensen & Minges, 2017, p. 34). It also contrasts with fierce competition in the local telegraph market during the 1890s (Winseck & Pike, 2007, p. 84).

Caribbean cable developers are driven by building "connectivity," not capacity, for which needs may already be met (Chard, 2014). This means that new cables are perceived to be both unnecessary and necessary by metrics of bandwidth or security. This tension surfaced when the government of the Cayman islands sought proposals for a third submarine cable. Opponents—namely, incumbent Cable & Wireless—claimed that even if local demand increased fivefold in the next decade, current capacity would be more than sufficient (Cayman News Service, 2020). However, both of the state's existing cables are over 20 years old, and the average economic lifespan of a cable is 25 years. A third link is currently planned through a spur on the AURORA cable system (TeleGeography, 2022).

U.S. conflict with Cuba, and the state's restrictive internet policies, also define local topologies. Disconnection between the two states is longstanding; in 1898, the U.S. offensively cut Cuban cables during the Spanish-American War (Fromageot, 1924, p. 843). Although U.S.-Cuban tensions are now relaxing, Cuba remains extremely isolated. At first glance, the state appears to connect to three undersea cables. However, two are U.S.-owned and only serve Guantánamo Bay (TeleGeography, 2022). U.S. law prevented American business dealings with Cuban companies after the 1959 revolution (Submarine Cable Networks, 2022) and, although Cuba was removed from the FCC's exclusion list in 2016, no cables have been permitted to land at the island (U.S. FCC, 2016). Cuba's only cable, ALBA-1, links to Venezuela and Jamaica. ALBA-1 was laid in 2011 but did not activate until 2013, which is unusual. Researchers also indicated that subsequent data traffic only flowed *into* the state (BBC News, 2013). A spur from the proposed ARCOS-1 cable made headlines as the first potential fiber connection between the U.S. and Cuba. However, the request for a Cuban spur was withdrawn in October 2020 (U.S. FCC, 2020).

The South Pacific

The cable industry's efforts in the South Pacific focus on building initial connections to far-reaching islands. This desire has driven local submarine cable demand but is now decreasing as more states connect for the first time (Submarine Telecoms Forum, 2021, p. 51). MANATUA, ready for service (RFS) 2020, was the first fiber-optic connection to the Cook Islands. Cook Island Prime Minister Puna emphasized the cultural significance of cable connectivity and multilateral development, stating that "this project is the dawn of a new era of cooperation and collaboration across Polynesia…It is the perfect model for the future of our region" *(Manatua Consortium, 2020).*

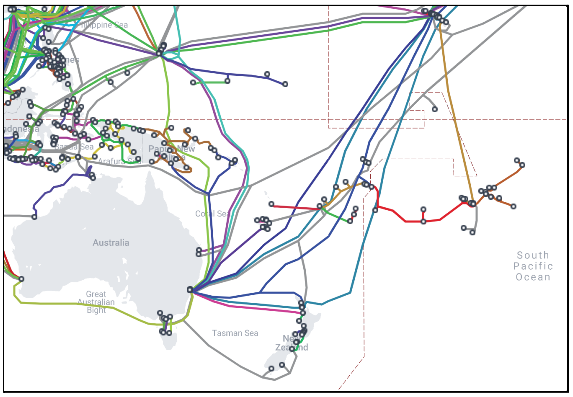


Figure 5: In-service and planned South Pacific cables (TeleGeography, 2022)

Other islands are in varying stages of developing redundancy. Guam is one of the best connected islands near the South Pacific. Cables are geographically incentivized to land at the island because it offers refuge from the nearby Mariana trench. It is also isolated from maritime traffic, reducing the likelihood of incidental damage, but still near to major hubs. As of 2015, more cables had landed on Guam than either California or Hawaii (Starosielski, 2015, p. 175). This sharply contrasts with Tonga, whose only international cable was severed during a recent volcanic eruption and subsequent tsunami. Emergency satellite communications are expected to provide only 10% of needed capacity and repairs may take four weeks (BBC News, 2022).

Of states with redundant connections, diversification efforts focus on new cable paths, not landing sites. This means that many South Pacific cables converge on central nodes like Sydney or Fiji. One explanatory factor is Australia's comprehensive legal regime, which restricts activity within cable protection zones (Matley, 2019, sec. 2). This limits incidental damage by humans but also restricts diversity by concentrating cable landing stations in Sydney and Perth. Cable companies are unwilling to shoulder the burden of increased costs from the establishment of new protection zones (Starosielski, 2015, pp. 57, 157). This trend is changing as diversification efforts promote new landings (TeleGeography, 2022).

Australia is also part of the Trilateral Partnership for Infrastructure Investment in the Indo-Pacific alongside the U.S. and Japan. The partnership promotes "transparency, open competition, sustainability, adhering to robust global standards, employing the local workforce, and avoiding unsustainable debt burdens" (U.S. DFC, 2018). This is a clear counter to China's regional BRI investment and parallels the formation of the Blue Dot Network, a standards-setting group by the same three states (U.S. DFC, 2019). Australia and New Zealand are also members of the Five Eyes Intelligence Alliance, which shares information with the U.S., Canada, and the United Kingdom (UK). In countering the BRI's influence, Australia—along with other alliance members—retain or expand their own surveillance capabilities over local networks.

The Trilateral Partnership funded the PC2 Palau branch from Facebook and Google's ECHO cable (RFS 2023), providing Palau's second international link, in a likely attempt to keep the bid from Chinese hands. Geopolitics and economic statecraft are concerns of the rich; although "some [small island developing states are] savvy enough to realise that there is some geopolitics and strategic competition issues going on…Pacific Island leader[s]...[are] just trying to get services for their people" (Investable Universe, 2020). At $30 million, PC2 would have cost Palau over 10% of its annual gross domestic product (Qiu, 2021a; The World Bank, 2021).

The partnership may also be involved with the proposed Humboldt cable between Valparaíso and Sydney. Initial interest from Huawei was intense and suggested a landing site in Shanghai. Despite encouragement from Chilean President Piñera and over $100 million Chinese investment in Santiago's data market, the Australian was selected alongside Japanese supplier NEC (Ashmore, 2021). Chile has received over 20 financing proposals "for an amount seven times the estimated investment" in the expensive project from development banks and others including Japanese, Argentine, and Brazilian entities (Bnamericas, 2021). The cable may also land at Rapa Nui (Easter Island), which lacks a fiber connection (Alley, 2020).

Developing Markets

This section evaluates areas of changing cable topologies. The Brazilian case is unique in Latin America because of its robust data industry and cable diversity. It also illustrates how states may seek to separate themselves from historical dependencies and reduce intelligence vulnerabilities. The Arctic, apart from a few contemporary efforts, is a new venue for cable deployment. This introduces some risk and increased costs, but it is also an opportunity to diversify the global network. The Arctic case also offers the opportunity to review two phenomena: connecting underconnected populations and the shadow of great power conflict on network topologies.

Brazil

Brail is a major conduit for Latin American data. Three states—Chile, Brazil, and Argentina—generate 80% of South American (SA) internet traffic (Bnamericas, 2021). Capacity to the Americas tripled between 2015 and 2019 but has slowed since (Submarine Telecoms

Forum, 2021, p. 30). Nearly all intercontinental traffic from SA passes through U.S. networks, and Miami in particular. Brazil is critical to Argentine and Uruguayan connectivity as data travels this Northbound route. Brazil is the most redundantly connected state in SA, and Fortaleza's landing stations are the only in SA which extend to Africa and Europe (TeleGeography, 2022). Brazil exemplifies moderate network diversity because, although connections reach a variety of external nodes, most of the state's landing sites are concentrated in Fortaleza. This is a significant weakness (Starosielski, 2018). Mitigation efforts include Google cable Firmina which will soon connect South Carolina, Southern Brazil, Uruguay and Argentina; bypassing Fortaleza altogether (TeleGeography, 2022).

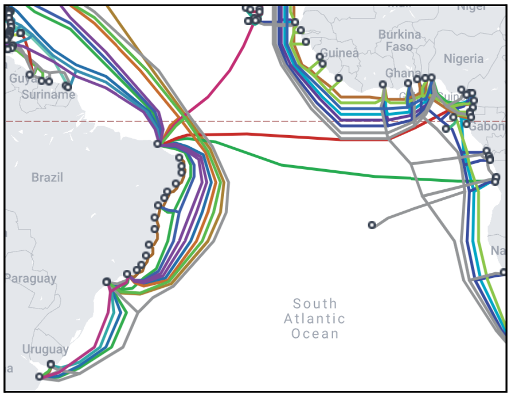


Figure 6: In-service and planned Brazilian cables (TeleGeography, 2022)

The 2013 Snowden Disclosures revealed large-scale U.S. and allied surveillance along submarine cables and are popularly viewed as a driver for non-U.S. cable development (Bueger & Liebetrau, 2021, p. 14). Discussions of U.S.-avoidant topologies frequently reference the BRICS cable, which would have connected Brazil, Russia, India, China, and South Africa in a diverse Southern route. The BRICS cable was proposed before the Disclosures but did not gain "significant traction or media attention" until afterwards (Lee, 2016). The project never came to fruition, a factor which could have fueled Chinese interest in cable network financing.

Brazil is often emphasized within this group as a state taking concrete steps to limit U.S. dependence and espionage. Hasler (2019) wrote that Brazil is "splitting up their international connections among firms based in a variety of countries," such that "no two new cables are being built to the same country." Brazilian President Rousseff herself also cited privacy concerns as a primary motivator for development of the now in-service EllaLink cable, which replaced an older link to Portugal and connects Brazil to Europe and Cape Verde (Emmott, 2014).

However, a longitudinal assessment presents an alternate explanation for Brazil's diverse routing and indicates that the Snowden Disclosures made little topological difference. In telegraph maps, Brazil is still connected to both Africa and Portugal (Schreiner, 1924, fig. "Chart of the World's Principal Telegraph Cables"). This topology is paralleled in 2012, the year before the Disclosures (Browning et al., 2012). Diversity in Brazilian routing is therefore not a new phenomenon but the *ongoing presentation of a static network topology*. Further, U.S. network centrality has not decreased since the Disclosures (Stronge & Mauldin, 2016), and U.S.-Brazil capacity grew by

50% between 2017-2021 (Submarine Telecoms Forum, 2021, pp. 30, 45). Both Brazil and the U.S. will likely remain central to SA connectivity.

The Arctic

The Arctic is a new and attractive region for cable development. Despite longstanding interest in Arctic topologies, northern routes were not feasible before the effects of climate change (Starosielski, 2015, pp. 15–16). Some seek Arctic routes to avoid U.S.-based networks (Reevely, 2022); the area is also "geopolitically stable and seismically safe" (True North Global Networks, 2021), with the potential to halve Europe-to-Asia latency (Submarine Telecoms Forum, 2021, p. 132). Further, the ice is a protective barrier to human interaction, reducing likelihood of incidental disruptions (Gerlach & Seitz, 2013, p. 16; Starosielski, 2015, p. 29).

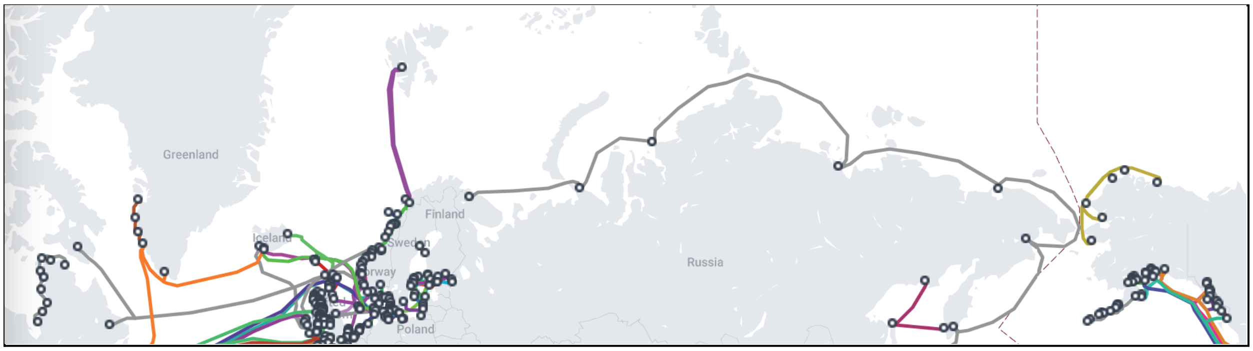


Figure 7: In-service and planned Arctic cables (TeleGeography, 2022)

Arctic cabling is unusually expensive (see Table 2) due to the cost of surveying unfamiliar routes, the necessity of ice-class cable laying vessels, and increased armoring to protect against freezing conditions (Pfeiffer & Khrennikov, 2019). Small, disparate Arctic populations generate insufficient demand to incentivize these costly networks (Starosielski, 2015, p. 20). This creates an expense gap which cable developers bridge using varied approaches. Co-founder and former CEO Elizabeth Pierce of Alaskan cable project Quintillion forged over $1 billion in contracts to secure investors and further the project. Although Pierce received jail time, the cable entered service in 2017—and reduced local bandwidth costs by 60% over three years (Carr, 2019; TeleGeography, 2022; CanArctic Inuit Networks, 2021). Polar Express, which traces Russia's Northern border, is funded exclusively by the Russian Ministry of Transport (Qiu, 2021b). Investment by the local government was scrapped by SednaLink in Northern Canada due to long wait times (Tranter, 2020). Another project, Far North Fiber, will connect Alaska, Canada, Ireland, Norway and Japan and appears to take a more traditional, consortium-based financing approach (DeGeorge, 2021).

Table 2: Comparative cost of Arctic cable systems.

Cable System	RFS Date	Region	Cost (million)	Length	Million USD / Thousand km
Polar Express (Qiu, 2021b)	2026	Transarctic	$889	12,620km	$70.5

Far North Fiber (True North Global Networks, 2021)	2025	Transarctic	$1,160	16,500km	$70.3
SednaLink (CanArctic Inuit Networks, 2021)	2022	Canadian	$107	2,100km	$51.0
EllaLink (Dawn-Hiscox, 2018)	2021	Transatlantic	$250	9,200km	$27.2
2Africa, before expansion (TechCentral, 2020)	2023	African	$1,000	37,000km	$27.0
Humboldt ("Brazil Joins Chile in Building First Fiber Optic Cable to Connect S. America and Asia," 2021)	2025	Transpacific	$338	13,180km	$25.6

One economic incentive for Arctic cable development is the possibility for local, energy-efficient data center markets. Cooling equipment in data centers requires substantive energy and water consumption. Arctic climates and renewable energy availability are conducive to lower cost, more environmentally friendly data center operations. However, building data centers in the Arctic—away from most end users—increases latency (Telehouse, 2017). Submarine cable networks are needed to reduce this. Although some northern communities are enthusiastic about the economic and connective opportunities of data center buildouts, better-connected areas protest abuse of local resources to power foreign services. After Facebook data center was announced in Dutch town Zeewolde, residents organized against the project, which would use local farmland, water, and electricity to power "porn [and] conspiracy theories" (Meaker, 2022).

Even though many Arctic cables stretch between redundantly connected states, their unique topology will reach communities that lack reliable or abundant internet access. Iqaluit, capital of Canadian territory Nunavut, currently relies on a single communications satellite but will soon be connected via the SednaLink cable (Reevely, 2022). This is a long-awaited development in Nunavut, which is predominantly Inuit and faces a "connectivity crisis" (CanArctic Inuit Networks, 2021). Former Iqaluit mayor and current chief operating officer of CanArctic Inuit Networks Madeleine Redfern, emphasized that the SednaLink cable, "a private project guided by northerners and enabling development in the north" is a form of "Indigenous *economic* reconciliation" (Reevely, 2022). Press releases further state that SednaLink will strengthen "Inuit culture and language," improve "education and health care," and increase "economic development opportunities" (CanArctic Inuit Networks, 2021). At least two other projects are underway to connect the territory (Tranter, 2020; Reevely, 2022).

Two Arctic cables, Far North Fiber and Polar Express, are contextualized by Arctic Connect, a failed parent project which would have connected Russia, Japan, and Norway. The split's cause is uncertain; some suggest failed financial negotiations with Japanese partners (Staalesen, 2021), others indicate difficulties with state approval by Russia due to "national security concerns" (Stolyarov, 2021). This is surprising because Russian cable operator Megafon, which partnered on Arctic Connect with Finish company Cinia, has reportedly close ties with the state's military and intelligence arms (Chapman, 2021, p. 20). Cinia is now associated with Far North Fiber, not

Polar Express. The two cables will take distinct routes and, per Far North Digital's CEO, are intended to be "complementary," not competing (DeGeorge, 2021).

Arctic cables would be difficult to monitor and under significant control by Russia (Tibbles, 2021), which commands the world's most robust icebreaker fleet (U.S. Coast Guard, 2017). Russia has demonstrated interest in internet infrastructure targeting; during the annexation of Crimea, Russian actors targeted the Simferopol Exchange Point and "will have noted the striking success in gaining information control over the region, and will be looking for where it can be applied elsewhere" (Giles, 2016, p. 64). International interest centers around activities by the Yantar, a Russian spy ship which may be capable of cable manipulation at the seafloor, and Russia's Belgorod, "one of the least understood submarines currently being built" (Sutton, 2019, 2021). Norway has requested assistance tracking nearby Russian submarines (Sanger & Schmitt, 2015) and Russian involvement is suspected in the recent disappearance of 9.5 tons of undersea cable from a Norwegian observatory (Scully, 2021). The UK also plans to build a new ship explicitly to protect cables from Russian manipulation (Moss, 2021), following the recommendation of a 2017 report on the Russian threat (Sunak, 2017, Chapter 5).

Factors in local development

Cable chokepoints in the Red Sea and the South China Sea have high redundancy. The Red Sea's geographic boundaries largely prevent diversification, though some progress is occuring in the SCS. Low diversity and redundancy was expected of the Island networks. This holds in the South Pacific but less so in the Caribbean, where more states have secondary connections. In developing markets, high diversity and low redundancy was anticipated. Brazil is a counterexample, with the best redundancy and diversity in South America. Due to concentrated landings in Fortaleza, Brazil is classified as medium diversity. Brazilian cables also present an unanticipatedly static topology. Many cable development projects in the Arctic follow entirely new routes, increasing diversity for already well connected states, but their speculative nature produces near-zero regional redundancy. Analysis of cost, local data markets, global connectivity dynamics, diplomacy and culture, the risk of incidental and intentional damage, and intelligence access are examined below. This analysis is summarized in Table 3.

Table 3: Detailed case summary

	Red Sea	**South China Sea**	**Caribbean**	**South Pacific**	**Brazil**	**Arctic**
Redundancy	High	High	Medium	Low	High	Low
Diversity	Low	Medium	Medium	Low	Medium	High
Cost	Monopoly	Uncertain	Duopoly	Foreign competition	Uncertain	Most expensive
Local data markets	Limited	High	Limited	Limited	Developing	Limited
Global connectivity	Static	Early development	Late development	Mid development	Static	Early development

dynamics						
Incidental damage	High	High	High	High	Medium	Uncertain
Diplomacy & culture	Exclusive	Exclusive	Exclusive	Inclusive	Exclusive	Variable
Intentional damage	Highest	Highest	Lowest	Lowest	Lowest	Uncertain
Intelligence	Concentrated	Distributed	Concentrated	Concentrated	Distributed	Distributed

Summary of discussions in sections 4.1-4.7.

Who bears the cost?

Costs, born primarily by private actors, include the price of surveying, materials, operation, repairs, and other necessary services. The Red Sea and Caribbean indicate monopolized or duopolized markets, which may stagnate local diversification and increase costs. The duopoly in the Caribbean case is a contrast to the competitive telegraph market, which may have boosted historical network diversity. Given static network topologies, resistant to change, it is unclear how consolidated markets might reduce diversity over time.

Cost has a close relationship to diversity. For example, the SCS has many alternative routes, though these may be longer and more costly. The compounding of regional topologies despite alternatives illustrates how chokepoints may develop without physical restrictions. Many cost-intensive cables are nontheless planned for the Arctic instead of following other, cheaper paths. Diverse routes provide reliability that may prove profitable in the face of catastrophic disruptions elsewhere. For these Arctic developers, risk mitigation balances immediate costs against long-term resilience and gains. Immediate investment costs are more salient to small states that struggle to balance connectivity security needs with relatively low consumer demand.

Connections to small island developing states are generally supported by external loans, equity or grants, which has facilitated connection of nearly all island states to one or more cables (Jensen & Minges, 2017, p. 13). Future connectivity opportunities include “piggy-backing” or “island hopping.” Piggy-backing connects islands via a spur on a nearby cable system. However, spurs must be planned in advance, as “it is virtually impossible to add a branch to an existing cable” (Jensen & Minges, 2017, p. 41). Seizing these opportunities requires quick turnarounds that may not align with the slow process of acquiring international development grants (Starosielski, 2015, p. 191). No legal requirements exist for cable developers to include spurs (Jensen & Minges, 2017, p. 42). Island hopping envisions a network of interconnecting, short island cables that share external traffic. Because short cables are cheapest, this is best suited to close island chains.

American-allied and Chinese investment are increasingly at odds in cable network development. Although investment from either party is sometimes perceived as insecure, heightened competition in submarine cable financing may increase network redundancy, especially for small nations or expensive projects. Considering one group of actors may invite bids from the other, increasing overall investment. In regions like the South Pacific, potentially legitimate economic or information security concerns arising from foreign cable operators, suppliers, or investors, must be balanced against the risk of disconnection. From either perspective, when dealing with an adversary, you may as well get a bargain.

Keeping up with local data markets

Data center markets create demand for stable, high capacity connectivity infrastructure like submarine cables. Local markets are not uniformly saturated across significant chokepoints. In the SCS, tech giant Singapore actively restricts its overdeveloped data industry. The percentage of internet users is also much higher along SCS chokepoints than in the Red Sea; approximately 90% in Singapore, Malaysia, and Taiwan compared to 72% in Egypt and 59% in Djibouti (ITU, 2021). Although Egypt and Djibouti are outliers for the region, their connectivity is still low compared to the SCS chokepoints. This imbalance between local markets and global connectivity portrays Red Sea landing points as "nodes of abundance, enabling the interlinking of the rest of the world," which lack local access even as "the technical means of improving Internet access…has either already made landfall or passes just off their shores" (Thorat, 2019, pp. 260–261).

The Arctic is a unique case where market forces may diversify topologies. This contradicts the perspective presented by Starosielski (2015, p. 62). In a distributed design, content providers would build data centers within local markets. However, it may be cheaper to build data centers in favorable environments and invest in infrastructure to serve external markets (Agrawal, 2021). This externalization strategy may also be more environmentally friendly, as companies like Google shift compute workloads across global data centers by renewable energy availability (Radovanovic, 2020). The resulting preference for northern development may limit southern data center investment. Put another way, although "policymakers, telco data centers and operators in emerging Asian markets view subsea cables as a positive trend…cables will drain away all the workloads from emerging Asia to large farms in the cooler, greener and calmer climes of the temperate zones" (Agrawal, 2021). Strategic externalization of data center markets will also have to contend with data nationalism and jurisdictional issues. The result is a complex trade-off where demand for efficiency (and the cables that support efficient externalization) must be balanced against not only long- and short-term costs, but data nationalization trends and actors' obligations to regulations shaping where data storage and processing can take place.

The development of local data markets also differentiates the Arctic and island cases, which are otherwise similar. Arctic states are typically large, well-established economies seeking to connect isolated areas. This parallels some islands—like Hawaii or Puerto Rico—whose cable networks receive unusually high investment. However, data center innovation in the Arctic provides an incentive for development which is missing in the South Pacific and Caribbean. Difference in reputation and perceived returns may therefore help carry Arctic cables through the early stages of project development, and helps explain why Arctic cable builds are accelerating.

Connectivity dynamics and the role of extant topologies

The perceived cost effectiveness of stable routes from the telegraph network shapes some current topologies. For instance, Brazil's current topology mirrors its early telegraph network. Arctic networks do not share this legacy. The Arctic is a new frontier in submarine cabling and may require substantial government investment due to high costs. This is also true for island networks. Telegraph maps show substantially more connections between Caribbean islands than their South Pacific counterparts (Schreiner, 1924, fig. "Chart of the World's Principal Telegraph Cables"), perhaps due to either the Caribbean's closeness to the U.S. or the shorter distance between islands, which would make cablelaying more economically viable. This has led to greater redundancy in the Caribbean as compared to the South Pacific, which is still connecting some islands.

Changing network dynamics do not occur in a vacuum and would impact other areas. Developing new routes adds redundancy that reduces dependence on low diversity chokepoints like in the Red Sea and the SCS. Catastrophic connectivity loss in Egypt, currently "the biggest single-point failure in the world," would dramatically increase demand on other systems worldwide (Starosielski, 2018). Arctic alternatives to Telecom Egypt's local monopoly may also encourage more competitive transit rates. Similarly, increased redundancy in the South Pacific would reduce reliance on SCS chokepoints. This is already happening as U.S. policies push investment away from landing points in Hong Kong and towards Australian and/or Japanese companies. Less attention has been paid to the Strait of Malacca near Singapore, which remains a vulnerable chokepoint.

Coping with the risks of incidental damage

Cables are at the greatest risk for incidental damage by human actors near the shoreline. Natural damage is more distributed. Volcanoes and tsunamis may affect the shoreline or cables at varying depths; landslides and earthquakes are most likely to cause damage on the continental shelf or in the deep sea (Public-Private Analytic Exchange Program, 2017, pp. 7–8). Landing points and near-shore chokepoints are among the most vulnerable to incidental human damage. Island states also have a higher risk factor due to an increased potential for natural damage. Brazil, without either of these exacerbating factors, is at less risk. The potential for damage in the Arctic is unknown.

One of the broadest threats to the cable network is climate change, which may increase the frequency of natural damage. Improved cable technology and protections may counter this trend, but cable landing sites are inherently coastal structures, unprepared to withstand rising sea levels (Carter et al., 2009, pp. 39–41). By 2033, thousands of miles of terrestrial cables are expected to be underwater (Borunda, 2018). Because the economic lifespan of a cable is twenty years—and the lifespan of a cable landing station longer than that—accommodating realistic projections of climate change is a pressing concern.

Mitigating geopolitical threats

The effects of intentional damage vary by target and strategy. For example, an actor seeking to disrupt connectivity to Vanuatu could target the state's one cable (ICN1) at the island's only landing station or offshore using a fishing trawler. This would have limited effects on the broader network but significant effects for Vanuatu. Attacking Vanuatu's connectivity where that cable connects to Fiji might have greater effects, as would targeting Vanuatu through an attack on cable landing stations in Sydney, where landings are concentrated. All would accomplish the same goal.

Some areas are more likely to be attacked than others, including geopolitically rich targets in cases like the SCS or Red Sea. In extreme cases, attacks at chokepoints could have intercontinental effects. However, the risk of intentional damage is generally low. Focused attention on Russian actors is a likely example of threat inflation; it is unclear where Russia might target submarine cables, not least because significant disruption would severely curtail Russia's own connectivity (Matsakis, 2018).

Calls for improved submarine cable protections by international bodies must be reconciled with the inability for international legislation to secure the submarine cable network during conflicts. Despite two centuries of development and the growing importance of cable networks, current governance structures are sharply lacking in scope and implementation. Even the Australian method, which formalizes submarine cable protections, introduces insecurity by limiting diversity. Put another way:

> *To waste time then on projects intended to make cables secure in times of war would not be unlike pouring water into the sea…What would be gained by that?...To say that [submarine cable sabotage] would conflict with some paragraph in international law…would have no practical result. The precedents made during the world war are of record. To some extent they will be incorporated in the new set of rules for international conduct; in their entirety however, they will be seized upon as valid excuses in the next war.*
>
> *International communications, then, be this land or submarine or wireless telegraphy, will in the future be at the mercy of the power that can impose its will. That aspect of the case is so definite that consideration for the purpose of finding an alternative is futile.* (Schreiner, 1924, p. 200)

Fear of sabotage has prompted some to recommend establishing "dark" fiber networks, excluded from public maps (Sunak, 2017). This would not increase cable security. Publication of submarine cable routes was hotly contested in the mid-20th Century, but necessitated by new fishing equipment that damaged cables more frequently. While hiding submarine infrastructures may protect against nefarius actors, it increases the likelihood for incidental damage (Starosielski, 2015, pp. 151–159). Low diversity routing strategies imply dark cables would likely be laid near to their publicly-known counterparts, making them equally vulnerable to the next largest category of breaks: natural events. Security by obscurity is a risky strategy and even "hidden" cables may be located by advanced technologies (Xu et al., 2016, p. 602). Finally, most submarine cables do not use all capacity, with the "lit" portion averaging only 18% worldwide (Submarine Telecoms Forum, 2021, p. 29). This means that dark cables would not meaningfully increase the ratio of used-to-available capacity.

Navigating diplomatic and cultural ties

Diplomacy and culture may be leveraged exclusively or inclusively in narratives that connect or disconnect from other states. Inclusive connection uses cultural ties to argue for interconnection, as in the case of the South Pacific and Arctic. Exclusive narratives are used to restrict landing points or to strategically disconnect from other states. This is seen across nearly all cases. Connections outside of Egypt are limited in the Red Sea, connections to China are limited in the SCS, connections to Cuba are limited in the Caribbean, connections to the U.S. are limited in Brazil, and connections between Russia and the West are limited in the Arctic. Notably, the U.S. is involved with several identified examples, either as the driver or target of exclusive policy.

Contemplating endemic intelligence threats

Intelligence access to the submarine cables can be sorted between concentrated and distributed topologies. In a concentrated network, most data passes through a small number of nodes that may provide collection access. In a distributed network, transmitted data is not particularly vulnerable to any one state. Concentrated networks exist in the Red Sea, to which Egypt has particular access, and in the island cases, which are most accessible to American-allied groups. This includes the Five Eyes alliance, which work in tandem to ensure favorable network dynamics for intelligence gathering.

The exploitation of global communications for intelligence gains is endemic and should not be associated exclusively with any one state. Although some signals intelligence services—like the NSA and the UK's Government Communications Headquarters—may receive more attention than others, "in the game of foreign surveillance, there are few clean hands" (Crowley, 2013). Even following the Snowden disclosures, French Foreign Minister Bernard Kouchner told France Info radio that it was not NSA's activities, but their scope, that drew envy and performative scorn from global leaders (LoGiurato, 2013).

Conclusion

Varied and localized security conditions indicate that cable network assessments must consider local and regional factors. It is insufficient to say that increased redundancy or diversity is needed without specifying where, and how both benefits and costs will be distributed. It is also insufficient to claim that any one actor or type of actor is a threat to the "network" without clarifying the vector of attack and the scope of its implications. Frequently, disruptions may not threaten the network at all, only local states which will soon be reconnected following a routinized repair process. More nuanced approaches to evaluating submarine cable security will improve the credibility of and usability of assessments, reducing threat inflation and providing more actionable, appropriately scoped information for mitigating security concerns.

The interplay between geopolitics and network development is evident across cases as emboldened state leaders discriminately license, operate, and finance global communications links. This may stagnate diversification, retrenching current dependencies. It may also increase diversity, as in the SCS. However, the best cable development, with an eye to long-term security, is imaginative and maximally inclusive, alleviating dependencies by reducing reliance on any one entity. States should conceptualize a high redundancy and high diversity “ideal” network topology that distributes risk and facilitates equitable interconnection. This would also follow extant trends as the network becomes more diverse and “meshed” (Faidherbe et al., 2021, p. 61). It also highlights the misalignment of interests between private and public actors, which differently value profitability and communications security.

U.S. actors remain central to shaping the cable network through unilateral investment, global partnerships, and far-reaching governance. American hyperscalers—Google, Facebook, and Amazon Web Services—are central among these, as are American partnerships like the Trilateral Partnership for Investment in the Indo-Pacific and Five Eyes alliance. American governance, including FCC licensing patterns, have proven influential in both the Caribbean and South China Sea by limiting cable landings at “insecure” states. However, the U.S. is far from the only actor in this sphere; China increasingly asserts itself into the global development and surveillance of communications infrastructure (Burdette, 2021).

Contrary to its initial categorization, Brazil’s cable network is less “developing” than initially imagined. Instead, it is both unchanging and exceptionally robust among its neighbors. Brazil may become a model for South-South cable connections, especially as African networks grow. The economic lifespan of cables means that generational change in network topology is slow. Nevertheless, the development of submarine cables in the far North and Global South may lead to a redistribution of data flows from a concentrated middle. These emerging topologies are uniquely able to learn from the risks and vulnerabilities that characterize some established regions. Although capital-intensive, early investment in diversification may trade short term financial benefits for long term resilience that limits the development of chokepoints. Global hyperscalers and cloud companies may take this perspective on network topologies, becoming well-funded developers able to both bear the cost of diverse cable systems and benefit from their development.

Based on qualitative indicators explored here, ongoing work is operationalizing some of these indicators to more effectively evaluate risk indicators, further validate known risks and vulnerabilities, identify less obvious topological factors that may create risks and vulnerabilities, and evaluate possible scenarios in regions with emerging demand for improved cable topologies. Additional cases will explore low diversity regions that may see new topologies in coming years. Prospective cases include South Africa, the Indian Ocean, and the Western coast of South America. As the technological and economic landscape shifts, these markets in the Global South, like those in the Arctic, may benefit from tools to navigate new stages of development and avoid the pitfalls which create local vulnerabilities.

References

2021 Annual Report to Congress: Executive Summary and Recommendations. (2021). U.S.-China Economic and Security Review Commission. https://www.uscc.gov/sites/default/files/2021-11/2021_Executive_Summary.pdf

Agrawal, P. (2021, December 7). Subsea cable builds will strangle data center demand in emerging Asia. *Data Center Dynamics*. https://www.datacenterdynamics.com/en/opinions/subsea-cable-builds-will-strangle-data-center-demand-in-emerging-asia/

Alley, A. (2020, July 28). Chile's Transoceanic Cable to connect to New Zealand and Australia. *Data Center Dynamics*. https://www.datacenterdynamics.com/en/news/chiles-transoceanic-cable-connect-new-zealand-and-australia/

Angwin, J., Savage, C., Larson, J., Moltke, H., Poitras, L., & Risen, J. (2015, August 15). AT&T Helped U.S. Spy on Internet on a Vast Scale. *The New York Times*. https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html

Ashmore, L. (2021, October 13). China and the "Asia-South American Digial Door. *The Diplomat*. https://thediplomat.com/2021/10/china-and-the-asia-south-america-digital-door/

BBC News. (2013, January 21). *"Curious" Cuban net cable has activated, researchers say*. https://www.bbc.com/news/technology-21120786

BBC News. (2022, January 19). *Tonga undersea cable needs "at least" four weeks to repair: NZ*. https://www.bbc.com/news/world-asia-60034179

Blackwill, R. D., Cohen, J. A., & Economy, E. C. (2021, December 15). *Territorial Disputes in the South China Sea*. Council on Foreign Relations. https://cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

Bnamericas. (2021, May 14). *South America embraces Chile's trans-Pacific cable project*. https://www.bnamericas.com/en/news/south-america-embraces-chiles-trans-pacific-cable-project

Borunda, A. (2018, July 18). *The Internet Is Drowning*. National Geographic. https://www.nationalgeographic.co.uk/science-and-technology/2018/07/internet-drowning

Brake, D. (2019). *Submarine Cables: Critical Infrastructure for Global Communications*. Information Technology & Innovation Foundation. https://www2.itif.org/2019-submarine-cables.pdf

Brazil joins Chile in building first fiber optic cable to connect S. America and Asia. (2021, May 13). *Reuters*. https://www.reuters.com/world/americas/brazil-joins-chile-building-first-fiber-optic-cable-connect-s-america-asia-2021-05-13/

Browning, N., Krisetya, M., Lairson, L., & Mauldin, A. (2012). *Submarine Cable Map* [Map]. TeleGeography. https://submarine-cable-map-2012.telegeography.com/

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, *0*(0), 1–23. https://doi.org/10.1080/13523260.2021.1907129

Burdette, L. (2021). Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese

Strategy. *Journal of Public and International Affairs*, *32*. https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy

Burnett, D., Davenport, T., & Beckman, R. (2013). Why Submarine Cables? In *Submarine Cables: The Handbook of Law and Policy*. Martinus Nijhoff.

CanArctic Inuit Networks. (2021, January 5). CanArctic Inuit Networks' SednaLink Fibre to eliminate Nunavut and Nunatsiavut Connectivity Crisis by November 2022. *Submarine Telecoms Forum*. https://subtelforum.com/fibre-optic-network-between-iqaluit-nu-and-clarenville-nl-which-will-dramatically-improve-connectivity-in-to-inuit-nunangat-by-november-2022/

Carr, A. (2019, October 8). The Billion-Dollar High-Speed Internet Scan. *Bloomberg Businessweek*. https://www.bloomberg.com/news/features/2019-10-08/quintillion-ceo-s-promise-to-wire-the-arctic-was-1-billion-scam

Carter, L., Burnett, D., Drew, S., Marle, G., Hagadorn, L., Barlett-McNeil, D., & Irvine, N. (2009). *Submarine cables and the oceans: Connecting the world* (No. 31; Biodiversity Series). UNEP-WCMC/ICPC. https://www.unep-wcmc.org/system/dataset_file_fields/files/000/000/118/original/ICPC_UNEP_Cables.pdf?1398680911

Cayman News Service. (2020, August 31). *Third undersea cable pointless, says C&W*. https://caymannewsservice.com/2020/08/third-undersea-cable-pointless-says-cw/

Chapman, B. (2021). Undersea Cables: The Ultimate Geopolitical Chokepoint. *FORCES Initiative: Strategy, Security, and Social Systems*, 46.

Chard, I. (2014, March 12). Ahead of the Curve: Caribbean telecoms comes full circle. *Capacity Media*. https://www.capacitymedia.com/articles/3318441/AHEAD-OF-THE-CURVE-Caribbean-telecoms-comes-full-circle

Clarke, L. (2021, August 19). Geopolitical tensions over subsea cables may have big implications for internet infrastructure. *Tech Monitor*. https://techmonitor.ai/policy/geopolitics-of-submarine-cables-us-china-facebook

Cochrane, P. (2021, March 4). Red Sea cables: How UK and US spy agencies listen to the Middle East. *Middle East Eye*. http://www.middleeasteye.net/news/red-sea-cables-how-us-uk-spy-agencies-listen-middle-east

Crowley, M. (2013, October 31). Spies Like Us: Friends Always Spy on Friends. *Time*. https://swampland.time.com/2013/10/31/friends-always-spy-on-friends/

Dawn-Hiscox, T. (2018, December 17). *Cabo Verde Telecom to invest in EllaLink submarine cable*. https://www.datacenterdynamics.com/en/news/cabo-verde-telecom-invest-ellalink-submarine-cable/

DeGeorge, K. (2021, December 22). A new Arctic fiber project aims to link Asia and Europe via the Northwest Passage. *ArcticToday*. https://www.arctictoday.com/a-new-arctic-fiber-projects-aims-to-link-asia-and-europe-via-the-northwest-passage/

Dorling, P. (2013, December 5). Forget the needle, take the haystack. *The Sydney Morning Herald*.

https://www.smh.com.au/technology/forget-the-needle-take-the-haystack-20131206-2yudy.html

Emmott, R. (2014, February 24). Brazil, Europe plan undersea cable to skirt U.S. spying. *Reuters*. https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224

Faidherbe, P., Campagne, L., Krebs, G., & Devos, J. (2021, January). Submarine Cable Hubs Around the World. *Submarine Telecoms Forum*, *116*, 58–61.

FitzGerald, D. (2015, August 12). Attacks on Fiber Networks in California Baffle FBI. *Wall Street Journal*. https://www.wsj.com/articles/attacks-on-fiber-networks-in-california-baffle-fbi-1439417515

Fonseca-Hoeve, B., Marius, M., Osepa, S., Coffin, J., & Kende, M. (2017). *Unleashing the Internet in the Caribbean: Removing Barriers to Connectivity and Stimulating Better Access in the Region* (p. 71). Internet Society.

Fromageot, H. (1924). Case of the Cuba Submarine Telegraph Company, Limited (Claim No.27). *American Journal of International Law*, *18*(4), 842–844. https://doi.org/10.2307/2188863

Gelpern, A., Horn, S., Morris, S., Parks, B., & Trebesch, C. (2021). *How China Lends: A Rare Look into 100 Debt Contracts with Foreign Governments*. Peterson Institute for International Economics, Kiel Institute for the World Economy, Center for Global Development, and AidData at William & Mary. https://www.ssrn.com/abstract=3840991

Gerlach, C., & Seitz, R. (2013). *Economic Impact of Submarine Cable Disruptions*. APEC Policy Support Unit. https://www.apec.org/Publications/2013/02/Economic-Impact-of-Submarine-Cable-Disruptions

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

Gorman, L. (2020, January 5). 5G Is Where China and the West Finally Diverge. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2020/01/5g-where-china-and-west-finally-diverge/604309/

Hasler, J. (2019, March 13). Huawei is better positioned to spy on us than we think. *Washington Post*. https://www.washingtonpost.com/politics/2019/03/13/huawei-is-better-positioned-spy-us-than-we-think/

Hinck, G. (2018, March 5). Evaluating the Russian Threat to Undersea Cables. *Lawfare*. https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables

Hurley, J., Morris, S., & Portelance, G. (2018). *CGD Policy Paper 121: Examining the debt implications of the Belt and Road Initiative from a policy perspective*. Center for Global Development. https://www.cgdev.org/sites/default/files/examining-debt-implications-belt-and-road-initiative-policy-perspective.pdf

ICPC. (2015). *Sharks are not the Nemesis of the Internet—ICPC Findings*. International Cable Protection Committee. https://cdn.arstechnica.net/wp-content/uploads/2015/07/ICPC-sharks.pdf

Investable Universe. (2020, October 30). *Big Micronesian submarine cable gets support from high places*.

https://investableuniverse.com/2020/10/30/palau-trilateral-infrastructure-partnership-us-japan-australia-cable/

ITU. (2021). *Percentage of Individuals using the Internet*. International Telecommunications Union. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Jensen, M., & Minges, M. (2017). *Ensuring Sustainable Connectivity in Small Island Developing States* (p. 140). Internet Society.

Judge, P. (2021, May 25). *China to push ahead with commercial underwater data centers in Hainan, 100 promised*. https://www.datacenterdynamics.com/en/news/china-to-push-ahead-with-commercial-underwater-data-centers-in-hainan-100-promised/

Kono, K. (2019). *Strategic importance of, and dependence on, undersea cables* (H. Beckvard, Ed.). The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf

Lairson, L., Krisetya, M., Mauldin, A., & Hull, J. (2021). *Submarine Cable Map 2021* [Map]. TeleGeography. https://submarine-cable-map-2021.telegeography.com/

Lee, S. (2016, January 8). International Reactions to U.S. Cybersecurity Policy: The BRICS undersea cable. *The Henry M. Jackson School of International Studies*. https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/

LoGiurato, B. (2013, October 24). *Former French Foreign Minister Nails It On The Outrage Over US Spying On Foreign Leaders*. Business Insider. https://www.businessinsider.com/nsa-spying-outrage-merkel-germany-obama-france-hollande-2013-10

Long, D. (2020, June 8). China Works On Undersea Cables Between Paracel Island Outposts. *Radio Free Asia*. https://www.rfa.org/english/news/china/undersea-paracels-06082020190921.html

Manatua Consortium. (2020). *All Systems Go: Manatua Consortium Confirms One Polynesia Fibre Cable Ready to Light Up the South Pacific*. Manatua Consortium. https://www.subcom.com/documents/2020/Manatua_RFS_FINAL_22JULY2020.pdf

Martinage, R. (2015, October 26). Under the Sea: The Vulnerability of the Commons. *Foreign Affairs*, *Jan/Feb 2015*. https://www.foreignaffairs.com/articles/commons/under-sea

Matley, H. E. (2019). Closing the gaps in the regulation of submarine cables: Lessons from the Australian experience. *Australian Journal of Maritime & Ocean Affairs*, *11*(3), 165–184. https://doi.org/10.1080/18366503.2019.1653740

Matsakis, L. (2018, January 5). What Would Really Happen If Russia Attacked Undersea Internet Cables. *Wired*. https://www.wired.com/story/russia-undersea-internet-cables/

Meaker, M. (2022, July 1). Facebook’s Data Center Plans Rile Residents in the Netherlands. *Wired UK*. https://www.wired.co.uk/article/facebook-dutch-data-center

Morel, C. (2016). Threats beneath the seas: Vulnerabilities in the global cable network (E. Mandley, Trans.). *Hérodote*, *163*(4).

Moss, S. (2021, March 23). *UK’s Royal Navy to build new surveillance ship to “protect” submarine cables*. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/uks-royal-navy-build-new-surveillance-ship-protect-submarine-cables/

Navy Lookout. (2021, March 10). *The threat to world’s communications backbone – the vulnerability of undersea cables*. https://www.navylookout.com/the-threat-to-worlds-communications-backbone-the-vulner ability-of-undersea-cables/

Pfeiffer, T., & Khrennikov, I. (2019, September 12). Melting Arctic Means New Undersea Cables for High-Speed Traders. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-09-12/global-warming-gives-traders-and-google-an-arctic-speed-lane

Portman, R., & Carper, T. (2020). *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers* (p. 104) [Staff Report]. United States Senate Permanent Subcommittee on Investigations. https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf

Public-Private Analytic Exchange Program. (2017). *Threats to Undersea Cable Communications*. U.S. Office of the Director of National Intelligence. https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf

Qiu, W. (2021a, March 29). *Australian AIFFP Signs Loan Agreement for Palau Cable 2*. Submarine Cable Networks. https://www.submarinenetworks.com/en/systems/trans-pacific/palau-cable-2/australian-aiffp-signs-loan-agreement-for-palau-cable-2

Qiu, W. (2021b, August 13). Russia Builds Polar Express Subsea Cable along Arctic Coastline—Submarine Networks. *Submarine Cable Networks*. https://www.submarinenetworks.com/en/systems/asia-europe-africa/polar-express/russia-builds-polar-express-subsea-cable-along-arctic-coastline

Quarless, D. (2015). *A new era in Caribbean telecommunications*. Economic Commission for Latin America and the Caribbean. https://www.cepal.org/en/notas/new-era-caribbean-telecommunications

Radovanovic, A. (2020, April 22). *Our data centers now work harder when the sun shines and wind blows*. Google. https://blog.google/inside-google/infrastructure/data-centers-work-harder-sun-shines-wind-blows/

Reevely, D. (2022, January 6). *Laying fibre into the far Canadian North, with help from Norway*. The Logic. https://thelogic.co/news/the-big-read/laying-fibre-into-the-far-canadian-north-with-help-from-norway/

Sanger, D. E., & Schmitt, E. (2015, October 25). Russian Ships Near Data Cables Are Too Close for U.S. Comfort. *The New York Times*. https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html

Schreiner, G. A. (1924). *Cables and Wireless and Their Role in the Foreign Relations of the United States*. The Stratford Co.

Scully, E. (2021, November 12). Norwegian surveillance which can detect submarines has cables cut. *Daily Mail*. https://www.dailymail.co.uk/news/article-10196799/Norwegian-undersea-surveillance-network-capable-detecting-submarines-cables-cut.html

Sechrist, M. (2010). *Cyberspace in Deep Water: Protecting Undersea Communication Cables by Creating an International Public-Private Partnership*. Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/files/publication/PAE_final_draft_-_04301

0.pdf

Staalesen, A. (2021, May 31). Megafon halts trans-Arctic cable project Arctic Connect. *ArcticToday*. https://www.arctictoday.com/megafon-halts-trans-arctic-cable-project-arctic-connect/

Starosielski, N. (2015). *The undersea network*. Duke University Press.

Starosielski, N. (2018). Strangling the Internet. *Limn*, *10*. https://limn.it/articles/strangling-the-internet/

Stolyarov, G. (2021, August 6). Russia starts operation to lay undersea fibre optic cable through Arctic. *Reuters*. https://www.reuters.com/technology/russia-starts-operation-lay-undersea-fibre-optic-cable-through-arctic-2021-08-06/

Stronge, T., & Mauldin, A. (2016, April). *Mythbusters: Revenge of the Cable Myths, Part I.* SubOptic 2016 Conference. https://blog.telegeography.com/mythbusters-revenge-of-the-cable-myths-part-i

Submarine Cable Networks. (2022). *ARCOS-1*. https://www.submarinenetworks.com/en/systems/brazil-us/arcos-1

Submarine Telecoms Forum. (2021). *Industry Report. 10*.

Sunak, R. (2017). *Undersea Cables: Indispensable, insecure*. Policy Exchange.

Sutton, H. I. (2019, November 10). Russia's Suspected Internet Cable Spy Ship Appears Off Americas. *Forbes*. https://www.forbes.com/sites/hisutton/2019/11/10/russias-suspected-internet-cable-spy-ship-appears-off-americas/

Sutton, H. I. (2021, June 29). Russia's New Super Submarine, Belgorod (K-329). *Covert Shores*. http://www.hisutton.com/Belgorod-Class-Submarine.html

Swimhoe, D. (2022, January 27). Singapore enters pilot phase to restart data center development; will accept some new applications. *Data Center Dynamics*. https://www.datacenterdynamics.com/en/news/singapore-enters-pilot-phase-to-restart-data-center-development-will-accept-some-new-applications/

TechCentral. (2020, May 14). *Facebook-backed Africa mega cable will cost R18-billion*. https://techcentral.co.za/facebook-backed-africa-mega-cable-will-cost-r18-billion/175982/

TeleGeography. (2020, September 11). Cable Compendium: A guide to the week's submarine and terrestrial developments. *Comms Update*. https://www.commsupdate.com/articles/2020/09/11/cable-compendium-a-guide-to-the-weeks-submarine-and-terrestrial-developments/

TeleGeography. (2022). *Submarine Cable Map*. https://www.submarinecablemap.com/

Telehouse. (2017, April 28). *Telehouse Green: Making the Move to Colder Climates*. https://www.telehouse.com/making-the-move-to-cooler-climates/

The World Bank. (2021). *Palau*. https://data.worldbank.org/country/palau

Thorat, D. (2019). Colonial Topographies of Internet Infrastructure: The Sedimented and Linked Networks of the Telegraph and Submarine Fiber Optic Internet. *South Asian Review*, *40*(3), 252–267. https://doi.org/10.1080/02759527.2019.1599563

Tibbles, J. (2021, January). Politics or Planning: Which is Shaping the Network of the Future? *Submarine Telecoms Forum*, *116*, 38–40.

Tranter, E. (2020, December 23). *Company plans to build $107M fibre-optic cable from Newfoundland to Nunavut*. CTV News.

https://www.ctvnews.ca/business/company-plans-to-build-107m-fibre-optic-cable-from-newfoundland-to-nunavut-1.5243445

True North Global Networks. (2021). *Far North Digital/True North Global Networks Sign MoU with Cinia for Pan-Arctic Fibre Cable*. https://www.arctictoday.com/wp-content/uploads/2021/12/FILE_0679.pdf

U.S. Coast Guard. (2017). *Major Icebreakers of the World*. Office of Waterways and Ocean Policy. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Office%20of%20Waterways%20and%20Ocean%20Policy/20170501%20major%20icebreaker%20chart.pdf?ver=2017-06-08-091723-907

U.S. DFC. (2018, July 30). *US-Japan-Australia Announce Trilateral Partnership for Indo-Pacific Infrastructure Investment*. U.S. International Development Finance Corporation. https://www.dfc.gov/media/opic-press-releases/us-japan-australia-announce-trilateral-partnership-indo-pacific#

U.S. DFC. (2019, November 4). *The Launch of Multi-Stakeholder Blue Dot Network*. U.S. International Development Finance Corporation. https://www.dfc.gov/media/opic-press-releases/launch-multi-stakeholder-blue-dot-network

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

U.S. FCC. (2016). *FCC International Bureau Removes Cuba from the Exclusion List*. U.S. Federal Communications Commission. https://www.commlawmonitor.com/wp-content/uploads/sites/811/2016/02/FCC-Cuba-Exclusion-List-Removal-PN.pdf

U.S. FCC. (2020). *Public Notice* (SCL-00290NS). U.S. Federal Communications Commission.

Wikimedia Foundation v. National Security Agency/Central Security Service, No. 20-1191 (United States Court of Appeals for the Fourth Circuit September 15, 2021). https://www.ca4.uscourts.gov/opinions/201191.P.pdf

Winseck, D., & Pike, R. (2007). *Communication and Empire: Media, Markets, and Globalization, 1860–1930*. Duke University Press.

Xu, C., Chen, J., Yan, D., & Ji, J. (2016). Review of Underwater Cable Shape Detection. *Journal of Atmospheric and Oceanic Technology*, *33*(3), 597–606. https://doi.org/10.1175/JTECH-D-15-0112.1