

Purdue University

Purdue e-Pubs

---

FORCES Initiative: Strategy, Security, and Social  
Systems

College of Liberal Arts

---

12-13-2021

## Undersea Cables: The Ultimate Geopolitical Chokepoint

Bert Chapman

*Purdue University*, chapmanb@purdue.edu

Follow this and additional works at: <https://docs.lib.purdue.edu/forces>



Part of the Admiralty Commons, American Politics Commons, American Studies Commons, Asian Studies Commons, Civil and Environmental Engineering Commons, Comparative and Foreign Law Commons, Comparative Politics Commons, Defense and Security Studies Commons, E-Commerce Commons, Economics Commons, Emergency and Disaster Management Commons, Environmental Policy Commons, Environmental Studies Commons, History Commons, Human Geography Commons, Infrastructure Commons, International and Intercultural Communication Commons, International Business Commons, International Law Commons, International Relations Commons, Law of the Sea Commons, Legal History Commons, Legislation Commons, Library and Information Science Commons, Military and Veterans Studies Commons, Military, War, and Peace Commons, National Security Law Commons, Operations and Supply Chain Management Commons, Peace and Conflict Studies Commons, Public Administration Commons, Public Affairs Commons, Public Policy Commons, Science and Technology Studies Commons, and the Transnational Law Commons

---

### Recommended Citation

Chapman, Bert, "Undersea Cables: The Ultimate Geopolitical Chokepoint" (2021). *FORCES Initiative: Strategy, Security, and Social Systems*. Paper 1.  
<https://docs.lib.purdue.edu/forces/1>

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact [epubs@purdue.edu](mailto:epubs@purdue.edu) for additional information.

# Undersea Cables: The Ultimate Geopolitical Chokepoint

December 2021  
The FORCES Initiative



---

# The FORCES Initiative

BRNG 1240

College of Liberal Arts

Purdue University

West Lafayette, IN 47907

765 494 3666

**[forces@purdue.edu](mailto:forces@purdue.edu)**

**<http://purdue.university/forces>**

---

## EDITORIAL TEAM

Professor Bert Chapman

Purdue University Libraries

[chapmanb@purdue.edu](mailto:chapmanb@purdue.edu)

## ✓ ACKNOWLEDGEMENTS

The author wishes to thank Ann O'Donnell for her editorial assistance and David Zwicky for his assistance on patent searching.

# EXECUTIVE SUMMARY

---

Countries globally are heavily dependent on undersea communication cables which are run by commercial companies and tend to be neglected by national governments.

- ▶ **97% of global communications** are transmitted via these cables which are part of a network of an estimated 212 cable systems containing 750,000 miles of fiber.
- ▶ **Satellite technology** is unable to handle modern digital economic and societal requirements.
- ▶ Individual days may see **\$10 trillion in financial transfers** by these cables and 15 trillion financial transactions processed.
- ▶ **Undersea cables are also imperative for aviation and industries using cloud computing and artificial intelligence.**
- ▶ **Repairing these cables is a complicated process** requiring determining the location of the break using a built-in monitoring system, the owner contacting cable repair sites to assess damage, time needed to repair damage may range from hours or days with the average global repair time being 27 days in 2019.
- ▶ In early August 2019, **India shut down Internet and phone service** in Jammu and Kashmir to deter opposition to legislation changing the status of these disputed regions.
- ▶ **Within eleven days of this shutdown, shopkeepers were running short on vital supplies** such as baby food and insulin which were usually ordered online while also creating cash shortages and the inability to process credit.
- ▶ Rupturing such lines **globally would produce cascading failures** immobilizing much of the international communications system and Internet for several weeks. Affected areas would include international finance, military logistics, medicine, commerce, agriculture, energy flows, food supply deliveries, and potentially produce a global depression.

These scenarios makes it imperative that the U.S. and its allies, and other international actors, enhance measures to ensure the security of undersea cables and severely punish those who would damage or destroy these critical infrastructures. This work strives to enhance awareness of the vital economic and national security significance of these critical infrastructures and makes recommendations to ensure their security and reliability against potential attempts by hostile powers like China and Russia or other national, transnational, and subnational entities to take steps to sabotage and destroy these cables with ruinous consequences for personal and international economics and security.<sup>1</sup>

*It is not the taking of individual ships or convoys...that strike down the money power of a nation; it is the possession of that overbearing power on the sea, which drives the enemy's flag from it, or allows it to appear only as a fugitive...by controlling the great common, closes the highways by which commerce moves to and from the enemy's shores.<sup>2</sup>*

Alfred Thayer Mahan

# OVERVIEW AND HISTORICAL INTRODUCTION

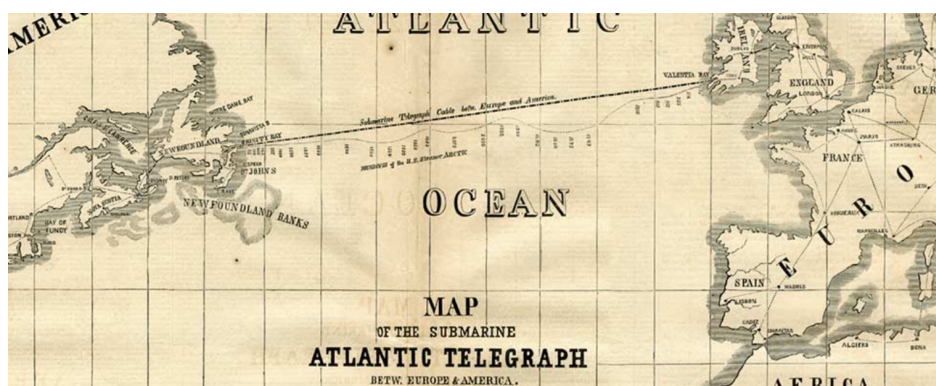
This work provides historical and contemporary overviews of this critical geopolitical problem, describes the policy actors addressing this in the U.S. and selected other countries, and provides maps and information on many undersea cable work routes. These cables are chokepoints with one dictionary choke points as “a strategic narrow route providing passage through or to another region.”<sup>3</sup>

## FIRST TRANSOCEANIC CABLE LINE

Contemporary submarine cables began on July 29, 1858 when the HMS Agamemmon and USS Niagara met in the middle of the Atlantic Ocean joining over 1,000 miles of copper cable by lowering it to the sea floor and completing the world’s first Trans-Atlantic cable stretching from Ireland to Newfoundland. Queen Victoria and President James Buchanan exchanged telegrams on August 16, 1858 and their combined messages of less than 100 words,

took 17 hours and 40 minutes to transmit representing the fastest message ever sent between Washington and London. Despite the involvement of U.S. and Royal Navy ships, this was a private sector owned and financed endeavor owned and financed by the Atlantic Telegraph Company created by New York businessman Cyrus West Field (1819-1892).<sup>4</sup>

FIGURE 1: 1858 ATLANTIC SUBMARINE CABLE MAP



Source: Frank Leslie’s Illustrated Newspaper<sup>5</sup>

Development of undersea cables would play a major role in enabling the British Empire to administer its dispersed dominions and respond to strategic contingencies<sup>6</sup> An 1859 U.S. State Department report on international commerce contains ample documentation of the economic significance of submarine cables in the United Kingdom and other countries.<sup>7</sup> In 1884, the Convention for the Protection of Submarine Cables was signed by 40 different countries establishing the precedent that, "The breaking or injury of a submarine cable, done willfully or through culpable negligence, and resulting in the total or partial interruption or embarrassment of telegraphic communication, shall be a punishable offense, but the punishment inflicted shall be no bar to a civil action for damages."<sup>8</sup> Evidence of the increasing importance of undersea cables in British imperial policymaking was reflected in the 1885 Submarine Telegraph Act, which imposed a maximum criminal penalty of five years imprisonment for anyone intentionally attempting to break or injure an undersea cable and up to three months imprisonment and a maximum fine of £100 (\$486) (\$14,300 in 2021) if these cables were damaged by culpable negligence.<sup>9</sup>

The 1958 Geneva Convention on High Seas enacted the legal principle that nation states could not obstruct undersea cable construction in international waters in Articles 2 and 26.<sup>10</sup> The 1982 United Nations Convention on the Law of the Sea (UNCLOS) aspires to be the preeminent international legal instrument on oceans.

It consists of 167 members and Articles 112-115 cover undersea cables. Article 112 says countries are entitled to lay such cables and pipelines on the bed of high seas beyond the continental shelf. Article 113 enables countries to enact laws criminalizing the breaking of undersea cables by vessels of their own countries, but does not give warships the right to board vessels suspected of intentionally attempting to damage undersea cables in international waters, making it difficult for naval powers to deter hostile vessels from such activity. Article 114 allows each country whose cables or pipelines are broken to compel the perpetrator to pay repair costs and Article 115 gives countries authority to adopt laws and regulations to sacrifice anchors or fishing gear to avoid injuring cables to be indemnified if they take all reasonable precautionary measures. UNCLOS provisions also fail to account for the emergence of fiber optical cables in the late 1980s, which have become predominant over satellites in international cable transmission. During 2012 congressional testimony, the U.S. Chamber of Commerce noted that satellites could carry no more than 7% of U.S. voice and data traffic further illustrating the critical importance of undersea cables in international economic, legal, and strategic policymaking.<sup>11</sup>

The United States is one country which has not ratified UNCLOS despite efforts of presidential administrations of both parties and some elements within Congress and international affairs organizations to achieve this goal. Understandable reasons for U.S. refusal to

ratify UNCLOS include U.S. membership not providing maritime rights or freedoms the U.S. already enjoys and that maintaining a strong U.S. Navy is the best way for the U.S. to maintain its rights. The U.S. already has a legal framework through domestic law and bilateral agreements for deep seabed mining and should not subject U.S. companies to the edicts of an unaccountable international bureaucracy forcing them to pay excessive fees to the International Seabed Authority for redistribution to developing countries. The U.S. is a sovereign nation and does not need an UN-based commission's approval to access gas and oil resources in the U.S. continental shelf. Royalties the U.S. retains for natural resource extraction should only be used to benefit the American public; resources the U.S. needs to access on its extended continental shelf can be negotiated through bilateral treaties with adjacent countries. Acceding to UNCLOS would expose the U.S. to climate change lawsuits and other litigation brought by UNCLOS members, which would harm U.S. economic, environmental, and military interests; and the U.S. has successfully defended its Arctic interests since acquiring Alaska in 1867 and since UNCLOS' establishment. The U.S. gains nothing from ratifying UNCLOS.<sup>12</sup>

## **TECHNOLOGIES INVOLVED INCLUDING PATENTS**

Before discussing geopolitical implications of undersea cables, it is helpful to look at the multiple technological factors involved in creating this network covering

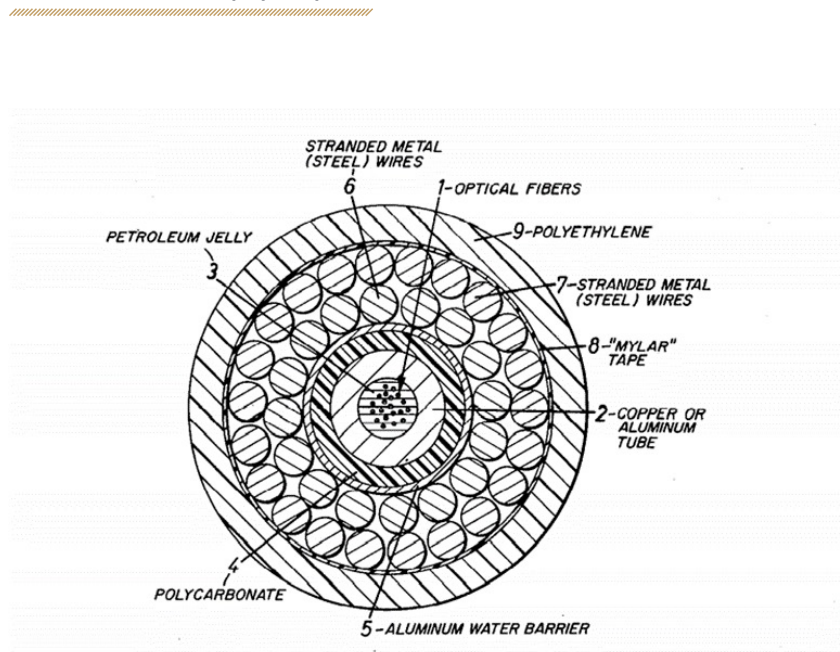
the world's circumference. Installing these cables is a highly professional skill requiring technologies such as automatic control, communication, and navigation. Required equipment for submarine cable installation includes a cable ship, jointing and testing equipment, and underwater installation equipment. Cable ship infrastructure includes drum cable machines, linear cable machines for laying cable, submarine optical cable storage tanks, professional installation machines, and control management software. During the 1960s and 1970s submarine coaxial communication cable development into the main methods of transoceanic communication. Submarine cable curvature radius usually exceeds one meter and a radius of 1.5 meters is required to ensure submarine communication cable and repeater safety between the pulley group design and ship stern during the laying process.<sup>13</sup>

Submarine optical cable technology has experienced exponential development in subsequent decades including reaching weights of over 10,000 tons, using drum-type and linear machine laying equipment. Making greater use of Internet technology to facilitate installation and remote management, using burial machines weighing between 5-15 tons to bury cables one meter below the ocean floor, and the increasing use of remote operating vehicles to carry out cable installation. This technological development has resulted in increased interconnectivity, which can be susceptible to physical and cyber-attacks.<sup>14</sup>

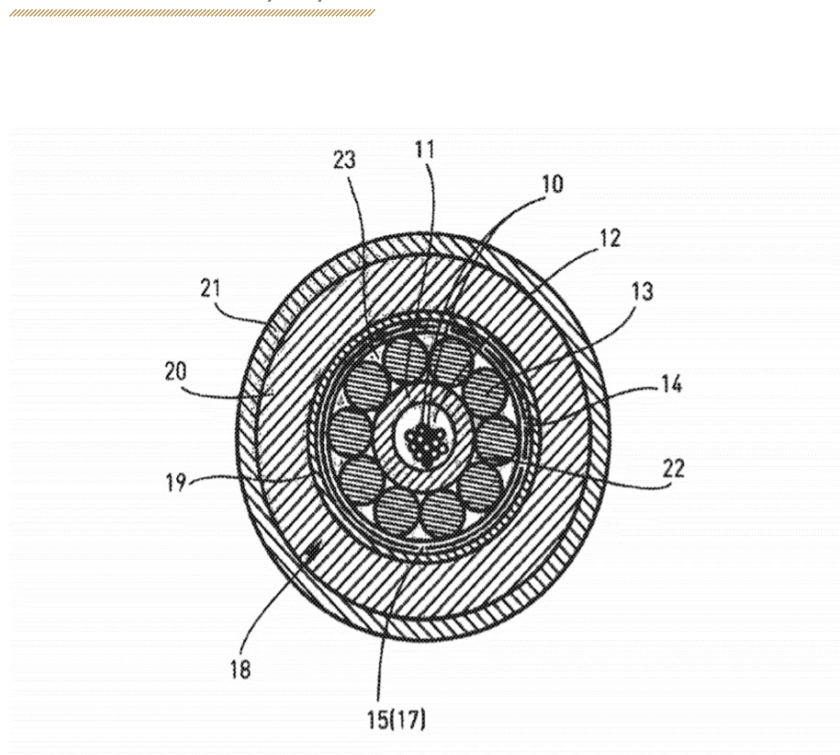


The following pictures of patents and photographs of undersea cables document their physical appearance and illustrate the factors involved in installing these objects globally.

**FIGURE 2: PATENT, 4,278,835**



**FIGURE 3: PATENT 10,481,356**



## ORGANIZATION OF UNDERSEA CABLES

Undersea cables are produced and owned by private companies representing individual countries, multinational consortia, and some national governments. These cables transmit most international voice and data traffic including military, government, emergency response, air traffic, subway, rail, and port traffic. Stephen Malphrus, a former Chief of Staff to former Federal Reserve Chair Ben Bernanke noted, "When communication networks go down, the financial service sector does not grind to a halt, rather it snaps to a halt." These cables are part of a global network containing 750,000 miles of fiber and recent destruction of cables has had international repercussions. There have been exponential increases in the speed of these over 160 years with a 2019 transatlantic transfer by the company Infinera achieving a speed of 2.62 terabits per second or 4.8 million high definition movies simultaneously. Cables cost \$200-\$500 million to build with some cables being on top of the ocean floor in deep seas, those crossing shallower continental shelf waters are armored and buried one to two meters below the seafloor to protect them from damaging activities.<sup>17</sup>

Recent years have seen natural and human caused events result in temporary disruption of undersea cables. On December 26, 2006, a series of earthquakes off Taiwan's southwest coast produced undersea landslides in the Luzon Strait severing six of seven undersea cables

distributing Internet and phone services from North America to Taiwan, China, Hong Kong, Singapore, and South Korea. Taiwan's largest telecommunications operator Chungwa Telecom reported 100% Internet outage to Hong Kong and Southeast Asia, trading of the Korean won halted in Seoul, 80% of Hong Kong's communications capacity was wiped out in minutes, and Asia's most important financial center had to rely on a SINGLE cable to transfer billions of dollars in trades and transfers globally. It took 11 ships 49 days to finish repairs.<sup>18</sup>

Another example of disruption to undersea cables and its civil and military implications was reflected by the inadvertent December 2008 cutting of three undersea cables connecting Italy and Egypt. This knocked out 80% of connectivity between Europe and the Middle East. Pakistan lost 70% of its Internet connectivity and India lost between 50-60% of its westbound connectivity. This was particularly problematic for the U.S. and British militaries, which had 200,000 troops in Iraq at that time and relied on commercial cable networks for 95% of their strategic communications. U.S. Air Force Unmanned Aerial Vehicles (UAVs) were heavily used in counter-terrorism operations in Iraq and Pakistan. These assets are remotely piloted from Europe and the U.S. requiring 500 MBs bandwidth to operate, which cannot be achieved without a strong undersea cable network. Lieutenant Colonel Donald Fielded off the 50th US Communications Squadron stressed that these cable breaks caused UAV flights originating from Iraq's Balad Air Force Base to fall from hundreds of daily

combat sorties to “tens.” During its 2014 conquest of Crimea, Russia made extensive use of hybrid warfare to seize control of the peninsula’s Internet infrastructure, control the information flow, and portray its actions as legitimate. Russian Special Forces only need to secure an Internet exchange point at Simferopol to cut connections to the rest of Ukraine.<sup>19</sup>

# POLICYMAKING & LEGISLATION

## AUSTRALIA AND NEW ZEALAND GOVERNMENT AND POLICY STRUCTURE

Australia and New Zealand are both heavily dependent on undersea cable communication for their economic growth and national security, which carry the preponderance of bulk voice and data traffic in and out of these countries. A 2013 Australian Parliamentary Library study determined nearly \$A 220 billion (\$224.642 billion) in non-cash payments are made each business day using undersea cables representing 20% of Gross Domestic Product. Such factors have made them global leaders in developing legal architecture to protect their continuing access to these critical geopolitical infrastructures. In 2005, the Australian Government establishing a regime for protecting these cables landing in Australia by giving the Australian Communications Authority (now the Australian Communications and Media Authority (ACMA)) power to declare protection zones relating to undersea cables where certain activities may be prohibited, restrictions may be imposed on other activities, and carriers wishing to install undersea cables

in Australian waters must apply and receive permission from ACMA.<sup>20</sup>

A 2013 Australian Strategic Policy Institute (ASPI) study on this subject warned that the majority of these cables are located near protection zones in Perth and Sydney. This makes them vulnerable to accidental or intentional breakage, warned that the Australian Federal Police who is responsible for ensuring compliance with national laws takes a reactive instead of proactive enforcement approach, and that cable company owners and operators say the Australian Safety Authority and Fisheries Management Authority are not doing a good job of monitoring cable protection zones. A Royal Australian Navy Sea Power Center assessment noted cables are vulnerable to accidental damage from earthquakes, fishing trawlers, anchors, dumping, sand dredging, turbidity currents, and espionage by state actors and terrorists.<sup>21</sup>

During 2017/18 ACMA granted permission for installation of an undersea cable connecting Sydney and the United States, which was completed on June 30, 2018; granted two protection zone installation permits to conduct Perth and Singapore; and approved three separate



requests extending the duration of existing protection zone permits.<sup>22</sup> Under current Australian law, the maximum penalties for intentionally interrupting or obstructing submarine communications is 12 months imprisonment and a fine of \$A 4,200 (\$3,226). The maximum penalty for an individual engaging in conduct and being negligent and injuring an undersea vessel as a result of an Australian-flagged vessel breaking or injuring a submarine cable is 3 months imprisonment and a \$A 2,100 (\$1,613) fine. An emerging undersea cable geopolitical matter Canberra will also have to confront is if neighboring countries such as Papua New Guinea and the Solomon Islands decide to adopt Chinese Internet infrastructure unless Australia increases its development to these countries to expand and maintain their undersea cables.<sup>23</sup>

Enforcing violations of undersea cable infrastructure is a problem in national and international law. A 2007 Tulane Maritime Law Journal analysis was skeptical that national governments possessed the legal authority to arrest saboteurs under the United Nations Convention on the Law of the Sea and 2005 Suppression of Unlawful Acts Convention Amendments. This work went on to maintain that the possibility of terrorist attacks against undersea cables and pipelines was not considered by international legal authorities or giving nation states the international legal authority to protect pipelines and undersea cables.<sup>24</sup>

During 2018, the Australian Government enacted the Security of Critical Infrastructure Act, which aspired

to create a legal framework for managing critical infrastructure such as undersea cables. This statute gave the Minister of Home Affairs responsibility for compiling a register of critical infrastructure assets but prohibiting the public disclosure of this register with a criminal penalty two years imprisonment and/ or fine of \$A 26,640 (\$20,463).<sup>25</sup>

The legal foundation for New Zealand's undersea cable protection begins with the 1996 Submarine Cables and Pipeline Protection Act. This established a maximum criminal penalty of NZ \$250,000 (\$178,487) for anyone convicted of willfully or negligently damaging or permitting a ship or equipment to damage a submarine cable or pipeline and owns or operates the ship involved in causing such damage. This statute establishes fourteen Cable Protection Zones (CPZ) where anchoring and most types of fishing are banned to prevent cable damage. These CPZ's are enforced by New Zealand's Ministry of Transport and consist of the following areas with fishing and anchoring in these areas producing the following fines \$NZ 2000 (\$1,427) plus court and legal costs for recreational boat users offenses, \$NZ 100,000 (\$71,334) for fishing and anchoring where commercial gain is involved, and \$NZ 20,000 (\$14,279) in other cases.<sup>26</sup>

## U.S. GOVERNMENT POLICY STRUCTURE

The U.S.' civilian and military undersea cable policymaking structure is byzantine and labyrinthine with many agencies having jurisdictional engagement in this arena. U.S. laws are codified into the United States Code (USC), which is broken down into 54 title or subject areas. A quick online search of the USC using the U.S. House of Representatives Office of Law Revision Counsel website <https://uscode.house.gov/> retrieves relevant citations from 10 of these 54 titles.

- ▶ 3 USC 301 gives the Federal Communications Commission (FCC) authority to approve or revoke licenses to land or operate submarine cables in the U.S. without presidential approval.<sup>27</sup>
  - ▶ 10 USC 113 gives the Secretary of Defense statutory authority to build such cables and pipelines.<sup>28</sup>
  - ▶ 26 USC 168 can allow for undersea cables to be tax-exempt if part of an exclusive communication link between the U.S. and one or more foreign countries.<sup>29</sup>
  - ▶ 33 USC 3 allow the Army Corps of Engineers to prepare regulations on areas of navigable waters featuring such cables to regulate explosives transportation in these waters.<sup>30</sup>
  - ▶ 33 USC 3204 allow the National Oceanic and Atmospheric Administration (NOAA) and the Federal Emergency Management Administration (FEMA) to integrate tsunami warning systems into federal undersea cables.<sup>31</sup>
- This statutory cornucopia continues with 42 USC 9113, which imposes criminal penalties of up to two years, fines of up to \$5,000, or both for negligently breaking of injuring undersea cables.<sup>32</sup>
- ▶ 42 USC 9164 requires the Energy Department and other interested federal agencies and departments to establish and enforce regulations and standards of the safe construction and operation of undersea cables and equipment subject to U.S. jurisdiction.<sup>33</sup>
  - ▶ 43 USC 1331 gives international ships and aircraft navigation and overflight freedoms and the ability to lay undersea cables and pipelines under UNCLOS within the U.S.' contiguous zone.<sup>34</sup>
  - ▶ 47 USC 26 gives military ship commanders to require foreign ship commanders to provide documentation from ships trespassing in areas where U.S. undersea cables are,<sup>35</sup> and
  - ▶ 47 USC 34 prohibits individuals landing or operating in the U.S. from using an undersea cable

to directly or indirectly connect U.S. territory with any foreign country without a written license from the President.<sup>36</sup>

The Commerce Department's National Oceanic and Atmospheric Administration (NOAA) regulates whether and how proposed submarine cables may be installed in National Marine Sanctuaries according to international agreements the U.S. is part of and according to international law. NOAA is authorized to assess fair market value fees along with administrative and monitoring costs involved with the ongoing presence of commercial cables in National Marine Sanctuaries. Additional NOAA cable responsibilities include administering the Coastal Zone Management Act, which seeks to manage coastal resources balancing economic development and environmental conservation. The National Marine Fisheries Service (NMFS) is a trustee for coastal and marine resources including commercial and recreational fisheries, marine mammals, and endangered and threatened species and their habitats, which may be impacted by cable laying operations. NOAA permits are required when underwater cable laying may impact marine mammals, which can include underwater noise and surface and underwater vessel activity.<sup>37</sup>

Several Defense Department (DOD) entities are involved in undersea cable policymaking activities. These include the Naval Seafloor Cable Protection Office (NSCPO). Established in 2000, by Naval Facilities Engineering Command, NSCPO is

the contact point between DOD and Navy seafloor cables. Such cables are used for fleet underwater test and training ranges, sensor systems, communications and data links, and observation and monitoring systems.<sup>38</sup>

The USNS Zeus is the U.S.' only cable laying/repair ship and is responsible for transporting, deploying, repairing, and retrieving undersea cables. It has been in service since 1984 and its contractors were General Dynamics and National Steel & Shipbuilding Corporation. Its length is 513 feet, beam is 73 feet, it displaces 15,174 tons, maximum speed is 14 knots, and its crew size is 58.<sup>39</sup>

The Army Corps of Engineers is authorized to regulate artificial islands, installations, and devices (including cables) on the U.S. outer continental shelf seabed with this authority being focused on how cables can potentially impact navigation and national security along with carrying out National Environmental Policy Act (NEPA) analyses unless another agency has primary authority over the cable permitting process. The Defense Information Systems Agency (DISA) is responsible for securing and enhancing DOD telecommunications networks including the undersea communication constellation. This agency also sponsors research in these areas and awards grants to contractors.<sup>40</sup>

The Energy Department's Federal Energy Regulatory Commission (FERC) possesses some authority over proposed undersea cables to be laid on the U.S. continental shelf. Examples of

such projects include constructing and operating hydrokinetic projects on the Outer Continental Shelf such as wave power generation facilities. Cable laying related to such projects would involve assessing cable environmental impacts along with collaborating with the Army Corps of Engineers on possible national security and navigational impacts.<sup>41</sup>

The Federal Communications Commission (FCC) is responsible for submarine cables landing in the U.S. The 1921 Cable Licensing Act gives the FCC licensing authority covering “any submarine cable directly or indirectly connecting the United States with one foreign country, or connecting one portion of the United States with any other portion thereof.” FCC authorities also include regulating the landing and operating of communication cables laid in U.S. coastal waters with Executive Order 10,530 (May 10, 1954) giving the FCC power to exercise presidential authority to issue, revoke, or withhold licenses to land and operate submarine cables in the U.S. after receiving the Secretary of State’s approval.<sup>42</sup>

This agency’s International Bureau, Telecommunications, and Analysis Division is responsible for issuing licenses to own and operate undersea cables and landing stations in the U.S. and is also responsible for authorizing modifications, transfers, or assignments of existing cable landing licenses. On August 29, 2017 this division of the FCC issued its 2015 International Circuit Capacity Report, which revealed that the total available capacity of U.S. international cables increased from 91,000 gigabit per

second circuits (GPBS) in 2014 to nearly 120,000 GPBS in 2015. It also documented a 35% growth in submarine cable capacity between 2007-2015; with the Atlantic Region accounting for 40% of total available capacity, the Pacific Region for 37%, and the America’s Region for 23%. This document also noted that the top foreign landing points for U.S. submarine cables were Colombia 9, Japan and the United Kingdom 7, Panama 6, Brazil and Venezuela 5, and Australia and Mexico.<sup>43</sup>

Various Department of the Interior agencies may become involved in undersea cable policymaking. The Bureau of Ocean Energy Management (BOEM) derives authority from the 2005 Energy Policy Act to regulate cables supporting energy production, transmission, and transportation from energy sources besides oil and gas from the Outer Continental Shelf and cables laid to construct and maintain oil and gas platforms.<sup>44</sup> Cables operators seeking to build cables through terrestrial or marine areas administered by the National Park Service and U.S. Fish and Wildlife Service go through those agencies approval processes. In addition, the Antiquities Act of 1906 gives the President the authority to protect natural and cultural objects and potentially restrict cable laying through designating properties as national monuments. A relatively recent example of this was President George W. Bush using Antiquities Act authorities to designate the Papahānaumokuākea Marine National Monument in the northwestern Hawaiian Islands on June 15, 2006.<sup>45</sup>



## RECENT U.S. LEGISLATION INCLUDING SUBMARINE CABLE REGISTRY

Undersea cables have received some attention in recent congressional legislation and debate, but they are primarily a niche subject for maritime security cognoscenti instead of being a focal point of international security and international economic analysis and debate. Rep. Rob Wittman (R-VA), a member of the House Armed Services Committee, has written that despite rhetoric about wireless and cloud computing the Internet does not involve invisible waves jumping from earth to space satellites and returning but by cables deep under the ocean's surface. Since these cables are privately owned and maintained anyone with hostile intent and the ability to execute such intent can drastically impact our lives by attacking and destroying these cables. Using historical analogies, Wittman mentioned British destruction of most German undersea cables during World War I and the Soviet Union cutting cables off eastern Canada in 1959. He then noted that while cable laying and repair is easy for wear and tear and incidental damage there is not a clear and robust response plan for responding to intentional attacks on undersea cables.<sup>46</sup>

The Fiscal Year 2020 National Defense Authorization Act (NDAA) of December 20, 2019 saw Congress create a Cable Security Fleet within the Transportation Department's Maritime Administration (MARAD) to consist of two ships subsidized at \$5 million per year through Fiscal Year 2035. Further

conditions of this legislation including giving these vessels operating in areas designated by the Coast Guard as possessing a high risk of piracy to engage in non-lethal defense measures to protect the vessel and crew from unauthorized seizure at sea and that the Defense Department and Coast Guard will determine what non-lethal defense measures these ships and their crew can take.<sup>47</sup>

Despite the enhancement produced by the Cable Security Fleet's creation, the convoluted complexity of U.S. Government Internet security programs was reflected in a September 10, 2019 joint congressional hearing by subcommittees of the House Armed Services and Oversight and Reform Committees on national Internet architecture security. During the hearing, Rep. Michael Waltz (R-FL) asked Department of Homeland Security Assistant Director for Cybersecurity Jeannette Manfra who was responsible for defending undersea cables directly affecting the United States and its abilities to communicate in our economy and international waters. Manfra's response reflects the byzantine complexity, interconnectivity, and dysfunctionality inherent in undersea cable policymaking:

*"The majority of submarine cables are privately owned by a mix of domestic and foreign entities. The protection of these cables is a complex question, considering they travel through domestic and international waters, some of which are contested areas. While the U.S. and its allies have significant interest in ensuring*

*the safety and continued functionality of submarine cables, it will require a “concerted effort” from the United States and its allies to ensure the confidentiality, integrity, and availability of the data that traverses subsea systems, in addition to the physical security of the cable and cable landing station. While DHS is the communications sector-specific agency per PPD-21, the current responsibility for defending undersea cables landing in the United States involves a “whole of government” approach, which includes the Navy in our Exclusive Economic Zone (EEZ) and the Coast Guard within our 12 mile nautical sovereignty zone. Team Telecom— primarily made up of executive branch agencies DOD, DHS, and DOJ—acts as an advisory committee to the FCC in matters related to foreign investment into US domestic communications infrastructure. Letters of Assurance (LOAs) and Network Security Agreements (NSAs) are memorandums of understanding between the USG and the cable owners/operators that govern the location of assets, types of principal equipment, physical access controls, and other relevant factors surrounding the functionality and protection of undersea cable systems. DOD, DHS, and DOJ enforce Team Telecom agreements through periodic compliance and mitigation visits to cable landing sites, network operations centers, and other relevant infrastructure. The Department of Justice and Federal Bureau of Investigation investigate and prosecute criminal acts and espionage-related activities. These activities are informed by reporting from the intelligence community and various other*

*federal agencies.”<sup>48</sup>*

The House Armed Services Committee version of the FY 2022 NDAA passed on September 10, 2021 recognized the increasing importance of undersea warfare by directing the Government Accountability Office (GAO) to provide this committee a briefing on unmanned undersea and surface vehicles by March 1, 2022. Contents of this report were to include the extent to which the Navy has successfully identified all critical technologies necessary for unmanned maritime systems; how the Navy tracks technological development for unmanned maritime systems; and whether unmanned maritime technology systems meet Navy requirement and mission needs. It is uncertain whether this language will be included in the final FY 2022 NDAA.<sup>49</sup>

## INTERNATIONAL ASSOCIATIONS AND ORGANIZATIONS

Various international associations and government organizations also influence undersea cable policymaking. The International Cable Protection Committee, (ICPC) is an intergovernmental and commercial company organization, founded in 1958, whose membership consists of submarine telecommunications and power cable operators and cable ship owners and operators, which strives to help members improve undersea cable security by exchanging relevant environmental, legal, and technical information. ICPC includes more than 170 members from 65 countries.<sup>50</sup>

The United Nations Commission on Law of the Sea (UNCLOS), ratified in 1982 by many countries, but not the U.S., whose objections include surrendering U.S. sovereignty and freedom of action, being subject to international lawsuits that would be economically injurious and harm U.S. environmental and military interests, and have to transfer seabed mineral resource royalties to the International Seabed Authority and though it to corrupt and unaccountable nations.<sup>51</sup>

The International Maritime Organization (IMO) established in 1948 as Inter-Governmental Maritime Consultative Organization, the IMO Convention entered into force in 1958, and IMO received its present name in 1982. IMO describes its purpose as “to provide machinery for cooperation among Governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade; to encourage and facilitate the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation and prevention and control of marine pollution from ships.”<sup>52</sup>

# INFRASTRUCTURE DISRUPTION & DAMAGE

Any country, individual, or transnational terrorist group could seek to damage or destroy undersea cables.

## RUSSIA AND CHINA

Two countries of particular concern to undersea cable infrastructure to the U.S. and its allies include Russia and China. An early example of U.S. concern over Soviet/Russian attempts to destroy undersea cables occurred between February 21-25, 1959 when the Soviet trawler *Novorossiisk* disrupted communications between various U.S., Canadian, and European locales by damaging five transatlantic cables near Newfoundland in a rectangle bounded by the following coordinates: Latitude 49°24 N; Longitude 50°12 W; Latitude 49°32 N; Longitude 49°48 W; Latitude 50°13 N; Longitude 51°00 W; and Latitude 50°22 N; Longitude °50.36 W. In response, at 11:55 AM Eastern Standard Time on February 26, 1959, the commander of the USS *Roy O. Hale*, using his authority under the 1884 Convention for the Protection of Undersea Submarine Cables, sent an unarmed party of one officer and four enlisted men to board the *Novorossiisk* and examining the ship's papers with its commanders consent. The U.S. announced

it reserved the right to make claims for damages against Moscow and the Soviet Union protested against this activity.<sup>53</sup>

U.S. concern over Russian undersea cables continued in the 1970s, when the specially adapted nuclear submarine USN *Halibut* spent several months tapping Soviet communication cables in the Sea of Okhotsk north of Japan as part of Operation Ivy Bells.<sup>54</sup> The current edition of *The Military Balance* notes "the recent focus on the potential vulnerability of the undersea cable network raises issues of how to monitor, identify, and...defend against attacks on these vital information arteries...this and the recent events in the Gulf point to an increased need for persistent surveillance so that hostile activities can be identified, attributed, and tackled."<sup>55</sup>

An October 25, 2015 New York Times article referencing U.S. intelligence and military personnel maintaining that Russia's increasing geopolitical assertiveness could lead it to sever fiber optical cables at hard-to-access locations to halt the instantaneous communications abilities these cables provide with devastating consequences. Earlier in 2015 the Russian spy ship *Yantar*, carrying



two self-propelled deep-sea submersible craft, slowly cruised the U.S. east coast to Cuba the site of a major U.S. cable landing point at Guantánamo Bay. During this journey, Yantar was constantly monitored by U.S. satellites, ships, and planes with naval officials saying the ship and its submersibles were capable of cutting cables miles below the ocean's surface. Such operations are consistent with increasing Russian assertiveness in locales as varied as Crimea, Syria, and eastern Ukraine and reflect Moscow's emphasis on hybrid warfare to cripple NATO decision-making.<sup>56</sup>

Speaking before the Royal United Services Institute (RUSI) on December 14, 2017, British Chief of Defense Staff Air Chief Marshall Stuart Peach, maintained that the threat from Russia's Navy with modernized conventional submarines and ships represents "a new risk to our way of life." A story on this event also noted that retired U.S. Navy Admiral James Stavridis said Internet cables could be a tempting target for the Russians, other powers, and that U.S. and its NATO allies should prepare for increased maritime hybrid activity from China, Iran, and Russia.<sup>57</sup>

Recent evidence also demonstrates Russian efforts to control the Northern Sea Route and gain exclusive access to its seabed mineral resources could also increase this region becoming a focal point for undersea cable conflict. Russia is backing building an extensive 14,000 kilometer/8,680 miles network of fiber optical cables along its northern littoral from Finland to Japan and including

China, which will impact Moscow's relations with the West and Beijing. This project is estimated to cost \$800 million to \$1.2 billion while providing data speeds of up to 200 terabytes per second. The Russian Government and Russian businesses do not currently possess necessary financial capitalization to build this and are seeking foreign investors through Scandinavia, Japanese, and one Russian company in the Arctic Connect consortium. Megafon, the Russian participant in Arctic Connect has close ties with the Russian Federal Security Service (FSB) and Ministry of Defense. This project is expected to be completed by 2023 and would likely give the FSB the ability to monitor and read much data passing between Japan and Europe and incentivize Moscow to covertly install additional undersea cable systems, which could include sensing networks comparable to the Integrated Undersea Surveillance System (IUSS) used by the U.S. Navy to support antisubmarine warfare and tactical forces by detecting, classifying, and providing timely information reporting on submarines and other contacts of interest.<sup>58</sup>

China is also heavily interested in undersea cables and this has been reflected in its business acquisition practices and military force development including deployment of 12 underwater drones in the Indian Ocean between December 2019-February 2020. Chinese tech companies like Huawei Marine Networks have laid 59,499 kilometers/36,488 miles of undersea cables in 98 projects encompassing the Indo-Pacific, South Pacific, and Atlantic regions. These firms

have gone from 7% of undersea cable projects in 2012 to 20% in 2019. New Chinese fiber-optic submarine cables area supplemented by the 33-satellite Beidou Navigation Satellite System seeking to provide an alternative to U.S.-led Global Positioning Satellite and achieving global coverage by 2020. Beidou including Indonesia, Laos, Pakistan, and Thailand covers over 30 Belt and Road Initiative (BRI) countries. China's Digital Silk Road (DSR) also includes the Pakistan and East Africa (PEACE) Cable connecting Pakistan to Kenya with additional extension to France in 2021; a cable linking Cambodia and Hong-Kong; and the 25,000 km/15,500 mile Asia-Africa-Europe (AAE) cable involving China Unicom. Australia had to intervene to stop Beijing building an undersea cable to the Solomon Islands.<sup>59</sup>

Beijing's increasing geopolitical assertiveness jeopardizes the undersea cable infrastructure of adjacent powers such as South Korea. China may use its increasing military power in undersea and other maritime domains and likely will engage in lawfare to engage in hostile attacks against undersea cables and promote its illicit undersea territorial claims in the Indo-Pacific region. This may be done through using People's Liberation Army (PLAN) assets or using its maritime militia and fishing fleets to coerce countries and ships representing these countries requiring the use of undersea cables near China in order to engage in gray zone warfare against these countries to acquiesce in Beijing's extraterritorial claims. Such behavior is ultimately consistent

with the doctrine of unrestricted warfare espoused by the People's Liberation Army to compensate for its perceived inferiority against the U.S. and its allies during a high technology war.<sup>60</sup>

# RECOMMENDATIONS AND SOLUTIONS

---

The past year has seen the world become familiar with the disastrous economic, national security and public health implications of infectious disease has demonstrated by the Coronavirus pandemic. It is now time for world opinion to become aware of the economic and national security implications of losing access to the information transmitted by undersea cables. Cable information and data transmission have gone from the initial 17 hours and 40 minutes it took to transmit messages between President Buchanan and Queen Victoria to the fastest cables transferring data at speed of nearly 25 terabytes per second, which is twice the amount of the annual data generated by the Hubble Space Telescope.<sup>61</sup>

Losing such access for even a short amount of time would have asphyxiating consequences, which would cascade across the globe and take a long time to work around and overcome. Undersea cables and their geoeconomic and geopolitical criticality involve Mahan's emphasis on command of the sea, Corbett's on seapower's critical communication requirements, Mackinder's on the importance of the Eurasian heartland, and Spykman's emphasis on the rimland's

strategic importance.<sup>62</sup> Numerous works of varying quality and perspectives and numerous international strategic trends, exacerbated by the Coronavirus pandemic, are placing increasing emphasis on the vulnerability of the U.S. and its maritime allies to supply chain disruptions and hostility from countries as varied as China, Iran, North Korea, and Russia. Some of these works are beginning to recognize the vitally important role undersea cables play in our emerging geoeconomic, geopolitical, and strategic environment and urge the U.S. and its maritime allies to take a more assertive stance against the powers threatening the international geopolitical order.<sup>63</sup>

Despite the acute physical and social strain imposed by the Coronavirus, there are several steps political, technical, and military steps democratic countries can take individually to ensure the stable and uninterrupted flow of information and data through undersea cables. These include:

## POLITICAL

Exploring the possibility of driving a wedge between Russia and China by emphasizing how Russia's ties with Vietnam puts Moscow in potential with Beijing over

South China Sea maritime disputes and access to energy resources.

Promote more transparency, oversight, and standards into the Maritime Silk Road and the Belt and Road Initiative while emphasizing that the lack of such transparency could produce attempts by Beijing and its allies to attack critical undersea cables as a means of gaining coercive geopolitical advantage. An attribute of this would be working to ensure that companies under Chinese and Russian leverage such as Rostelecom and Huawei are thwarted in their attempts to gain influence in democratic maritime countries, which could be used to further Beijing's and Moscow's interests. Maritime countries should also use the American Enterprise Institute and Heritage Foundation's China Global Investment Tracker as a template to counter Chinese influence on undersea cable infrastructure investment by avoiding cable companies having ties with Chinese or Russian cable firms, which could result in use of these cables being curtailed or severed.

Australia, European countries, India, Japan, and the U.S. using economic development as a means of exerting geoeconomic and geopolitical leverage to dissuade nations from favoring Chinese and Russian efforts to restrict the free flow of information and strategic communications through undersea cables.<sup>64</sup>

## **POLITICAL/MILITARY**

The U.S. supporting partners and allied nations such as Japan

through multilateral exercises, advanced technological transfers, weapons sales, and greater intelligence sharing to preempt potential attempts to seize control of undersea cables.

NATO and its Allied Maritime Command must transition from a Eurocentric maritime orientation to expand its operations into the Atlantic and Mediterranean to protect against potential threats to submarine cables.

Encourage India to expand its emphasis on homeland defense to include maritime operations and capability including engagement with countries such as Indonesia, the Philippines, and Vietnam to increase their commitment to securing undersea cable communications.

## **TECHNICAL**

The importance of powers outside of China and Russia thinking of how undersea cables secure, store, and share information from one location to the next. Private sector accomplishment of maritime cybersecurity for national security is to large to be accomplished without governmental involvement. Controlling key information flows originating in the global undersea fiber optic cable networks is critical for strategic victory in multiple future conflict scenarios. This also applies to U.S. Navy missional and operational objectives in the critical IndoPacom region.<sup>65</sup>

## MILITARY

Training U.S. and allied maritime forces in monitoring and repairing undersea cables. Increasing lethality of ships in U.S. Cable Security Program and liberalizing rules of engagement for crews of these ships to use deadly force against hostile actors trying to disrupt or destroy submarine cables. Assigning at least one cable repair ship to regions covered by U.S. geographic unified military combatant commands is highly desirable.

## TECHNICAL/MILITARY

Training U.S. and allied maritime forces in monitoring and repairing undersea cables. Increasing lethality of ships in U.S. Cable Security Program and liberalizing rules of engagement for crews of these ships to use deadly force against hostile actors trying to disrupt or destroy submarine cables. Assigning at least one cable repair ship to regions covered by U.S. geographic unified military combatant commands is highly desirable.

Steps for enhancing undersea cable security include incorporating assessments of attacks on undersea cable infrastructure and best practices for responding to such attacks into national military strategy documents. Conducting national risk assessments and establishing a national risk register to identify undersea cable risks to maritime countries. Including secure cable landing sites into national critical infrastructure facilities and incorporate necessary security measures.

Establishing Cable Protection Zones such as Australia's around coastal areas with high-value communications corridors. Deploy better monitoring on cables by requiring private sector contractors to place sensors capable of detecting sonar frequencies near key undersea infrastructure and along cable routes.

## TECHNICAL/POLITICAL

Promote greater geographic diversity of undersea cables and increase criminal penalties for disrupting or destroying such cables. Increase building of backup systems to promote resiliency and redundancy. Consider pushing for a new international treaty to protect undersea cables with stiff penalties for disrupting and destroying them. Such an agreement is only realistically possible among democratic maritime nations since authoritarian nations would not be honest brokers in enforcing such agreements. Increase naval exercises involving undersea cables and regularly review maritime capabilities among NATO and other global democracies. Make it clear that maritime countries will not tolerate attacks upon this critical infrastructure and are willing to use military force against those attacking undersea cables.<sup>66</sup>

It is also essential for national security leaders in the world's democratic countries to repeatedly educate their residents on the critical importance of undersea cables to national economic and strategic interests. This is not likely under the Biden Administration, but congressional leaders and national security analysts

concerned with this subject must take the lead in this endeavor until the U.S. has a presidential administration that takes this matter seriously. Other countries must also take the lead in stressing the importance of this subject and the need to protect this vital infrastructure. Failure to rectify these deficiencies and educate the public could result in a cyber Pearl Harbor/911 cataclysm that will be extremely difficult to recover from and make the Coronavirus' discomfort and disruption seem minor.



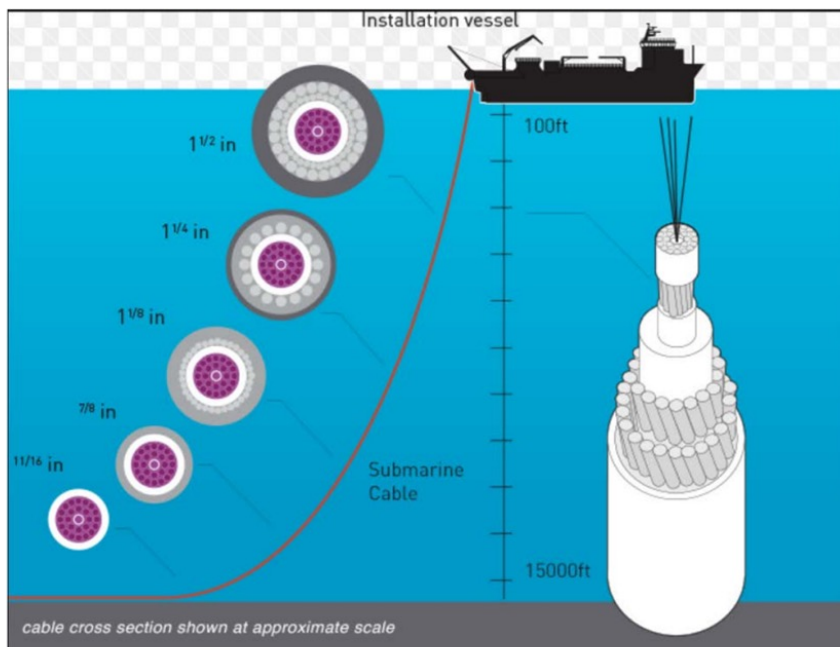
# APPENDIX

FIGURE 4: CABLE LAYING



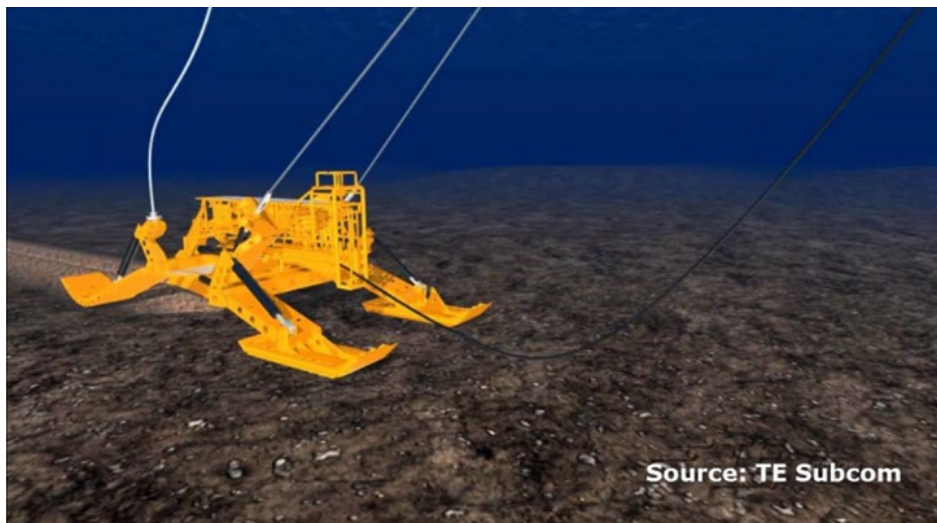
Source: Office of the Director of National Intelligence <sup>67</sup>

FIGURE 5: CABLE CROSS SECTIONS AT VARIOUS DEPTHS



Source: Office of the Director of National Intelligence <sup>68</sup>

FIGURE 6: SUBMERGED PLOUGH BURYING UNDERSEA CABLE



Source: Office of the Director of National Intelligence <sup>69</sup>

FIGURE 7: REMOTELY OPERATED VEHICLE (ROV)<sup>IXV</sup>



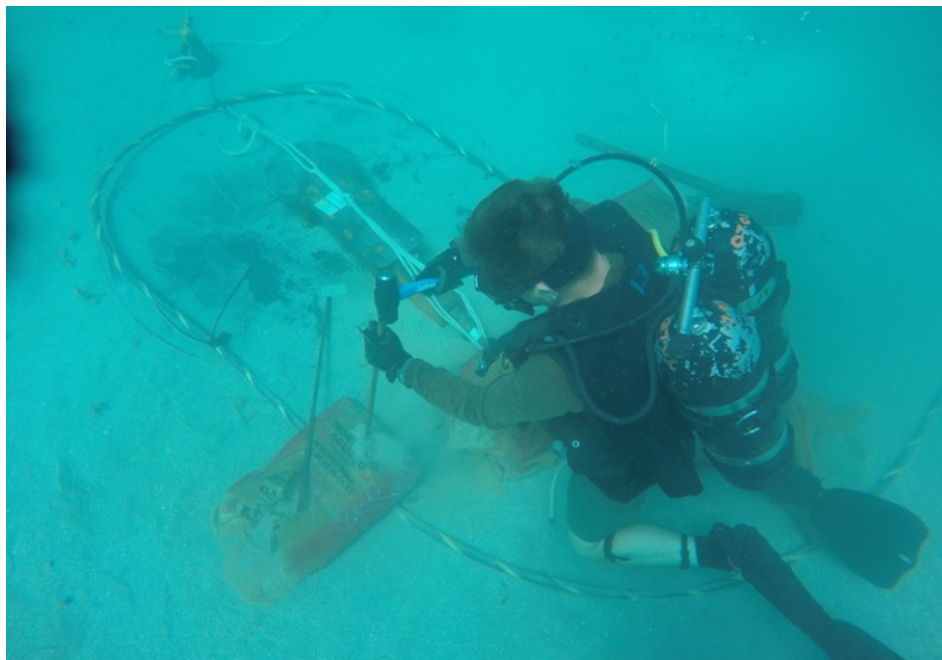
Source: Office of the Director of National Intelligence <sup>70</sup>

**FIGURE 8: GUANTANAMO BAY CABLE LANDING SITE**



Source: Defense Visual Instrumentation Distribution Service (DVIDS) <sup>71</sup>

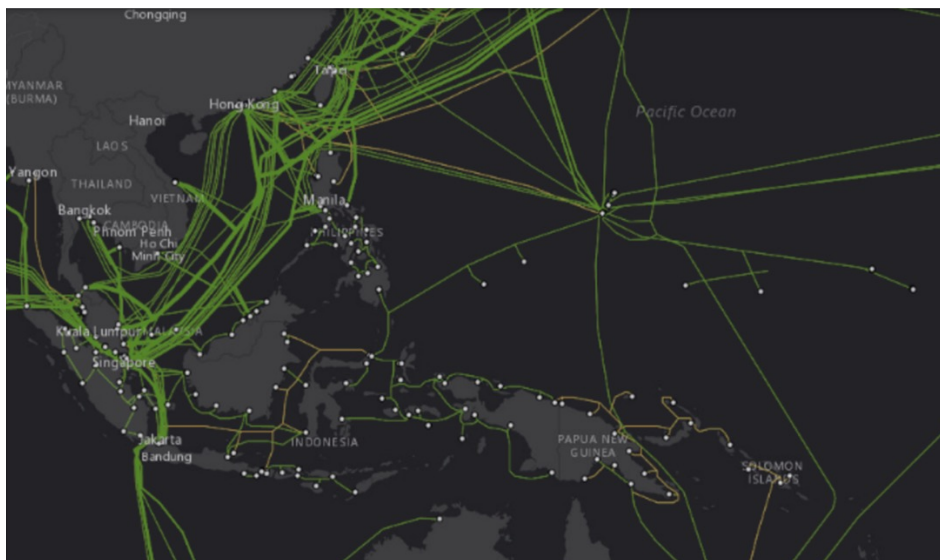
**FIGURE 9: NAVAL ENGINEER SECURES CONCRETE STAKES NEAR GITMO CABLE LANDING STATION**



Source: Office of the Director of National Intelligence <sup>72</sup>

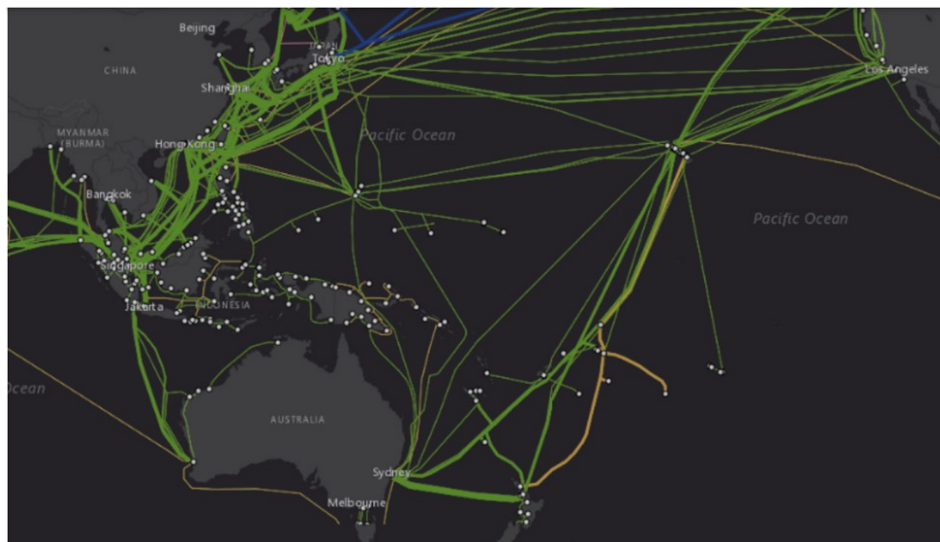


**FIGURE 10: SUBMARINE CABLE NETWORK IN NORTHEAST AND SOUTHEAST ASIA**



Source: Submarine Cable Network in Northeast and Southeast Asia-National Bureau of Asian Research Maritime Awareness Project<sup>73</sup>

**FIGURE 11: SUBMARINE CABLE NETWORK ACROSS THE PACIFIC OCEAN**



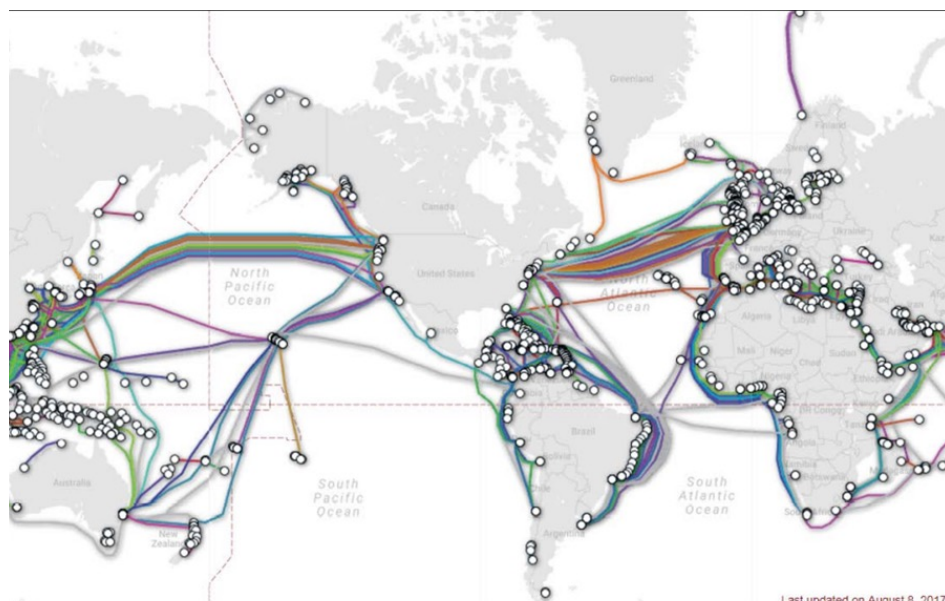
Source: Submarine Cable Network Across the Pacific Ocean<sup>74</sup>

FIGURE 12: EUROPE-INDIA GATEWAY



Source: Europe-India Gateway <sup>75</sup>

FIGURE 13: GLOBAL SUBMARINE CABLE NETWORK



Source: Office of the Director of National Intelligence <sup>76</sup>

This selective table of 24 cables, their distances, and areas of coverage, initial operating dates, and ownership demonstrates the vast geographic proliferation and dispersion of undersea cables.

## FIGURE 14: SELECTED GLOBAL SUBMARINE CABLES AND OPERATORS

SOURCE: TELEGEOGRAPHY

NAME	READY FOR SERVICE	LENGTH	SELECTED OWNERS	SELECTED LANDING POINTS	CABLE WEBSITE
Africa Coast to Europe (ACE)	December 2012	17,000 km/10,540 miles	Dolphin Telecom, Cote d'Ivoire Telecom, Republic of Equatorial New Guinea	Carcevalos, Portugal; Accrs, Ghana; Conakry, Guinea; Lagos, Nigeria; Luanda, Angola, Duynefontein, South Africa	<a href="https://ace-submarinecable.com/">https://ace-submarinecable.com/</a>
Alaska United West (AU-West)	June 2004	2,400 km/1,488 miles	GCI	Seward, AK; Warrenton, OR	<a href="https://www.gci.com/">https://www.gci.com/</a>
Americas-II	August 2000	8,373 km/5,191 miles	Embratel, AT&T, Verizon, Spring, Altice Portugal	Hollywood, FL; St. Croix U.S. Virgin Islands; Port of Spain, Trinidad & Tobago; Camuri, Venezuela; Cayenne, French Guiana; Fortaleza, Brazil	No URL
Asia-Africa-Europe (AAE-1)	2017	25,000 km/15,500 miles	China Unicom, Telcom Egypt, Tlecommunications Co. Ltd., TeleYemen, Jio Infocom, Time.com	Abu Talat, Egypt; Aden, Yemem; Bari, Italy; Cape D'Aguiar, China; Marseille, France; Jeddah, Saudi Arabia, Mumbai, India	<a href="https://www.aaeone.com/aaeportal/">https://www.aaeone.com/aaeportal/</a>
Asia-Pacific Gateway (APG)	November 2016	10,400 km/6,448 miles	NTT, China Unicom; Chunghwa Telecom; VNPT International; Facebook; Time.com	Busan, South Korea; Chongming, China; Danang, Vietnam; Kuantan, Malaysia; Maruyama, Japan; Tanah Merah, Singapore; Toucheng, Taiwan.	No URL
Atlantic Crossing-1 (AC-1)	May 1998	14,3021 km/8,666 miles	Lumen	Beverwijk, Netherlands; Sylt, Germany; Whitesands Bay, United Kingdom, Brookhaven, NY	<a href="https://www.lumen.com/wholesale.html">https://www.lumen.com/wholesale.html</a>
Australia-Japan Cable (AJC)	December 2001	12,700 km/7,874 miles	AT&T, NTT, Softbank Corporation, Telstra, Verizon	Maruyama, Japan; Tumon Bay, Guam, US; Paddington, Australia	<a href="https://ajcable.com/">https://ajcable.com/</a>
Baltic Sea Submarine Cable	2000	1,042 km/646 miles	CITIC Telecom International	Helsinki, Finland; Stockholm, Sweden; Tallinn, Estonia	<a href="https://www.cicitel.com">https://www.cicitel.com</a> Hdgtrs: Hong Kong




NAME	READY FOR SERVICE	LENGTH	SELECTED OWNERS	SELECTED LANDING POINTS	CABLE WEBSITE
Caucasus Cable System	November 2008	1,200 km/744 miles	Caucasus Online	Balchik, Bulgaria; Potik, Georgia	<a href="http://www.go.ge/en/">http://www.go.ge/en/</a>
Chuuk-Pohnpei	May 2019	1,200 km/744 miles	Federated States of Micronesia Telecommunications Company	Pohnpei, Micronesia; Weno, Chuuk, Micronesia	<a href="https://fsmcable.com/chuuk/">https://fsmcable.com/chuuk/</a>
Far East Submarine Cable System	2nd Qtr 2016	1,855 km/1,150 miles	Rostelecom	Okha, Russia; Ola Russia; Ust-Bolsheretsk, Russia	No URL
Hawaiki	July 2018	14,000 km/8,680 miles	Hawaiki Submarine Cable LP	Pacific City, OR; Kapolei, HI; Pago Pago, American Samoa; Mangahai, New Zealand; Sydney, Australia	<a href="https://www.hawaiki.co.nz/">https://www.hawaiki.co.nz/</a>
Pacific Cable	2021	7,300 km/4,526 miles	América Móvil, Telxius	Puerto San Jose, Guatemala; Salinas, Ecuador; Lurin, Peru; Valparaiso, Chile	No URL
Peace Cable	4th Qtr. 2021	15,000 km/9,300 miles	Peace Cable Co. International Network, Ltd.- (Part of China's Digital Silk Road(DSR)	Marseille, France; Ab Talat, Egypt; Djibouti City, Djibouti; Hobyo, Somalia; Gwadar, Pakistan; Mombasa, Kenya; Victoria, Seychelles.	<a href="http://www.peacecable.net/">http://www.peacecable.net/</a>
SAFE	April 2002	13,500 km/8,370 miles	Telekom Malaysia, Telkom South Africa, Mauritius Telecom, Telecom Namibia, Vodafone	Baie Jacotet, Mauritius; Cochin, India; Mtunzini, South Africa; Penang, Malaysia, Saint Paul, Réunion	No URL
Tannat	1st Qtr. 2018	2,000 km/1,240 miles	Google, Antel Uruguay	Las Toninas, Argentina; Maldonado, Uruguay; Santos, Brazil	No URL
Tasman Global Access (TGA)	March 2017	2,288 km/1,418 miles	Spark New Zealand, Vodafone, Telstra	Oxford Falls, Australia; Raglan, New Zealand	No URL
TATA-TGN-TATA Indicom	November 2004	3,175 km/1,968 miles	Tata Communications	Changhi North Singapore; Chennai, India	<a href="https://www.tatacommunications.com/">https://www.tatacommunications.com/</a>

NAME	READY FOR SERVICE	LENGTH	SELECTED OWNERS	SELECTED LANDING POINTS	CABLE WEBSITE
Trans-Pacific Express (TPE)	2008	17,000 km/10,540 miles	China Unicom, Chungwa Telecom, KT, Verizon, NTT, AT&T	Nedonna Beach, OR; Maruyuma, Japan; Geoje, South Korea; Chongming, China; Tansuhui, Taiwan	<a href="https://tpecable.org:59876/">https://tpecable.org:59876/</a>
UAE Iran	1992	170 km/105 miles	Etisalat, Telecommunication Infrastructure Company of Iran	Fujairah, United Arab Emirates; Jask, Iran	No URL <sup>77</sup>

The following chart from the Office of the Director of National Intelligence documents possible threat scenarios facing undersea cables

FIGURE 15: GLOBAL SUBMARINE CABLE THREAT MATRIX

[Threat Impact Legend: Green = Low; Yellow = Medium; Red = High]<sup>1</sup>

	Overland & Last Mile	Near-Shore ~130ft	Off-Shore 130 - 300ft	Continental Shelf 300 - 600 ft	Deep Sea ~600 ft +
	<i>Threats</i>				
<b><u>Natural</u></b>					
Sharks	Green	Green	Yellow	Yellow	Green
Earthquake	Green	Yellow	Yellow	Red	Red
Landslide	Green	Green	Green	Red	Red
Volcano	Red	Red	Green	Red	Red
Tsunami	Green	Red	Yellow	Yellow	Yellow
<b><u>Accidental</u></b>					
Fishing	Green	Red	Yellow	Green	Green
Anchor dragging	Green	Red	Yellow	Green	Green
Dredging	Green	Red	Green	Green	Green
<b><u>Malicious</u></b>					
Cyber Attack	Red	Red	Green	Green	Green
Vandalism	Red	Red	Green	Green	Green
Activists	Red	Red	Green	Green	Green
Theft	Green	Red	Yellow	Green	Green

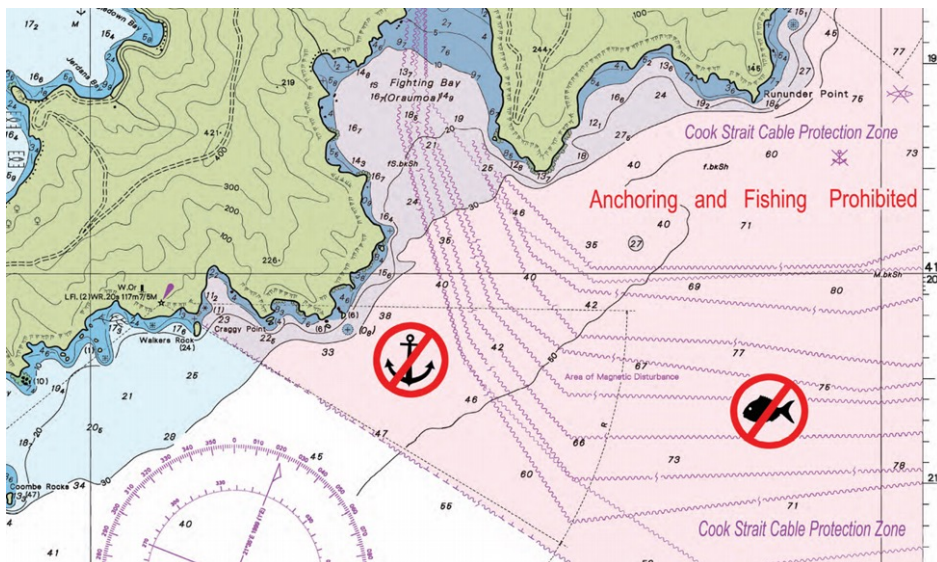
Source: Office of the Director of National Intelligence <sup>78</sup>

FIGURE 16: NEW ZEALAND CABLE PROTECTION ZONES

Area 1: Great Barrier Island
Area 2: Hauraki Gulf
Area 3: Kawau Island
Area 4: Whangaparoa Peninsula
Area 5: Muruwai Beach
Area 6: Takaroa
Area 7: Cook Strait
Area 8: Oaonui
Area 9: Hawke's Bay
Area 10: Maui A & B
Kupe Gas Project Protection Area -- no number
Maari Development Protection Area -- no number
Tui Area Development Protection Area -- no number
Pohokura Protection Area — no number <sup>79</sup>

Source: New Zealand Ministry of Transport

FIGURE 17: COOK STRAIT CABLE PROTECTION ZONE



Source: Transpower New Zealand <sup>80</sup>

FIGURE 18: USNS ZEUS



Source: U.S. Military Sealift Command <sup>81</sup>

FIGURE 19: ARCTIC CONNECT PROJECT



Source: Polar Journal <sup>82</sup>

# REFERENCES

---

<sup>1</sup> See See Rishi Sunak, *Undersea Cables: Indispensable, Insecure*, (London: Policy Exchange, 2017): 5-7; <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf> Accessed February 26, 2021; and Nadia Schadow and Brayden Helwig, "Protecting Undersea Cables Must Be Made a National Security Priority," *Defense News*, (July 1, 2020): 1-3; <https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/#:~:text=Undersea%20cables%20make%20instant%20communications,via%20these%20cables%20each%20day> Accessed March 11, 2021; and Blair Shephard, "Cutting Submarine Cables: The Legality of the Use of Force in Self-Defense," *Duke Journal of International and Comparative Law*, 31 (1)(2020): 199-220.

<sup>2</sup> Alfred Thayer Mahan, *The Influence of Seapower Upon History, 1660-1783*, 12th ed., (Boston: Little, Brown, and Company, 1918; Kindle location 2948).

<sup>3</sup> Merriam-Webster Dictionary, (New York: Merriam-Webster, 2021): <https://www.merriam-webster.com/dictionary/choke%20point>; Accessed October 28, 2021

<sup>4</sup> See Sunak, 12, 16; and John Steele Gordon, *A Thread Across the Ocean: The Heroic Story of the Transatlantic Cable*, (New York: HarperPerennial, 2003).

<sup>5</sup> "The Ocean Telegraph: So Striking an Instance of Steady Resolve," *Frank Leslie's Weekly*, (August 21, 1858): 3; <https://atlantic-cable.com/Article/1858Leslies/0821f.jpg>; Accessed October 28, 2021.

<sup>6</sup> Paul M. Kennedy, "Imperial Communications and Strategy, 1870-1914," *English Historical Review*, 86 (4)(October 1971): 728-752; <https://www.jstor.org/stable/563928> Accessed March 4, 2021.

<sup>7</sup> U.S. Secretary of State, *Commercial Relations of the United States for the Year Ending September 1858*, Senate Executive Document 35-37, Serial 991, (Washington, DC: William A. Harris Printer, 1859).

<sup>8</sup> Charles I. Bevans, *Treaties and Other International Agreements of the United States, 1776-1949*: 1: *Multilateral Agreements, 1776-1917*, (Washington, DC: U.S. Department of State, 1968): 92; <https://tile.loc.gov/storage-services/service/ll/lltreaties/lltreaties-ustbv001/lltreaties-ustbv001.pdf> Accessed March 18, 2021.

<sup>9</sup> *Submarine Telegraph Act of 1885*, <https://www.legislation.gov.uk/ukpga/Vict/48-49/49/contents> Accessed October 18, 2021. See "Computing Real Value Over Time With a Conversion Between U.K. Pounds and U.S. Dollars, 1791-Present," *Measuring Worth.com*; [https://www.measuringworth.com/calculators/exchange/result\\_exchange.php](https://www.measuringworth.com/calculators/exchange/result_exchange.php); Accessed March 4, 2021.







<sup>16</sup> "Patent 10,481,356 SUBMARINE COMMUNICATIONS CABLE AND METHOD AND DEVICE FOR THE PRODUCTION THEREOF," Patent Gazette, 1468 (3) November 19, 2019, 149-223; <https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=10481356.PN.&OS=PN/10481356&RS=PN/10481356> Accessed October 25, 2021.

<sup>17</sup> Sunak, 5; and Michael S. Mati, *The Protection of Undersea Cables: A Global Security Threat*, (Carlisle, PA: U.S. Army War College, 2012): 1; <https://purl.fdlp.gov/GPO/gpo148831> October 25, 2021; Schadow and Helwig; Rob Verger, "A 10 Million Pound Undersea Cable Just Set an Internet Record," *Popular Science*, (March 5, 2019): 1-5; <https://www.popsci.com/submarine-cable-data-transfer-record/>; Accessed March 8, 2021; and Bob Wargo, *Submarine Cables Remain Critical for Overseas Communications*, (Williamsburg, VA: Mid-Atlantic Regional Council of the Ocean, n.d): 3-4; <https://portal.midatlanticocean.org/ocean-stories/information-super-highway/>; Accessed March 11, 2021.

<sup>18</sup> Sunak, 19-20.

<sup>19</sup> *Ibid.*, 21-22, 37; Keir Giles, *The Next Phase of Russian Information Warfare*, (Riga: NATO Strategic Communications Centre of Excellence, 2016): 11-13; <https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176>; Accessed October 25, 2021; and APEC Policy Support Unit, *Economic Impact of Submarine Cable Disruptions*, (Singapore: Asia-Pacific Economic Cooperation Secretariat, 2013). <https://www.apec.org/publications/2013/02/economic-impact-of-submarine-cable-disruptions> Accessed October 25, 2021.

<sup>20</sup> "Telecommunications and Other Legislation Amendment: Protection of Submarine Cables and Other Measures," (Canberra: Federal Register of Legislation, 2021): 8-9; <https://www.legislation.gov.au/Details/C2005A00104>; Accessed March 8, 2021; and Genevieve Butler, *Telecommunications Legislation Amendment (Submarine Cable Protection) Bill 2013*, (Canberra: Australian Parliamentary Library, 2014): 4; [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/bd/bd1314a/14bd046](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1314a/14bd046) Accessed March 8, 2021.

<sup>21</sup> Jessica Woodall, "Australia's Vulnerable Submarine Cables," *The Strategist*, (May 31, 2013); <https://www.aspistrategist.org.au/australias-vulnerable-submarine-cables/>; Accessed March 8, 2021; and "The Economic Importance of Submarine Cables," *Semaphore*, 2 (2012): 1; [https://www.navy.gov.au/sites/default/files/documents/Semaphore\\_2012\\_2.pdf](https://www.navy.gov.au/sites/default/files/documents/Semaphore_2012_2.pdf) Accessed March 8, 2021.

<sup>22</sup> Australian Communication and Media Authority and Office of the Esafety Commissioner, *Annual Report 2017/18*, (Canberra: ACMA, 2019): 69; <https://www.acma.gov.au/publications/2018-10/report/ACMA-annual-report-2017-18> Accessed October 25, 2021.

<sup>23</sup> Holly Elizabeth Matley, "Closing the Gaps in the Regulation of Submarine Cables: Lessons from the Australian Experience," *Australian Journal of Maritime & Ocean Affairs*, 11 (3)(2019): 172; DOI:10.1080/18366592.2019653640, <https://www.tandfonline.com/doi/full/10.1080/18366592.2019.1653740> ; and Frank Smith, Aim Sinpeng, Ralph Holz, Sarah Logan, Jonathan Hutchinson and Hui Xue, *Australia's Cybersecurity Future(s): It's January 2024: Does Australia Still Have the Internet?*, (Barton: Australian Strategic Policy Institute, 2018): 8-9, 12; <https://www.aspi.org.au/report/australias-cybersecurity-futures> Accessed October 25, 2021.

<sup>24</sup> Stuart Kaye, "International Measures to Protect Oil Platforms, Pipelines, and Submarine Cables from Attack," *Tulane Maritime Law Journal*, 31 (2)(Summer 2007): 418-424.

<sup>25</sup> "Security of Critical Infrastructure Act, 2018," (Canberra: Federal Register of Legislation, 2021): 41; <https://www.legislation.gov.au/Details/C2018A00029>; Accessed October 25, 2021.

<sup>26</sup> See New Zealand Legislation, "Submarine Cables and Pipelines Protection Act 1996," (Wellington: Parliamentary Counsel Office, 2027): 7-8; <https://legislation.govt.nz/public/1996/0022/latest/DLM375803.html> Accessed October 25, 2021; and New Zealand, Ministry of Transport, "Protecting New Zealand's Undersea Cables," (Wellington: Ministry of Transport, 2020): 1-2; <https://www.transport.govt.nz/about-us/what-we-do/queries/protecting-new-zealands-undersea-cables> Accessed October 25, 2021.

<sup>27</sup> 3 USC 301, <https://www.govinfo.gov/content/pkg/USCODE-2018-title3/pdf/USCODE-2018-title3.pdf>; Accessed March 9, 2021.

<sup>28</sup> 10 USC 113, <https://www.govinfo.gov/content/pkg/USCODE-2018-title10/pdf/USCODE-2018-title10.pdf>; Accessed March 9, 2021.

<sup>29</sup> 26 USC 168, <https://www.govinfo.gov/content/pkg/USCODE-2018-title26/pdf/USCODE-2018-title26.pdf>; Accessed March 9, 2021.

<sup>30</sup> 33 USC 3, <https://www.govinfo.gov/content/pkg/USCODE-2018-title33/pdf/USCODE-2018-title33.pdf>; Accessed March 9, 2021.

<sup>31</sup> 33 USC 3204, <https://www.govinfo.gov/content/pkg/USCODE-2018-title33/pdf/USCODE-2018-title33.pdf>; Accessed March 9, 2021.

<sup>32</sup> 42 USC 9113, <https://www.govinfo.gov/content/pkg/USCODE-2018-title42/pdf/USCODE-2018-title42.pdf>; Accessed March 9, 2021.

<sup>33</sup> 42 USC 9164, <https://www.govinfo.gov/content/pkg/USCODE-2018-title42/pdf/USCODE-2018-title42.pdf>; Accessed March 9, 2021.

<sup>34</sup> 43 USC 1331, <https://www.govinfo.gov/content/pkg/USCODE-2018-title43/pdf/USCODE-2018-title43.pdf>; Accessed March 9, 2021.

<sup>35</sup> 47 USC 26, <https://www.govinfo.gov/content/pkg/USCODE-2018-title47/pdf/USCODE-2018-title47.pdf>; Accessed March 9, 2021.

<sup>36</sup> 47 USC 34, <https://www.govinfo.gov/content/pkg/USCODE-2018-title47/pdf/USCODE-2018-title47.pdf>; Accessed March 9, 2021.

<sup>37</sup> NOAA Office of General Counsel, "Submarine Cables-Domestic Regulation," (Washington, DC: National Oceanic and Atmospheric Administration, 2019): 1-2; [https://www.gc.noaa.gov/gcil\\_submarine\\_cables\\_domestic.html](https://www.gc.noaa.gov/gcil_submarine_cables_domestic.html) Accessed October 27, 2021.

<sup>38</sup> See U.S. Naval Facilities Engineering Systems Command, "NSCPO Background," (Washington, DC: Naval Facilities Engineering Systems Command, 2021?): 1-2; [https://www.navfac.navy.mil/products\\_and\\_services/dc/products\\_and\\_services/naval\\_ocean\\_facilities\\_program/sea\\_floor\\_cable\\_protection\\_nscpo/nscpo\\_background.html#:~:text=NSCPO%20Background%20History%20of%20the%20NSCPO%20The%20Naval,the%20Navy%20was%20averaging%2010%20breaks%20per%20year](https://www.navfac.navy.mil/products_and_services/dc/products_and_services/naval_ocean_facilities_program/sea_floor_cable_protection_nscpo/nscpo_background.html#:~:text=NSCPO%20Background%20History%20of%20the%20NSCPO%20The%20Naval,the%20Navy%20was%20averaging%2010%20breaks%20per%20year). Accessed October 27, 2021; and Bob Fredrickson and Catherine Creese, "Navy Undersea Cable Systems," (Port Hueneme, CA: Naval Facilities Engineering Service Center, n.d.); 39-42; [https://www.navfac.navy.mil/content/navfac/en/products\\_and\\_services/dc/products\\_and\\_services/naval\\_ocean\\_facilities\\_program/sea\\_floor\\_cable\\_protection\\_nscpo/news/\\_jcr\\_content/par1/pdfdownload\\_0/file.res/nscpo%20article%202.pdf](https://www.navfac.navy.mil/content/navfac/en/products_and_services/dc/products_and_services/naval_ocean_facilities_program/sea_floor_cable_protection_nscpo/news/_jcr_content/par1/pdfdownload_0/file.res/nscpo%20article%202.pdf) Accessed October 27, 2021.

<sup>39</sup> See U.S. Military Sealift Command, "Cable Laying/Repairing Ship," (Washington, DC: U.S. Military Sealift Command, 2021): 1; <https://www.msc.usff.navy.mil/Ships/Ship-Inventory/Cable-Laying-Repair-Ship/> ; Accessed March 10, 2021, and USNS Zeus (T-ARC-7) Cable Repairing Ship, (Washington, DC: U.S. Naval Vessel Register, 2021): 1; [https://www.nvr.navy.mil/SHIPDETAILS/SHIPSDETAIL\\_ARC\\_7.HTML](https://www.nvr.navy.mil/SHIPDETAILS/SHIPSDETAIL_ARC_7.HTML) ; Accessed March 10, 2021.

<sup>40</sup> "Submarine Cables-Domestic Regulation," 3. See also pp. 5-9 for additional domestic and international studies of undersea cables and their potential environmental impacts; George Galdorisi and Stephanie C. Hsieh, "Operationalizing the Joint Information Environment: Achieving Information Dominance With the Undersea Constellation," *U.S. Navy Journal of Underwater Acoustics*, 63 (4)(November 2014): 616-624; <https://apps.dtic.mil/sti/citations/ADA620398> Accessed October 27, 2021; and Department of the Navy (DON) 19.2 Small Business Innovation Research (SBIR) Proposal Submission Instructions, (Washington, DC: Department of the Navy, 2019): [https://navysbir.info/docs/Nav-19\\_2\\_SBIR-Topics-5-2-19.pdf](https://navysbir.info/docs/Nav-19_2_SBIR-Topics-5-2-19.pdf); Accessed October 27, 2021.

<sup>41</sup> "Submarine Cables-Domestic Regulation," 4.

<sup>42</sup> See *Ibid.*, 5; 47 USC 34; and "Federal Communications Commission," *Federal Register*, 19 (92) (May 12, 1954): 2711; <https://www.govinfo.gov/content/pkg/FR-1954-05-12/pdf/FR-1954-05-12.pdf> Accessed March 12, 1954.

<sup>43</sup> See U.S. Federal Communications Commission, "Circuit Data for U.S.-International Submarine Cables," (Washington, DC: Federal Communications Commission, 2020): 1-2; <https://purl.fdlp.gov/GPO/gpo150778> Accessed March 10, 2021; *Ibid.*, "International Circuit

Capacity Report, 2015", (Washington, DC: Federal Communications Commission, 2017): 1-2; <https://www.fcc.gov/reports-research/reports/international-circuit-capacity-reports/international-circuit-capacity-0> Accessed March 10, 2021; and National Oceanic and Atmospheric Administration, Office of General Counsel, "Submarine Cables-International Framework," (Washington, DC: National Oceanic and Atmospheric Administration, 2019): 1-2; [https://www.gc.noaa.gov/gcil\\_submarine\\_cables\\_international.html](https://www.gc.noaa.gov/gcil_submarine_cables_international.html) Accessed March 12, 2021; Updated circuit capacity reports and data by country and company through 2019 at <https://docs.fcc.gov/public/attachments/DA-20-1176A2.xlsx> Accessed March 10, 2021.

<sup>44</sup> See Public Law 109-58, "Energy Policy Act of 2005," 119 U.S. Statutes at Large 594, <https://www.congress.gov/109/plaws/publ58/PLAW-109publ58.pdf> Accessed March 10, 2021; and "Submarine Cables-Domestic Regulation," 5.

<sup>45</sup> See *Ibid.*, 3-5; and "Proclamation 8031: Establishment of the Northwestern Hawaiian Islands National Maritime Monument," Federal Register, 71 (122)(June 26, 2006): 36441-36475; <https://www.govinfo.gov/content/pkg/FR-2006-06-26/pdf/06-5725.pdf>; Accessed March 10, 2021.

<sup>46</sup> Rob Wittman, "The Greatest Risk to National Security You've Never Heard Of," Defense News, January 30, 2020; 1-2; <https://www.defensenews.com/battlefield-tech/c2-comms/2020/01/30/the-greatest-risk-to-national-security-youve-never-heard-of/?contentQuery=%7B%22section%22%3A%22%2Fopinion%2Fcommentary%22%2C%22from%22%3A48%2C%22size%22%3A10%2C%22exclude%22%3A%22%22%7D&contentFeatureId=f0fljrziYHYB5pv> Accessed March 11, 2021.

<sup>47</sup> See Ben Goldman, U.S. Maritime Administration (MARAD): Shipping and Shipbuilding Support Programs, (Washington, DC: Library of Congress, Congressional Research Service, 2021): Summary, 1-2, 7, 18; <https://crsreports.congress.gov/product/pdf/R/R46654> Accessed March 11, 2021; and Public Law 116-92; "National Defense Authorization Act for Fiscal Year 2020," 113 U.S. Statutes at Large, 1988-1997; <https://www.govinfo.gov/content/pkg/PLAW-116publ92/pdf/PLAW-116publ92.pdf> Accessed March 11, 2021.

<sup>48</sup> See U.S. Congress, House Committee on Armed Services, Subcommittee on Intelligence and Emerging Threats and Capabilities and U.S. Congress, House Committee on Oversight and Reform, Subcommittee on National Security, Securing the Nation's Internet Architecture, (Washington, DC: GPO, 2020): 30, 73; <https://purl.fdlp.gov/GPO/gpo144278> and Critical Infrastructure Review and Resilience, Presidential Policy Directive (PPD-21) was issued by President Obama on February 12, 2013; <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> Accessed October 18, 2021.

<sup>49</sup> U.S. Congress, House Committee on Armed Services, House Report 117-118; National Defense Authorization Act for Fiscal Year 2022 on H.R. 4350 Together With Additional and Dissenting Views, (Washington, DC: GPO, 2021): 18; <https://www.govinfo.gov/content/pkg/CRPT-117hrpt118/pdf/CRPT-117hrpt118.pdf>; Accessed October 18, 2021.

<sup>50</sup> Malcolm Eccles, International Cable Protection Committee: An Introduction to the ICPC, (London: ICPC, 2019: <https://www.iscpc.org/documents/?id=1751>; Accessed October 18, 2021.

<sup>51</sup> Bromund, Carafano, and Schaefer.

<sup>52</sup> Brief History of IMO, (London: International Maritime Organization, 2021): 1-3; <https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx> Accessed March 11, 2021.

<sup>53</sup> "U.S. and USSR Exchange Notes on Damage to Submarine Cables," Department of State Bulletin, 40 (1034)(April 20, 1959): <https://www.archive.org/details/departmentofstat4059unit/page/554/mode/2up?view=theater>; Accessed March 11, 2021; Roy O. Hale (DE-336), (Washington, DC: U.S. Naval History and Heritage Command, 2005): 1-2; <https://www.history.navy.mil/content/history/nhhc/our-collections/photography/numerical-list-of-images/nhhc-series/nh-series/80-G-241000/80-G-241613.html> Accessed March 11, 2021; and David W. Winkler, *Incidents at Sea: American Confrontation and Cooperation With Russia and China, 1945-2016*, (Annapolis: Naval Institute Press, 2017).

<sup>54</sup> Kyle Mizokami, "How a Super-Secret U.S. Navy Submarine Tapped Russia's Underwater Communications Cable: A Forgotten Cold War Tale," *The National Interest*, (June 29, 2017): 1-4; <https://nationalinterest.org/blog/the-buzz/how-super-secret-us-navy-submarine-tapped-russias-underwater-21370> Accessed March 12, 2021.

<sup>55</sup> "Chapter One: The Future of Maritime Competition," *The Military Balance*, 121 (1)(2021): 11; <https://DOI.10.1080/04597222.2021.1868790>; Accessed March 12, 2021.

<sup>56</sup> David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are to Close for U.S. Comfort," *New York Times*, (October 25, 2015): A1; <https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html> Accessed March 12, 2021.

<sup>57</sup> See Stuart Peach, Annual Chief of the Defence Staff Lecture 2017, (London: RUSI, 14 December 2017): 2; <https://ik.imagekit.io/po8th4g4eqj/prod/rusi-cds-annual-lecture-2017.pdf> Accessed October 27, 2021; and Andrew Chuter, "Russia's Naval Updates Threaten Underseas Comms Network, Says Top British Military Officer," *Defense News*, (December 15, 2017): 1-3; <https://www.defensenews.com/naval/2017/12/15/russias-naval-updates-threaten-undersea-comms-network-says-top-british-military-officer/> Accessed October 27, 2021.

<sup>58</sup> See Paul Goble, "New Undersea Cables Could Become a Flashpoint in the Arctic," *Eurasia Daily Monitor*, 18 <https://jamestown.org/program/new-undersea-cables-could-become-a-flashpoint-in-the-arctic/>; Accessed March 12, 2021; and U.S. Navy, Submarine Force Pacific, "About IUSS, Mission Statement," (Virginia Beach: Commander Undersea Surveillance, 2021):

1; <https://www.csp.navy.mil/cus/About-IUSS/>; Accessed March 12, 2021.

<sup>59</sup> See Hemmings, 10-11, 14; Schadlow and Hurwig, 2; Robert Fonow, "Cybersecurity Demands Physical Security," *Signal*, (February 2006): 1-2; <https://www.afcea.org/content/cybersecurity-demands-physical-security> Accessed March 12, 2021; Nitin Agarwala, "Advances by China in Deep Seabed Mining and Its Security Implications for India," *Australian Journal of Maritime & Ocean Affairs*, 13 2 (2021): 11; <https://doi.org/10.1080/18366503.2021.1871810>; Accessed March 12, 2021; and Michael O'Keefe, "The Militarisation of China: Stepping Up to the New Cold War?," *Security Challenges*, 16 (1)(2020): 100, 109; <https://www.jstor.org/stable/26908770>; Accessed March 12, 2021.

<sup>60</sup> Sean O'Malley, "Assessing Threats to South Korea's Undersea Cable Communications Infrastructure," *Korean Journal of International Studies*, 17 (3)(December 2019): 385-414; <https://doi.org/10.14731/kjis.2019.12.17.3.385> Accessed March 12, 2021; Shuxian Luo and Jonathan G. Painter, "China's Maritime Militia and Fishing Fleets," *Military Review*, 101 (1) (January-February 2021): 6-21; <https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Panther-Maritime-Militia-1.pdf> Accessed October 27, 2021; Isaac Benjamin Kardon, "Rising Power, Creeping Jurisdiction: China's Law of the Sea," Ph.D. Dissertation, Cornell University, 2017; 91,109, 252, 266, 288, 295, 325-326, 355; <https://ecommons.cornell.edu/handle/1813/47720> Accessed October 19, 2021; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China*, (Washington, DC: DOD, 2020): 16, 20, 73, 148; <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF> Accessed March 12, 2021; and Qiao Lang and Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, 1999); <https://www.c4i.org/unrestricted.pdf> Accessed March 12, 2021.

<sup>61</sup> Schadlow and Helwig, 1.

<sup>62</sup> See Mahan, *The Influence of Seapower Upon History*; Julian Corbett, *Some Principles of Maritime Strategy*, (London: Longman, Greens, 1918); Halford Mackinder, "The Geographical Pivot of History," *The Geographical Journal*, 23 (4)(April 1904): 421-444; *Ibid.*, *Democratic Ideals and Reality: A Study in Reconstruction*, (New York: Henry Holt and Company, 1919); and Nicholas Spykman, *America's Strategy in World Politics*, (New York: Harcourt, Brace, and Company, 1942).

<sup>63</sup> See Nicole Starosielski, *The Undersea Network*, (Durham: Duke University Press, 2015); Michael Auslin, *Asia's New Geopolitics: Essays on Reshaping the Asia-Pacific*, (Stanford, CA: Hoover Institution Press, 2020); Antulio Echevarria II, *War's Logic*, (New York: Cambridge University Press, 2021); Geoffrey Gresh, *To Rule Eurasia's Waves: The Great Power Competition At Sea*, (New Haven: Yale University Press, 2020); Robert Martinage, "The Vulnerability of the Commons," *Foreign Affairs*, 94 (1)(January/February 2015): 117-126; and U.S. Office of the Director of National Intelligence, *Threats to Undersea Cable Communications*,



(Washington, DC: ODNI, 2017); <https://purl.fdlp.gov/GPO/gpo149138>; Accessed March 12, 2021.

<sup>64</sup> See China Global Investment Tracker, Derek Scissors, ed., (Washington, DC: American Enterprise Institute and Heritage Foundation, 2021): <https://www.aei.org/china-global-investment-tracker/> Accessed March 15, 2021; and Gresh, Kindle location 5424-5642.

<sup>65</sup> Sunak, 34-36.

<sup>66</sup> See Sunak, Gresh, *On Contested Shores: The Evolving Role of Amphibious Operations in the History of Warfare*, Timothy Heck, ed., (Quantico, VA: Marine Corps University Press, 2020): <https://purl.fdlp.gov/GPO/gpo151172> Accessed March 22, 2021; and Colin S. Gray, *Leverage of Seapower: The Strategic Advantage of Navies in War*, (New York: The Free Press, 1992). I am also indebted to Chris Parry of the Mackinder Forum for stressing the importance of maritime countries like the U.S., United Kingdom, India, and other democracies cooperating together against geopolitical threats from countries such as China and Russia.

<sup>67</sup> Threats to Undersea Cable Communications, (Washington, DC: Office of the Director of National Intelligence, 2017): 1; <https://purl.fdlp.gov/GPO/gpo/149138> Accessed March 5, 2021.

<sup>68</sup> *Ibid.*, 21.

<sup>69</sup> *Ibid.*, 12.

<sup>70</sup> *Ibid.*, 36.

<sup>71</sup> "UCT One-Unit of Choice for GITMO Cable Landing, [Image 6 of 6]," (Washington, DC: Defense Visual Information Distribution Service, January 20, 2016); <https://www.dvidshub.net/image/2362995/uct-one-unit-choice-gtmo-cable-landing> Accessed October 27, 2021.

<sup>72</sup> "UCT ONE-Unit of Choice for GITMO Cable Landing, [Image 4 of 6]," (Washington, DC: Defense Visual Information Distribution Service, October 28, 2015); <https://www.dvidshub.net/image/2362993/uct-one-unit-choice-gtmo-cable-landing> Accessed October 27, 2021.

<sup>73</sup> *Submarine Cable Network in Northeast and Southeast Asia*, (Seattle: Maritime Awareness Project, National Bureau of Asian Research, n.d.), 2; <https://www.nbr.org/publication/submarine-cables/> Accessed October 27, 2021.

<sup>74</sup> *Ibid.*, *Submarine Cable Network Across the Pacific Ocean*, 3; <https://www.nbr.org/publication/submarine-cables/> Accessed October 27, 2021.

<sup>75</sup> *Europe-India Gateway*, (Washington, DC: Telegeography, 2021): <https://www.submarinecablemap.com/submarine-cable/europe-india-gateway-eig-1/>; Accessed October 27, 2021.

<sup>76</sup> Threats to Undersea Cable Communications, 1.

<sup>77</sup> See Telegeography *Submarine Cable Map*; <https://www.submarinecablemap.com/> 1; Accessed October 27, 2021; and John Hemmings, "Reconstructing Order: The Geopolitical Risks in China's Silk Road," *Asia Policy*, 15 (1)(January 2020): 14; <https://muse.jhu.edu/article/748991/pdf>

<sup>78</sup> Threats to Undersea Cable Communications, 7-8.

<sup>79</sup> New Zealand, Ministry of Transport, Protecting New Zealand's Undersea Cables, (Wellington: Ministry of Transport, 2020): 1-2; <https://www.transport.govt.nz/about-us/what-we-do/queries/protecting-new-zealands-undersea-cables> Accessed October 27, 2021.

<sup>80</sup> "Are You Cable Conscious?," (Wellington: Transpower New Zealand, 2008): 4; <https://www.transpower.co.nz/resources/cook-strait-cable-maps-are-you-cable-conscious> Accessed October 27, 2021.

<sup>81</sup> USNS Zeus, (Washington, DC: U.S. Military Sealift Command, 2020): 1; <https://www.msc.usff.navy.mil/Ships/Ship-Inventory/Cable-Laying-Repair-Ship/> Accessed October 27, 2021.

<sup>82</sup> Heiner Kubny, "Getting Started With the Arctic Connect Project," Polar Journal, (November 20, 2020): 1-2; <https://polarjournal.ch/2020/11/20/erste-schritte-zum-arctic-connect-projekt/>; Accessed October 27, 2021.