2024

Securing Subsea Cable Critical Infrastructure, Holes in the Governing Legal Framework in the United States and Internationally

Sydney Brooke Pleasic

Securing Subsea Cable Critical Infrastructure, Holes in the Governing Legal Framework in the United States and Internationally

Abstract

Submarine data cables are highly regarded as the core critical infrastructure of the digital age, with over 99% of all global communications traveling through these fiber optic lines under the sea floor.[1] These cables form the physical infrastructure that supports one of the most vital communication networks of our modern world. They are relied on by military operations, the scientific community, everyday citizens when accessing the global internet, and the finance industry with these subsea cables being responsible for carrying out roughly $10 trillion worth of financial transactions a day.[2] Given the importance of subsea cables to a functioning society and everyday life, which is only exacerbated in times of crisis, it may come as a surprise that the subsea network is often overlooked. The significance of this critical infrastructure is not entirely lost on the United States, EU, and other nations abroad. However, little action has been taken to secure the cables from current threats that both the United States and other international nations face regarding this crucial network, including threats from natural hazards such as hurricanes and tsunamis and the inevitable everyday risks of anchoring ships and fisher trollers that sever the physical cables,[3] as well as the more intentional based threats of hybrid warfare and the growing presence of authoritarian state control of subsea cables and hubs.[4]

---

[1] Lieutenant Commander Dennis E. Harbin III, *Targeting Submarine Cables: New Approaches To The Law Of Armed Conflict In modern Warfare*, 349 Military Law Review 349, (2021), https://tjaglcs.army.mil/mlr/targeting-submarine-cables-new-approaches-to-the-law-of-armed-conflict-in-modern-warfare.
[2] Colin Wall and Pierre Morcos, *Invisible and Vital: Undersea Cables and Transatlantic Security*, CSIS, (June 11. 2021) https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security.
[3] NATO CCDCOE, *Strategic Importance of, and Dependence on Undersea Cables*, NATO CCDCOE, at 1-2, (November 2019) https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.
[4] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council, at 1, (September 13, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.

In the United States, while recognizing subsea cables as critical infrastructure, no single agency or legal instrument is used to regulate and secure the network.[5] Instead, the United States government has taken a fragmented approach, delegating overlapping authority to numerous agencies with little clarity.[6] This approach has resulted in dormant authority with no agency obligated to develop policy or oversee the protection of the United States subsea cable network generally, leaving the United States and private actors ill-equipped to respond to global data and communication interruptions.

If we look internationally, nations have signed on as parties to the United Nations Convention on the Law of Sea Treaty (UNCLOS) which, is often called the Constitution for the Oceans.[7] UNCLOS is responsible for establishing a jurisdictional framework for subsea cables, creating cable protection zones for laying cables, and providing a dispute resolution framework for cable interference.[8] However, the treaty has gaps in protection; notably, the creation of cable zones poses the potential unintended consequence of increasing awareness of the location of cables which subsequently increases the likelihood of attack. In addition, UNCLOS has a history of nonenforcement[9] and was last updated in 1982,[10] thus lagging the relevant threats these cables face today. There are a number of states that have signed on to the treaty, but the continued

[5] The Communications Sec., Reliability And Interoperability Council IV, W*orking Group Report 8 Submarine Cable Routing and Landing*, CSRIC at 11 (Dec. 2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf.
[6] NOAA, *Submarine Cables: Domestic Regulation* (Oct. 4, 2022), https://www.noaa.gov/gc-international-section/submarine-cables-domestic-regulation.
[7] Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 Cath. U. J. L. & Tech at 667 (Dec. 2015), https://scholarship.law.edu/jlt/vol24/iss1/4.
[8] Oceans & Law Of The Sea United Nations, *United Nations Convention on the Law of the Sea of 10 December 1982 Overview and full text* (July 13, 2022), https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm.
[9] Christian Bueger & Tobias Liebetrau, *Protecting hidden infrastructure: The security politics of the global submarine data cable network,* Contemporary Security Policy, at 398 (Mar. 29, 2021), https://doi.org/10.1080/13523260.2021.1907129.
[10] Oceans & Law Of The Sea United Nations, *supra* note 8.

refusal of the United States to become a signatory and securing ratification to modernize the international agreement seems unlikely.

This paper aims to bring awareness to the often overlooked but heavily relied on piece of critical infrastructure, the subsea cable network. Emphasizing why the network is important to secure, why the current legal frameworks regulating the cable network seem inadequate and offering some recommendations for moving forward. Part I of this paper introduces what exactly is the subsea cable network, how it is exposed and, why prioritizing its security is so important. Part II of this paper examines the leading threats and harmful actors recognized by the United States and international nations and how they affect the subsea cable network. Part III of this paper outlines the United States' current legal framework governing the subsea cable protections and highlights the deficiencies. Part IV analyzes the history of international frameworks in place to secure subsea cables abroad leading to UNCLOS and details how the treaty comes up short of offering modern-day protection. Part V looks ahead to securing subsea cables in years to come and proposes a course of action that considers the United States' unique attributes and suggests a specific approach that the United States could adopt to fill in the gaps in its domestic policy and international obligations that follows the 3R's; Redundancy, Regulation, and Repair to achieve network resiliency.

Part I: Introduction

If you woke up this morning and logged on to social media, answered an email you received overnight, or clicked on a news article that showed up on your phone, it most likely linked you to the global internet. It appeared on your phone after traveling through some part of the 552-fiber optic cable network that lies on the ocean floor.[11] Given the expansive growth of

[11] TeleGeography, *Submarine Cable FAQ* (2023), https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

the internet, the implementation of cloud storage[12], and the COVID-19 pandemic forcing the world to shift to doing most things online,[13] we rely on this subsea cable network more than ever before. However, there are inadequate protections in place to secure such a heavily relied-on piece of communication infrastructure. To understand why these cable networks are at risk and why fixing the inadequacies in the current governing legal regimes to secure these networks should be made a priority, some background on what precisely these subsea cables are and how they work is necessary to recognize how they currently are or can be exploited.

A. What Is the Subsea Cable Network

The subsea cable network often referred to as the backbone or central nervous system of our global internet, consists of physical cables with a fiberoptic core that lay at the bottom of the ocean and allow for data and communication to be carried from one shore to another and ultimately reach your phone.[14] As of early 2023, the subsea cable network consisted of roughly 552 active or planned submarine cables that connect every continent together apart from Antarctica.[15] To offer some context three major routes include; the Trans-Atlantic which connects New York to London, the Tans-Pacific connecting Los Angeles to Tokyo, Hong Kong, Singapore, and Sydney[16] and the Americas which connects Miami to Brazil and New York.[17]

Not all cables are the same, as with many other technological developments, improvements quickly outpace the piece of technology thus, cable capacity varies a lot.[18] The

[12] Jonathan E. Hillman, *Securing the Subsea Network A Primer for Policymakers*, CSIS, at 3 (Mar. 2021), https://www.csis.org/analysis/securing-subsea-network-primer-policymakers.
[13] Jason Petty, *How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea*, CJIL, Vol. 22, No. 1, Article 18, 260, 267 (Jun. 22, 2021), https://chicagounbound.uchicago.edu/cjil/vol22/iss1/18
[14] Jonathan Kim, *Submarine Cables: the Invisible Fiber Link Enabling the Internet*, Dgtl Infra (May 4, 2022), https://dgtlinfra.com/submarine-cables-fiber-link-internet/.
[15] Submarine Cable FAQ, *supra* note 11.
[16] Kim, *supra* note 14.
[17] *Id*.
[18] Submarine Cable FAQ, *supra* note 11.

most recent cable installed called the MAREA has a capacity of 224 TBPS or 224,000 GBPS,[19] considerably greater than the FEA cable that began service in 1997 which, has a capacity of 500 GBPS.[20] While on average, cables have a minimum life span of 25 years, they often become outdated first as new cables can provide more capacity for less cost.[21]

The subsea cable market is an established sector of the global economy with prominent manufactures of the physical components, installers whom lay the actual cable, operators who oversee the continuing operation of the network, and owners who fund and benefit from the sea cables operating.[22] Building subsea cables is an expensive endeavor, past projects such as FASTER, the partly Google backed cable, cost 300 million dollars to build.[23] 2Africa currently the world's longest subsea cable, extending 45km around Africa, connecting roughly 33 countries cost just under 1 billion dollars to complete.[24] The projected was initiated by Meta but the cable is owned by a consortium of seven other international partners including: China Mobil, MTN(South Africa), Orange (French), Saudi Telecom, Telecom Egypt, Vodafone (U.K.), WIOCC (Africa), and Center3 (STC) to cover the cost.[25]

In the 1990s consortium ownership by telecommunication companies of the subsea cable network were very popular and remained so for many years.[26] Specifically with cables that offer higher bandwidth and connect to more countries whose projected length often results in higher

---

[19] *Id.*
[20] Kim, *supra* note 14.
[21] Submarine Cable FAQ, *supra* note 11.
[22] Kim, *supra* note 14.
[23] Amit Chowdhry, *Google Invests In $300 Million Underwater Internet Cable System To Japan*, Forbes (Aug. 12, 2014) https://www.forbes.com/sites/amitchowdhry/2014/08/12/google-invests-in-300-million-underwater-internet-cable-system-to-japan/?sh=61ea16201617.
[24] Mary Zhang, *Equinix Brings 2Africa Subsea Cable to Genoa and Milan*, Dgtl Infra, (Feb. 24, 2021), https://dgtlinfra.com/equinix-2africa-subsea-cable-genoa-milan/.
[25] Kim, *supra* note 14.
[26] Jill C. Gallagher, *Undersea Telecommunication Cables: Technology Overview and Issues for Congress*, Congressional Research Service, at 1-2 (Sept. 13, 2022), https://crsreports.congress.gov/product/pdf/download/R/R47237/R47237.pdf/.

initial costs.[27] The expense of building such cables has often made it necessary, or at least from an economic view point, smarter for a group of businesses to come together to spread out the cost, thus in exchange for financial backing a company would receive a portion of the cables capacity to use or sell off.[28] The eight international partners of 2Africa listed above are a classic example of a consortium ownership consisting of telecommunication carriers who all have ownership over some capacity of the cable.

Recently the subsea cable market has seen an expansion in private exclusive ownership.[29] As of 2020, 65% of cables were owned by one entity, often shorter in length and less connections.[30] Cloud service providers and Over-The-Top companies whose business model relies on fast and reliable network capacity to provide their services over the internet have been shifting to independent and exclusive ownership of cables or smaller consortium ownership rather than buying network capacity from larger consortiums.[31] In 2021 Google, Meta, Amazon, and Microsoft represented 69% of all international capacity.[32] This past March of 2023, Google's third privately owned subsea cable the Equiano, connected Portugal to South Africa and has branching units that connect to Nigeria, Togo, and more became operational.[33] Notwithstanding the very well-funded companies of Google, Amazon, Meta, and the like, have cables that are longer with more connections that and heavily used, are under an consortium ownership often

---

[27] Sherman, *supra* note 4 at 8.
[28] Kim, *supra* note 14.
[29] *Id.*
[30] Sherman, *supra* note 4 at 7.
[31] *Id.*
[32] Telegraphy, *The State of Network 2023 Edition*, at 4 (2023), https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2023.pdf?utm_campaign=Prospect%3A%20Networks%202&utm_medium=email&_hsmi=60033117&_hsenc=p2ANqtz-_UruwyJ0OHVD9afQPzsNIfB_N9ae-mCq7jFHaP2uz4rfianajj78ho7ahLCfWfn_wWCCIMzNDeUEtrMLY0ropF4pOVzqN1LxlZEMdTioDyJj8nddk&utm_content=60033117&utm_source=hs_automation.
[33] Submarine Cable Networks, *Equiano*, https://www.submarinenetworks.com/en/systems/euro-africa/equiano#:~:text=Equiano%20cable%20system%20is%20the,(St%20Helena)%2C%20etc.

consisting of different national based entities.[34] Such an ownership style of these subsea cables poses specific problems in delegating responsibilities accompanying ownership rights such as, which entity is going to take the lead in monitoring, repairing, and securing the subsea cables.

B. Manufactures and Installers of Subsea Cables

The manufacturing market representing companies who build the physical components of the subsea cable and sometimes provide installation services like laying the cables along the sea floor, are heavily dominated by a few market participants.[35] Notably, four key companies: Alcatel Submarine Network (ASN), owned by Nokia, a Finnish multinational telecommunication company, Subcom a United States cable manufacturer and installer, NEC, a Japanese multinational IT company,[36] and lastly, HMN formerly Huawei Marine Network, regarded as a Chinese state actor invested entity.[37] The market for installers have shared key players including Subcom and Alcatel,[38] Orange Marine based in France,[39] and Global Marine Systems based in Britain[40].

Manufactures of subsea cables present a threat to the security of the cable network that is worth highlighting. Given the thickness of subsea cables and the depth of the ocean that the cable lays at the bottom of, once a cable is out at sea interfering with the connection is often impractical and even if an operation is successful, it likely will be discovered.[41] However, manufactures have an opportunity to build backdoors[42] into the subsea cable, technology to

[34] Kim, *supra* note 14.
[35] *Id.*
[36] Hillman, *supra* note 12 at 7.
[37] *Id.*
[38] Kim, *supra* note 14.
[39] Christian Bueger, Tobais Liebetrau, Jonas Franken, *Security Threats to Undersea communications Cables and Infrastructure: Consequences for the EU*, European Parliament SEDE sub-committee, at 38 (Jun. 2022), https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf.
[40] Bueger & Liebetrau, *supra* note 9 at 405.
[41] Franken, *supra* note 39 at 30.
[42] NIST CSRC, *Glossary: backdoor*, NIST, https://csrc.nist.gov/glossary/term/backdoor

compromise the security of the cable network from the moment of installation.[43] Such fear has been present between the United States and China's subsea cable manufactures and installers for some time. In November of 2022, President Biden and the Federal Communications Commission (FCC), motivated by such suspicions, banned the future sale of Huawei Marine's services or equipment to the United States.[44] As a China based cable manufacturer and repairer, the decision excluded any of Huawei's subsea cables from connecting to the United States and bans any repair services to cables.

C. Exposure and Vulnerabilities to the Subsea Cables

The subsea cable network has multiple components and it is important to understand that each part represents a point of exposure waiting to be taken advantage of by malicious actors or natural occurring threats that effect the reliability of the internet and global communications. The cable, often described as being no wider than a garden hose, has a core consisting of fiber optic wires as thick as a strand of hair.[45] It is through those fiberoptic wires that the data and communications, composed of light signals, are transmitted by pulsing light that drives the signal along.[46] The cable runs along the ocean floor making it vulnerable to both intentional and unintentional causes of physical damage including fishing boats trolling the water and ships anchoring at sea, both which, are a widely attributed causes of severing cables.[47] The cables are similarly vulnerable to threats of intentional harm such as, the alleged capacity of Russia's navy

[43] Justin Sherman, *Cybersecurity Under The Ocean Submarine and US National Security*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2301, at 7 (Jan. 18, 2023), https://www.hoover.org/research/cybersecurity-under-ocean-submarine-cables-and-us-national-security.
[44] *FCC Bans Authorizations for Devices That Pose National Security Threat,* U.S. Fed. Commc'ns Comm'n (Nov. 25, 2022), https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat.
[45] Submarine Cable FAQ, *supra* note 11.
[46] OptronicsPlus, *Fiber Optics vs Copper Cabling: Understanding the Difference*, White Paper, at 3, https://optronicsplus.net/downloads/whitepapers/OP_Fibre_Optics_vs_Copper_Cabling_Understanding_the_Difference_White_Paper_Rev.1.0.pdf.
[47] Gallagher, *supra* note 26 at 10.

and its spotted activity around marine cables,[48] have been part of the North Atlantic Treaty Organization (NATO) discussions over the past few years.[49] Since the cables remain exposed on the ocean floor, the optic wires are wrapped in more layers of various materials forming a protective casing[50] that allows the cable to withstand the pressure of the ocean and a high extent of physical damage that can be associated with marine activity.[51]

The installation of the physical cable starts at a shoreline where a boat dredges the ocean floor and is followed by a cable laying ship that releases spools of cable on board.[52] As the boat and accompanying cable travels out to sea it is buried under the sea bed as a protective measure to shield the fiber optic wires from being damaged or tampered with.[53] As the cable makes its way to deeper depths where there is less human activity, the cables are simply laid on the bottom of the ocean[54] as it becomes impractical to reach the depths of the sea floor to bury the cable and there is less of a need to hide the cable for its own protection.

As the cables come up to shore, they run into a Beach Manhole which is a concrete tunnel, that allows the subsea cable to touch land as the light signal continues to a specific device.[55] Where the cable first meets land common tactics of espionage, techniques to intercept data and communications, become more feasible such as tapping. Additionally, due to the location of beach manholes on the shoreline, natural hazards such as hurricane and tsunamis are

---

[48] Harbin, *supra* note 1 at 358.
[49] NATO, *Online Press Conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defense Ministers*, (Oct. 22, 2020) https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en
[50] Kim, *supra* note 14.
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] Communications Sec., Reliability and Interoperability Council, *Working Group 4A Submarine Cable Resiliency, Final Report: Clustering of Cables and Cable Landings*, CSRIC at 4 (Aug. 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG4A_Final_091416.pdf.

recognized threats to the integrity of the cable as the physical infrastructure can be damaged or wiped out.[56]

From the beach manhole, the fiberoptic wires extension from the subsea cables continues onto to a Cable Landing Station (CLS).[57] CLS's are onshore facilities who receive the light signal, transmit it back into an electronic signal, than send the signal inland to a telecommunication or service provider's data center where the signal goes to the appropriate network and on the way to your device.[58] Therefore, at a minimum the cable will connect to two CLS's, one on each shore.[59] It is at a CLS where subsea cables systems are exposed to network attacks, for example denial of service, malware, or unauthorized access to systems as a result of hacking. Digital attacks against the subsea cables by targeting a CLS remain especially undervalued as a potential threat but at each point of the network whether on the ocean floor, at the beach manhole, or further inland at the CLS, the subsea cable network's unprotected vulnerabilities wait to be exposed to digital harm, physical damage, sabotage, and espionage from various threats.

D. Why Are Subsea Cables Important

The subsea cable network is part of the physical infrastructure that makes up the global internet and allows for international communication and data fluidity across-national borders. While there is much buzz around the idea of satellite constellations and internet drones providing internet access, subsea cables remain superior.[60] Satellites account for only 0.37% of internet access and are used primarily to provide access to the internet in less developed areas, like to

[56] *Id.*
[57] Kim, *supra* note 14.
[58] Working Group 4A, *supra* note 56, at 5.
[59] *Id.* at 4.
[60] Submarine Cable FAQ, *supra* note 11.

those who are landlocked and have no ability to connect to subsea cables.[61] Furthermore, the speed of data and communications across fiber optic cables nearly reach the speed of light[62] and the price of fiber optic cables are unmatched and will remain so for the foreseeable future.[63]

Society has become growingly dependent on cloud networks that creates an illusion in many minds that you can access something from the internet through a wireless connection. In reality, cloud storage and processing, while hosted on the internet, relies on a network of remote servers. If the remote servers lie across the ocean, anything one accesses from the cloud must cross through the physical infrastructure of the subsea cables to link to your device.[64] Same with OTT media services that rely on streaming their content over the internet.[65] That is why companies such as Amazon, Microsoft, Meta, and Alphabet (Goggle) are seeking to build their own network of subsea cables to support the need for data demand that drives their businesses.[66] These services include streaming services like Amazon Prime or Netflix, Amazon web services, OneDrive, Microsoft Teams, Outlook, Facebook, Instagram, YouTube, and Goggle maps.[67] The most recent cables installed have a capacity of carrying 250 TBPS of data or communications which can serve 3.3 million devices streaming 4k-resoultion videos at the same time.[68] This is all to say that without functioning subsea cables, the global internet which we have come to heavily depend on, would cease to exist.

Part II: Threats

[61] *Id.*
[62] OptronicsPlus, *supra* note 47 at 4.
[63] Wall and Morcos, *supra* note 2.
[64] NATO CCDCOE, *supra* note 3 at 1.
[65] Kim, *supra* note 14.
[66] Gallagher, *supra* note 26 at 3.
[67] Kim, *supra* note 14.
[68] Hillman, *supra* note 12 at 4.

Scholars who have spoken on the need to secure subsea cables which, has been aptly called the hidden infrastructure, credit the lack of awareness on its "triple" invisibility.[69] Frist, subsea cables are critical infrastructure that we rely on everyday but tend to only pay attention to the physical aspects when it stops working.[70] Second, subsea cables are underground and while we use them daily, we never seem them, [71] and as the saying goes "out of sight out of mind", one can truly claim that they are invisible. Third, cables are often overlooked simply because they are out at sea in a phenomenon called "Sea Blindness".[72] Policy makers tend to think of the sea as absent of human activity thus no need to regulate. The reality is that the subsea cable network is an undervalued, understudied, and poorly protected piece of critical infrastructure facing a wide range of threats and continued ignorance by lawmakers places the United States and countries aboard in a vulnerable position as the cables can be tampered with and consequently, the implications on our society are constrained only by an actor or mother nature's imagination.

A. Types Of Threats

The current state of the subsea cable network faces two well recognized types of threats; physical and digital. Physical threats are those situations where an actor may touch and/or cause actual damage to the physical components of the cable.[73] For example, severing the actual cable on the ocean floor, manipulating cable paths, installing backdoors into the cable before installation, or tapping. Digital threats are the potential harm that can be done to the cables or system remotely by exploiting the digital aspect of the system,[74] often referring to unauthorized

[69] Bueger & Liebetrau, *supra* note 10 at 394.
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] Wall and Morcos, *supra* note 2.
[74] *Id*.

access to the subsea cable network via exploiting a Remote Management System (RMS) and interrupting the flow of communications and data by a malware or denial of service attack.

Physical harm to the subsea cable can be purposeful or unintended. Purposeful attacks on the cable network are often discussed in terms of espionage and sabotage, the former often credited to China as a state actor and the latter to Russia.[75] Espionage does not actually damage the cable but interferes with the connection in a way to gain control of data or communications passing through the fiberoptic wires. Sabotage refers to actual damage to the cable that severs the connection and with malicious intent. Unintended damage to the physical cable includes harm caused by natural hazards such as hurricane and volcanos or, accidental damage caused by human actors.[76] The leading public and reported cause of physical damage to a cable is fisherman severing cables when dropping anchors at sea or trolling which, accounts for two thirds of all reported and attributable cable interruptions.[77]

While physical threats have taken up a lot of attention in discussing how to secure the subsea cable network, digital threats present an ever-growing concern. The development and use of Remote Management Systems by subsea cable owners has reduced the security of this piece of critical infrastructure.[78] While in April 2022, the Department of Homeland Security (DHS) thwarted a cybersecurity attack on a subsea cable connection in Hawaii, and while details remain undisclosed the supposed actors was an international hacking group that gained credentials to

[75] Sarah Kuszynski and Ginny Barns, *The Geopolitics of Undersea Cables: Underappreciated and Under Threat*, London Politica, at 8-9 (Dec. 19, 2022), https://static1.squarespace.com/static/5efb88803e2328745c7b3c39/t/639f7e25ba5e494096dd02ac/1671396903006/Geopolitics+of+Undersea+Cables.pdf
[76] *Id.* at 5.
[77] Submarine Cable FAQ, *supra* note 11.
[78] Justin Sherman, *Cybersecurity Under The Ocean Submarine and US National Security*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2301, at 8 (Jan. 18, 2023), https://www.hoover.org/research/cybersecurity-under-ocean-submarine-cables-and-us-national-security.

access the RMS.[79] To see the implications that thwarted attacked would have had on the subsea cable network, if the plan was not stopped by the DHS one does not have to look much further than Colonial Pipeline attack in 2021 when a hacking group made up of nonstate actors shutdown an oil pipeline, another piece of critical infrastructure, that led to a spike in gas prices and panic in the United States.[80]

B. Harmful Actors

Each year the subsea cable network experiences on average between 100 to 200 faults or interruptions of which the majority are accounted for by accidental and non-hostile acts.[81] This poses the question: is the subsea cable network insecure? While the network has continued to function, it does not take much imagination to see that certain state actors might have motive to exploit these vulnerabilities.

Russia Sabotage

The United States Department of Defense (DOD) relies primarily on commercial subsea cables to carry out military operations and communicate with forces oversees.[82] This quickly leads to the conclusion that if a country has the capability to cut subsea cables that the United States military relies on and subsequently launches a kinetic attack, the United States armed forces would be at an extreme disadvantage to coordinate and defend without access to their communication network. While no incident of a severed cable has yet to be linked to a state actor, Russia's naval activity has been closely watched by NATO in recent years[83] and the

---

[79] Bill Gertz, *Threat to Undersea Cable in Hawaii Highlights danger of Future Internet Disruptions*, The Washington Times (Oct. 22, 2022), https://www.washingtontimes.com/news/2022/oct/22/threat-to-undersea-cable-in-hawaii-highlights-dang/.
[80] Stephanie Kelly and Jessica Resnick-ault, *One password allowed hackers to disrupt Colonial Pipeline*, Reuters (Jun. 8, 2021), https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
[81] Kuszynski and Barns, *supra* note 75 at 5.
[82] Harbin, *supra* note 1 at 356.
[83] NATO, *supra* note 49.

United Kingdom's navy, concerned of Russia's increased presence near subsea cables, has been tracking Russian submarine activity.[84] The idea of Russia attempting to sever submarine cables is not far-fetched, they already have a history of deploying hybrid attacks targeted at communication infrastructure. For example, in 2014 when Russia invaded Crimea, the military quickly targeted the peninsula's communication infrastructure to gain an upper hand.[85] Similar tactics have been employed at the beginning of the Russia Ukraine war, seizing communication infrastructure and rerouting data and communications to Russian networks.[86]

Beyond Russia's disposition to target communication infrastructure, Russia has announced a plan to build the world's second largest navy by 2027[87], thus Russia has been investing heavily to build their naval fleet. On the coast of the Barents Sea lies Olenya Guba, a Russian naval base which houses a fleet of naval ships including the notorious Yantar classified by Russia as a research ship but, widely accepted to be a reconnaissance ship fitted to carry manned drones[88] and AS-37 mini-submarines.[89] AS-37 mini-submarines on board of the Yantar have the capacity to reach depths of at least 6,000 meters and where found off the Irish coast at such depths following the route of the Norse and AE Connect-1cables that link Europe to the United States.[90] While there is no proof of such sabotage activities, it is assumed that the Yantar

---

[84] The Guardian, *UK Military Chief Warns of Russian Threat to Vital Undersea Cables*, https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables

[85] Rishi Sunak, *Undersea Cables: Indispensable, Insecure*, Policy Exchange, at 10 (2017), https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

[86] Adam Satariano and Scott Reinhard, *How Russia took Over Ukraine's Internet In Occupied Territories,* The New York Times, (Aug. 9, 2022) https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html.

[87] Sunak, *supra* note 85 at 29.

[88] Lukas Trakimavičius, *The Hidden Threat to Baltic Undersea Power* Cables, Nato Energy Security Centre of Excellence, at 3, https://www.enseccoe.org/data/public/uploads/2021/12/the-hidden-threat-to-baltic-undersea-power-cables-final.pdf.

[89] Rona David, *Submarine Cables: Risks and Security Threats*, Energy Industry Review (Mar. 25, 2022), https://energyindustryreview.com/analysis/submarine-cables-risks-and-security-threats/ .

[90] *Id.*

and the vessels it carries can carry out missions to cut subsea cables.[91]While the entire world grows more dependent on subsea cables to carry out everyday tasks, the military is not exempt. They too are vulnerable to threats posed to the subsea cable network and as hybrid warfare grows, it becomes expected that a future physical attack would be preceded by an attack on our communication infrastructure thus, the need to secure the subsea cable network is a priority to military as well as the rest of the world.

Growing Prescence of China Sponsored Espionage and Manipulation of Cable Paths

Following the 2013 leaks by Edward Snowden, which among other disclosures, revealed that the National Security Agency (NSA) on behalf of the United States, had participated in tapping of subsea cables[92]. There was immediate backlash that led many states to question its reliance on subsea cables that crossed the United States shores. China capitalized on such distrust and announced its Belt and Road Initiative (BRI), one goal of which was for China to build what is now called the Digital Silk Road.[93]

Cable Manipulation via the Digital Silk Road

Officially declared in 2015, The Digital Silk Road through the claimed interest of improving other countries telecommunication networks, provides funding on repayment plans, materials, and installers to build 5G networks and subsea cables which link developing nations to Chinese service providers.[94] However, China's neutral motive in entering such arrangements is not well hidden. Chinese State Official remarks clearly show that China views the subsea cable

[91] Trakimavičius, *supra* note 88 at 3.
[92] Lane Burdette, *Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy*, Princeton University, JPIA (May 5, 2021), https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy.
[93] *Id.*
[94] Geoffrey Irving, *Why the U.S. Dominates the Pacific's Subsea Cable Infrastructure*, The Maritime Executive (Feb. 5, 2023) https://maritime-executive.com/editorials/why-the-u-s-dominates-the-pacific-s-subsea-cable-infrastructure.

business value as lying in access to the data "although undersea cable laying is a business, it is also a battlefield where information can be obtained"[95]. Taking a closer look at how the BRI works, it is not hard to realize the power imbalance at play that allows China to leverage access to data and communications that cross over wires without ever reaching China's shores.

BRI conditions funding on confidentiality and termination clauses that are triggered if the developing country acts against Chinese state interests.[96] The reality is that likely developing countries value the chance of access to communication infrastructure over the threat of China's access to information crossing the fiberoptic cables. Thus, Chinese entities offer affordable rates suspected to be subsidized by the Chinese government to undercut other bids[97] and has grown a significant influence over the submarine cable market without having to build cables that land at China's coast. For example, HMN a Chinese based subsea cable manufacturer and installer, was competing to build the East Micronesia subsea cable system in the pacific region that would connect Micronesia Nauru and Kiribati, submitted a bid 20% below all others and financed by The Bank of China.[98] HMN is leading the BRI in expanding the Digital Silk Road that now owns 10% of the subsea cables in the global market and has built and repaired 25% of the cables.[99]

Espionage

While companies such as Huawei Marine, rebranded as HMN, claim to have no ties to the Chinese government, China's 2017 National Intelligence Law which, forces all Chinese

---

[95] Geoffrey Starks, *Statement of Commissioner Geoffrey Starks*, U.S. Fed. Commc'ns Comm'n, at 3 (2020) https://docs.fcc.gov/public/attachments/DOC-367238A6.pdf.
[96] Burdette, *supra* note 90.
[97] European Commission, *Commission imposes anti-subsidy duties on imports of optical fibre cables from China*, (Jan. 19, 2022), https://policy.trade.ec.europa.eu/news/commission-imposes-anti-subsidy-duties-imports-optical-fibre-cables-china-2022-01-19_en.
[98] Matthew P. Goodman and Matthew Wayland, *Securing Asia's Subsea Network: U.S. Interests and Stategic Options*, CSIS, at 6 (April 2022), https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options.
[99] Franken, *supra* note 39 at 32.

citizens and organizations to cooperate with China State Intelligence services with no protections under the law, suggests otherwise.[100] It is clear that a Chinese service provider, subsea cable manufacture, and cable installer would all be subject to the law and, any data or communications that these entities might possess as a result of crossing a subsea cable they have built, owned, or operated, would give the Chinese government a legal right too. Thus, cables built on BRI funding siphons data and communications into Chinas control.

The United States has been uncomfortable with China's presence in the subsea cable market for some time and growing concerns over government ties and espionage tactics led the Justice Department in 2020 to reject a subsea cable project for the first time on national security concerns due to it landing in Hong Kong.[101] The Pacific Light Cable Network was to be the first ever direct subsea cable connection between the United States and Hong Kong.[102] Initially proposed as a joint venture among multiple entities including Google, Facebook, and Pacific Light Data Co., a Hong Kong company and subsidiary of the fourth largest telecommunication service provider in China,[103] the FCC rejected the application and cited concerns of Chinese espionage efforts. Specially, China's continued determination to acquire United States citizens data and investments in subsea cable infrastructure would be vulnerable to exploitation by installing backdoors or tapping cables.[104] While the United States has taken a clear stance that China's activity in the subsea cable market pose a direct threat to the communication network, no meaningful action has been taken to ensure that United States citizen's data will not end up in the hands of the Chinese government.

---

[100] Burdette, *supra* note 90.
[101] Department of Justice, *Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States*, (Jun. 17, 2020), https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea
[102] *Id.*
[103] *Id.*
[104] *Id.*

Digital Threats Posed by Nonstate Actors

A rarely discussed threat posed to the subsea cable network and therefore neglected to be protected from, are digital threats carried out by nonstate actors. In recent years the development and integration of remote management systems (RMS) into the manufacturing sector has risen, reducing the need of on-site personal and subsequently everyday costs of running a business, and the subsea cable market is no exception.[105] However, RMS pose a unique threat to the subsea cable network whose exposed vulnerabilities have been capitalized by nonstate actors.

Physical threats to the subsea cable system whether it be sabotaging the fiberoptic wires which requires specialized equipment to sever the cable. Espionage tactics require capital to secure a boat to reach the cable to tap or control over some manufacturing entity that could install a backdoor into the fiberoptic cable while being built. Physical threats to subsea cables typically require resources beyond an average person's means thus, purposefully carried out acts are often attributed to nations.

On the other hand, RMS exposes the subsea cable network to everyday actors with little needed capital but the skill to hack into the network system. Additionally, RMS removes the physical nexus element that has constrained physical attacks to the subsea cable network. While tapping or sabotage requires the malicious actors to be near the cable to sever or tap into the fiber optic wires, RMS allows malicious actors to gain access to cable landing station (CLS) from anywhere around the world. This allows a hacker or terrorist group to breach a CLS and interrupt the flow of data and

[105] Justin Sherman, *The U.S. Should Get Serious About Submarine Cable Security*, Council on Foreign Relations, (Sep. 13, 2021), https://www.cfr.org/blog/us-should-get-serious-about-submarine-cabl e-security.

communications through the subsea cable on the shore of Virginia for example, while abroad.

As previously mentioned, such digital threats by nonstate actors against a subsea cable network owner with a CLS on the shores of Hawaii have been identified and subsequently foiled by United States federal security officials back in April of 2022.[106] The federal officials, while carrying out an investigation on the dark web, discovered that a hacker had gained login credentials to the telecommunication service providers network in Hawaii.[107] Given United States heavy military presence in Hawaii, including military bases that house the United States Indo-Pacific Command which is responsible for coordinating military responses of an area that covers over 52% of the world,[108] the potential consequences of taking down one of the five cables that connects Hawaii to the rest of the world made the DHS quickly respond and the hacker who gained credentials was arrested abroad.[109] Protecting subsea cables network from digital attacks requires that CLS's network security measures are appropriate. Simply converting to a dual factor authentication system, which is consider a norm in cybersecurity practice today, may thwart such unauthorized access to the cables network[110]. CLS is under the operation and management of private owners and, as the Colonial Pipeline incident supports, securing critical infrastructure is often behind and overlooked, despite the important role they play in society.

Part III: United States Law

The United States' legal framework for securing the subsea cable network at the domestic and global level consists of a patchwork of international treaties, domestic laws, and regulatory authority that are outdated and ineffective to deal with the modern day and future threats to such

---

[106] Gertz, *supra* note 79.
[107] *Id.*
[108] The Washington Times, *Topic: U.S. Indo-Pacific Command*, https://www.washingtontimes.com/topics/us-indo-pacific-command/.
[109] Gertz, *supra* note 79.
[110] Kelly and Resnick-ault, *supra* note 80.

a vital piece of critical infrastructure. The United States legal regime over the protection of subsea cables consists of the 1884 Convention for the Protection of Submarine Telegraph Cables (1884 Convention), an international treaty that imposes civil penalties if a party willfully or negligently sabotages a subsea cable.[111] Pursuant to carrying out the treaty, the United States vested enforcement power via the 1888 Submarine Cable Act[112] in the United States Coast Guard to pursue those who physically damaged cables and issue fines up to 5,000 dollars, this however has a history of rare enforcement.[113] Beyond the 1884 Convention the United States', international obligations to the subsea cable network are only constrained in times of war by the 1905 Hague Regulations, the Law of Armed Conflict, and customary international obligations,[114] [discussed in Part IV].

The crux issue of the subsea cable network's security from the United States domestic perspective is that the majority of the subsea cables relied on by United States citizens, government, and businesses are owned and operated by private or state-owned telecommunication and technology companies.[115] While the United States government in recent years has validated how important the subsea cable network is admitting, that as the nation becomes increasingly dependent on the global internet and communication network, and as technological advances are made, the United States will grow more vulnerable in relying on an unsecure network.[116] However, the extent of which the United States exerts domestic legal authority over the protection of the subsea cable network encompass only the regulatory power

---

[111] *Convention for the Protection of Submarine Telegraph Cables*, [herein after 1884 Convention], (Mar. 14, 1884), https://www.iscpc.org/information/government-and-law/#:~:text=International%20Convention%20of%20March%2014%2C%201884%20for%20the%20Protection%20of%20Submarine%20Cables
[112] 47 USC § 21.
[113] Petty, *supra* note 13 at 271.
[114] NBR, *Maritime Awareness Project: Submarine cables*, https://www.nbr.org/publication/submarine-cables/.
[115] Gallagher, *supra* note 26 at 2.
[116] *Id.*

of the FCC over granting licenses to private and international state-owned entities hoping to install cable connections to the United States[117] and governmental agencies with an overlapping claim of authority to regulate where and how the cables are laid.[118]

Regulatory Authority Over Laying Subsea Cables

United States legal authority to provide protection to the subsea cable network domestically is carried out by various governmental agencies who been granted overlapping authority to manage and regulate the laying of subsea cables in waters that the United States has a territorial claim over.[119] The laying of cables requires a coordinated effort thus, governmental agencies that have been granted legal power to justify their agencies inclusion in the laying of cables is vast. For example, the United States Army Corps of Engineers, National Oceanic and Atmospheric Administration (NOAA), The Department of Interior, and The Federal Energy Regulatory Commission are all vested with overlapping regulatory authority over the laying of subsea cable that "touches seabed of the United States outer continental shelf".[120] However, the extent of each agency's role regarding how and where to lay subsea cables remains unclear with a need for coordination. The United States has a relatively straightforward process for granting subsea cables licenses, the authority over the matter has been delegated to a lead agency, the FCC.

FCC and Team Telecom

The FCC is the main governmental agency with regulatory authority over granting the approval of laying of subsea cables that connect to the United States.[121] The FCC's authority

[117] FCC, *International Affairs: Submarine Cables*, https://www.fcc.gov/submarine-cables.
[118] NOAA, *Supra* note 6.
[119] NBR, *supra* note 112.
[120] NOAA, *supra* note 6.
[121] FCC, *supra* note 117.

resides in a grant of power pursuant to the Cable Landing License act of 1921[122] and Executive order No. 10530[123] which, vested the agency with power to review then grant or deny license applications to build and operate subsea cables that connect the United States on the condition it seeks advice from the Executive Branch and approval from the Secretary of State.[124] When an entity is looking to build a subsea cable to the United States it must apply to the FCC for approval, but the FCC does not work alone, if the project has more than 10 % foreign ownership the FCC seeks a Team Telecom review.[125] The Committee for the Assessment of Foreign Participation (Team Telecom) is a body made up of various security agencies including Department of Defense (DoD), Department of Justice (DoJ), and Department of Homeland Security (DHS)[126], they review the foreign ownership of subsea cable applications and make recommendations on whether the subsea cable project poses a national security threat to the United States and, if so, they would recommend denying the application.[127] Team Telecom recommended to the FCC to deny the Pacific Light Cable Network that connected to United States on Hong Kong under such national security concerns back in 2020.[128]

Private Agreements: Oregon Fisherman Cable Commission

The United States subsea cable sector is unique in that the United States government privately owns only two subsea cables linked to Guantanamo Bay, out of the rest of the subsea cable network, 22% of cables have at least one private United States owner. [129] Given the

[122] 47 U.S. Code Chapter 2.
[123] National Archives: Office of the Federal Register, *Executive Orders (Executive Order 10530, Part IV)*, https://www.archives.gov/federal-register/codification/executive-order/10530.html.
[124] FCC, *supra* note 117.
[125] Gallagher, *supra* note 26 at 14.
[126] Adam Chan, *CFIUS Team Telecom and China*, Lawfare,(Sept. 28, 2021), https://www.lawfareblog.com/cfius-team-telecom-and-china.
[127] Gallagher, *supra* note 26 at 14.
[128] *Id.*
[129] Sherman, *supra* note 4, at 23.

dominated private ownership of subsea cables that connect to the United States beyond federal authority there is a notable trend of private agreements that regulate subsea cable protection domestically once they have been installed. An example of such an established working arrangement is the Oregon Fisherman Cable Commission (OFCC).[130] The OFCC involved the coming together of two industries, the commercial fishing and telecommunication industry, that had a shared interest in regulating marine activities off the cost of Oregon.[131] Representatives of both industries come together and negotiated a cooperative agreement to minimize interferences with each other to the benefit of both business so they could thrive in the shared use of the sea.[132] The agreement established procedures that must be followed when a boat is operating near a subsea cable as well as a procedure if a boat make contact with the cable.[133] The agreement also includes the establishment of a 24 hour hot line whose operators are granted authority to approve the cutting fishing gear if it is snagged to a fiberoptic cable on the sea floor and the fisherman were provided monetary reimbursement for their damaged equipment from a compensation fund also created by the agreement.[134] Under the agreement the telecommunication entities agreed to employ reasonable care in installing and maintaining subsea cables that would avoid interference with the fishing activities.[135] Both entities vowed to communication and cooperation to continually ensure both industries would survive.[136] While not delegated legal authority, private agreements take advantage of legally binding written agreement so private entities like the

[130] NOAA, *Supra* note 6.
[131] OFCC, *About Oregon Fisherman's Cable Committee*, http://www.ofcc.com/TycoOFCC%20Agreement.pdf.
[132] *Id.*
[133] OFCC, *Procedures to Follow While Operating Near Submarine Fiber Optic Cables*, at 1-2, (Feb. 6, 2017), http://www.ofcc.com/Procedures2.6.17.pdf.
[134] TycoOFCC, *Agreement Between The Oregon Fishermen's Cable Committee, Inc., And Tycom Networks (US) Inc.*, at 1, http://www.ofcc.com/TycoOFCC%20Agreement.pdf.
[135] *Id.*
[136] *Id.*

OFCC can come together and take advantage of shared interests to ensure the protection of subsea cables from accidental acts.

Notwithstanding innovation solutions to protect the subsea cable network such as private agreements like the OFCC above, the domestic law the United States has at its disposable to secure the subsea cables is insufficient. The United States' legal arsenal contains inadequate enforcement powers and penalties rather, the most used legal authority is a grant of regulatory power over issuing licenses, the governmental agencies that have been granted legal say over the laying of the subsea cables is overlapping to a point that the government would likely result in a standstill if the powers were ever invoked at the same time. The state of the United States domestic law in governing subsea cables is missing a leading body of power with clear authority to create procedures, policies, enforce penalties, or coordinate a response, leaving the United States unable to efficiently respond to the security of the system if there ever was a targeted threat.

Part IV: International Law

The security of subsea cables from an international perspective poses an interesting conundrum given that subsea cables can be owned by multiple entities based in different countries, the cable itself connects to multiple countries with different legal regimes, and the cable runs through various parts of the ocean where different or no countries legal regimes reach protecting subsea cables where single parts can have a different, none, or multiple jurisdictional claims over it, a test of coordination and cooperation has been key. Thus, subsea cables have a long history of being governed by international treaties trying to define legal protections and jurisdictional authority. The most recent and comprehensive agreement among nations is the United Nations Convention Law of Seas (UNCLOS), but parties absent from it and gaps left in

its place are filled by earlier international agreements and existing national domestic law. This necessitates a discussion of all binding treaties in order to understand what exactly is protected under the international agreements.

A. Timeline of International Treaties

The 1884 Convention for the Protection of Submarine Telegraph Cables (1884 Convention)

The 1884 Convention is the first international agreement and subsequently the oldest to still be in effect that attempts to provide protection to subsea cables.[137] The 1884 Convention was adopted in Paris, today the treaty is only in force in 36 of original party nations.[138] The treaty's protections were applied retroactively to all parts of the subsea cable network that reside on the ocean floor in the high seas.[139] Article 2 conveys the purpose of the Convention that any purposeful or culpable negligence of physical damage done to a subsea cable that interrupts the data or communications passing through the cable, is a punishable crime.[140] Article 10 granted war vessels of signed party nations the authority to board a vessel at sea suspected of damaging subsea cables, excluding other naval ships.[141] To enforce the 1884 Convention, each signed party was to create domestic laws to carry out the obligations of the convention.[142] The United States remains a party to the 1884 convention and thus all international obligations imposed by the treaty however, has acknowledged later that the treaty developments as customary international law that it will follow as long as other nations do so.[143]

---

[137] 1884 Convention, *supra* note 111.
[138] NOAA, *Submarine Cables: International Framework*, (Mar. 1, 2019), https://www.noaa.gov/general-counsel/gc-international-section/submarine-cables-international-framework#:~:text=The%20Convention%20was%20concluded%20at,terms%20to%20protect%20submarine%20cables.
[139] 1884 Convention, *supra* note 111 at Article 1.
[140] *Id.* at Article 2.
[141] *Id.* at Article 10.
[142] *Id.* at Article 9.
[143] NATO CCDCOE, *supra* note 3 at 4.

The limit of the 1884 convention is that for there to be a violation, it has to be willful and cause physical damage to the cable that interrupt communications crossing therefore, it clearly covers sabotage of cables but likely not espionage which, often never have physical damage to the subsea cable and never interrupts the flow of data.

1907 Hague Regulation's and Law of Armed Conflict

1907 Hague Regulations (Hague) has great and specific importance to the protection of subsea cables. Hague is the only legally binding treaty enforced today that regulates the protection of subsea cables during times of war.[144] Article 54 of Hague states that attacking subsea cables, specifically that seizing and/or destroying of subsea cable that connects an occupied country and a neutral territory, is a lawful activity during war time.[145] The treaty states that targeting submarine cables during times of war is acceptable if it meets the test of absolute necessity and on the condition that the cables are restored or countries affected by the interruption of the cable are compensated at the end of the war.[146] The implications of the Hague regulations is that espionage, and more specifically sabotage, of subsea cables as a military missions during on ongoing war is likely acceptable.

The Law of Armed Conflict (LOAC) has interesting implications for attacking subsea cables during wartime as well. Under the LOAC military infrastructure remains a lawful target for attack, if a piece of infrastructure is used by both the military and civilians, it still considered a military object lawful to be targeted[147] if the attack is proportional considering its dual use[148].

---

[144] Harbin, *supra* note 1 at 351.
[145] *Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex*: *Regulations Concerning the Laws and Customs of War on Land*, art. 54, (Oct. 18, 1907), 36 Stat. 2277 [hereinafter 1907 Hague Regulations], https://ihl-databases.icrc.org/assets/treaties/195-IHL-19-EN.pdf.
[146] Harbin, *supra* note 1 at 372.
[147] *Id.* at 369.
[148] *Id. at* 368.

Given that 95% of military communication by DoD are sent through commercial subsea cables[149] the DoD would have to take reasonable measures to sperate its use of cables from the civilians while responding to armed attack. Thus, under the Hague and LOAC both espionage and sabotage of subsea cables seem to be legal during times of war.

The Geneva Convention on the High Seas and on the Continental Shelf 1958

The Convention on the High Seas (High Seas) adopt all protections offered to subsea cables under the 1884 Convention but established as a fundamental right to freedom to lay subsea cables in the high seas.[150] The Convention on the Continental Shelf (Continental Shelf) simply adds to the 1884 convention and High Seas that, nation states cannot obstruct the construction of subsea cables that lay outside the territorial sea.[151] Given that the only difference from the 1884 Regulation and the High Seas and the Continental Shelf is the inclusion of the right to construct subsea cables and freedom to do so unobstructed, the same gaps in protection in 1884 regulation are still present. That is espionage to subsea cables remains legal given it does not obstruct ones fundamental freedom to construct subsea cables and it does not damage or interrupt the flow of data and communications across the cable.

The United Nations Convention on the Law of the Sea (UNCLOS)

UNCLOS, which superseded the Convention on the High Seas and Continental Shelf[152] was adopted and signed by member state parties in 1982 and stands as the most comprehensive legal framework governing subsea cables to date, with over 150 member states parties to the

[149] *Id*. at 369.
[150] *Convention on the High Seas*, Article 26, (1958), https://www.iscpc.org/information/government-and-law/#:~:text=Convention%20on%20the%20High%20Seas%20(1958).
[151] *Convention on the Continental Shelf*, Article 4, (1958), https://www.iscpc.org/information/government-and-law/#:~:text=Convention%20on%20the%20Continental%20Shelf%20(1958).
[152] Submarine Cables: International Framework, *supra* note 138.

convention including China and the Russia Confederation[153] but excluding the United States. [154] UNCLOS approach to regulating and protecting the subsea cable networks was by dividing the ocean's territory into zones, each with a different legal status and regulations.

The first zone is called the Territorial Sea, it extends from the coastal state's shoreline outward for twelve nautical miles.[155] Within this water the costal state has legal jurisdiction over subsea cables being built through the water thus, can require permits for cables to cross through or deny cables being built and their domestic law governs what the costal state deems to be illegal.[156]

The second zone is called the Exclusive Economic Zone which, is not to go beyond 200 nautical miles out from the costal shoreline.[157] In the Exclusive Economic Zone, any state may lay cable on the ocean floor or burry the cable into the continental shelf.[158] In the EEZ it is unclear who has legal jurisdictional control over the cable, the cable owners or costal state, it is suggested that the cable owners may exercise their legal rights to lay cable but shall comply with costal law to the extent that no conflict forms.[159] The last zone is the High Seas which, is outside of any state jurisdiction thus anyone is free to lay cable.

Article 113 of UNCLOS carries over the requirements of 1884 convention that required party states to adopt laws that criminalized and penalized purposeful or culpable negligence of physical damage done to a subsea cable that interrupts the data or communications passing

---

[153] UNCLOS, *supra* note 8.
[154] Submarine Cables: International Framework, *supra* note 138.
[155] *Id.*
[156] *Legal Regimes Chart United Nations Law Of The Sea Convention (1982)*, at 2, https://www.iscpc.org/information/government-and-law/#:~:text=action%20for%20damages.-,Legal%20Regimes%20Chart,-Adobe%20Acrobat%20Document.
[157] *Id.*
[158] *Id.*
[159] *Id.*

through.[160] Thus, UNCLOS leaves a continued hole in the protection of subsea cables regarding espionage campaigns.[161] Tapping or interfering with the cable before it is laid that does not cause physical damage to the cable component and does not interrupt the passing communication are not considered a punishable offense under UNCLOS.[162] Therefore, while UNCLOS is the most comprehensive legal regimen providing protection to the subsea cables, it has glaring deficiencies, that being that espionage can legally be performed in any part of the ocean unless the coastal state's domestic law makes it a crime and the espionage occurs within the state's territorial sea.

Part V: Moving Forward for the United States

Three Rs of Resiliency

Most who are at least aware of the subsea cable network can agree that it is one of our most vital pieces of critical infrastructure, yet nobody has taken any real steps forward to protecting the network. Regardless of the advantages that may come from the dominantly private owned and operated subsea cable network supporting the United States, a stronger legal framework with clear governing roles, laws, illegal conduct, and fines is necessary. At the very least the United States should modernize its regulatory legal framework to close off the network's vulnerabilities from the clearly identified human and non-human actor posed threats. Nations internationally, both those party to UNCLOS and those who are not, need to consider filling the gaps left by the UNCLOS and the domestic laws. While nations can debate whether the likelihood that an amendment to UNCLOS is possible to cover espionage tactics, the most common purposeful attack to the subsea cable network, it is left unregulated by UNCLOS. It

[160] *Id.*
[161] *Id.*
[162] *Id.*

may be time to embrace the idea that one size does not fit all, and it would be beneficial to consider turning to national regional agreements to secure subsea cables compatible with the individual needs of smaller areas. To ensure the sustainability of the United States subsea cable network, my recommendations for future action is the adoption of a broader and updated legal framework that focuses on the three "R's" of resiliency that includes regulations, redundancy, and repairs.

Regulations

When it comes to the harmful threats and actors of the subsea cable network identified in this paper, natural hazards represents one of larger percentages of attributable causes of breaks and interruptions to the cable network each year. Unlike human actors who are sentient beings that understand laws and whose behavior can be controlled by enforcement powers of penalties or fines, mother nature cannot. Thus, the United States current domestic legal regime, focused on regulatory power, is adequately setup but is simply being underutilized to protect the cable network from natural hazards, leaving the heavily relied on critical infrastructure vulnerable to the will of storms.

Defending against natural hazards is one the quickest changes that the United States government can make in regard to closing off the United States subsea cable networks exposed vulnerabilities. My suggestion for defending against natural hazards, is simply taking the current regulatory scheme being used by the federal government that being the FCC's license granting authority, and have the FCC take natural hazards into consideration and pass on the concerns to subsea cable owners when they apply for a license.

When the FCC approves a new subsea cable, it should attach conditions to its approval or involve in the license application that the site of the cable landing station (CLS), which remains

vulnerable to natural hazards due to their proximity to shore line, be selected only after thoroughly considering the location's vulnerability to threats of hurricane, tsunamis, mudslides, etc. CLS's can be built on coastal land that experience infrequent hurricanes and tropical storms, like higher up on the east coast shore versus its southern coast counterpart which, would increase the subsea cables network resiliency. Additionally, the physical infrastructure making up the subsea cable connection can be reinforced with durable material to achieve a better chance of survival against riding out natural disasters. CLS's that are built in risky areas can incorporate waterproof elements into the CLS building or spend money on ensuring the beach manhole, a very vulnerable point of the subsea cable connection, can survive the pressure of storms when the ocean meets the shore. The general idea is to use conditions attached to approval of a license that the FCC has already be using and take national security measures into account to ensure owners take natural hazard threats into account when applying for a license.

Using the FCC's current regulatory power by attaching conditions to the approval of licenses can be used to reduce vulnerabilities facing the subsea network that have been identified in this paper. When it comes to digital threats that the subsea cable systems have faced, the regulatory authority of FCC can be leveraged to reduce the network's exposed vulnerabilities to such digital harms posed by Remote Management Systems. My suggestion would be granting licenses to build subsea cables and the continued right to operate the connection to network on the condition that the cable owners, and thus CLS manager, stay informed of developments in the field of digital vulnerabilities and continue to adopt best practices based on an industry custom standard.

As shown in Colonial Pipeline and the Hawaii subsea cable incident mentioned above, when it comes to digital threats there is a tendency for critical infrastructure to not stay current

on cybersecurity. Attaching conditions to compel owners to stay up to date on digital harms and adopt best practices, like dual factor authentication systems, would force cable owners to ensure they are thinking about the digital harms to the system. Thus, the FCC in granting approval for a license can require the CLS to adopt security measures to ensure the digital aspect of the CLS is not compromised. Additionally, I suggest that the CLS be forced to adopt physical security measures to ensure there is no unauthorized access via physical intrusion into the CLS. This could require the CLS to maintain cameras on the property, fence in the location, and use camouflage techniques to hide the purpose of the CLS to onlookers.

The last place where I propose where the current regulatory power of the FCC could be leveraged by placing conditions on granting subsea cable owners a license, is targeted at physical intentional damage. Whether it is the United States or a nation abroad that is a member of either UNCLOS or the 1884 Convention, purposefully damage a subsea cable that interferes with the passing of data or communications along the fiber optic wires, is a crime. The main issue with protecting our subsea cables against sabotage is the lack of ability to patrol the sea. However, I suggest that the FCC have the ability to grant licenses on the condition of attaching sensors to the subsea cables that could alert of activity nearby. Sabotage is unique in that it is an established crime but obtaining proof or crediting the attack to an actor is hard given the expansiveness of the subsea cable network thus, a solution would be instead of patrolling the seas, the sensors alert and obtain proof of damage done to the cable.

Fishing boats trolling the water and ships anchoring at sea, represent the largest attributable percentage of breaks and interruptions to the cable network each year. One of

the unique approaches that has been the result of the United States largely private subsea cable network to help reduce such unintentional harm has been the creation of the private agreement between subsea cables owners and fishing industries. My suggestion is that private agreements should be more often considered when it comes to protecting against unintended physical damage to subsea cables. Where damaging the subsea cable is not malicious, shifting toward an enforcement of penalty approach is ill advised. Especially where, we as a nation benefit from both industries having access to the shared use of the oceans. Thus, I suggest that mutually beneficial agreements be promoted, by sharing best practices of what worked for successful agreements rather than fine for unintended but physical damage to the cables by commercial fishing industry.

There is the potential to condition the use of sensors on granting approval of an FCC license to acquire proof and coordinate responses to sabotage or tapping attempts by state actors against the United States subsea cable network. Additionally, I acknowledge that there is the potential use of granting an FCC license on conditions to protect against espionage by requiring encryption, thus if United States data ends up being routed to China, it would be harder to access. However, mandatory encryption is far from an ideal solution, for it is always possible for the data to be decrypted. Therefore, the United States current regulatory domestic law remains inadequate to deter sabotage or espionage, this is primarily due to focus of attention being placed solely on regulatory powers not on enforcement powers. Thus, while there has been willful violations of the United States domestic law and international obligations that are in place to protect the subsea cable network from purposeful tempering, the Coast Guard's granted enforcement power over violations of law is fully focused on sabotage and has gone unpursued.

The regulatory application of power, granting conditions to FCC licensing, has appeal for it provides a quickly implemented solution by using a power system already in place, that being the granting of FCC licenses to cable owners with conditions regarding national security concern. My opinion and recommendation are that there is a clear lack of protection under regulatory law, domestic law, and international obligations that leave the subsea cable network exposed especially to espionage where no clear enforcement path is available to deter such actions. Thus a strong enforcement scheme with clear authority, delegated duties, and penalties and fines is necessary to deter attempts of physical attacks on the subsea cable network.

Redundancy

Redundancy is another way for the United States to protect the subsea cable network from natural hazards. When it comes to building a more resilient subsea cable system the importance of redundancy can be shown by Tonga. Tonga consists of a main island with roughly 170 surrounding outer islands out at sea.[163] Tonga has one subsea cable connecting its country and its inhabitants to the Internet.[164] In January of 2022 a volcanic eruption and earthquake hit Tonga and destroyed the only connection it had to the subsea cable network and thus, to the global Internet.[165] It took several weeks to repair the island's main connections and months for the outer islands.[166]

Redundancy is considered the best way to ensure that the subsea cable networks and thus countries connections to the global internet are secure from natural disasters. There is a low

[163] New Zealand Foreign Affairs & Trade, *About Tonga*, https://www.mfat.govt.nz/en/countries-and-regions/australia-and-pacific/tonga/new-zealand-high-commission/about-tonga/#:~:text=Tonga%20is%20a%20group%20of,as%20the%20Kingdom%20of%20Tonga.
[164] Gallagher, *supra* note 26 at 10.
[165] *Id.*
[166] *Id.* at 10-11

likelihood of a country being affected by natural disaster and that the harm is caused by an unintentional threat and non -human actor that cannot be controlled by regulators with authority to penalize. The only real way to secure the network from such an unpredictable threat is build more resilient physical infrastructure. One way to build resiliency is to build more connections to the subsea cable network and increase the likelihood that if hit by natural disaster not all connections will fail.

Additionally, promoting redundancy by investing in building multiple connections to a landmass helps secure the subsea cable network from sabotage. If a cable is severed intentionally by a human actor and there is more than one connection to the country, the data and communications will simply go to the next available route thus, while severing a cable can take time and money to repair, dealing with permits to access the cable for repair and other bureaucratic matters, the flow of data communication will not be lost. Focusing on building redundancy also protects from the potential of an intentional cutting of communication networks before a military strike.

Repairs, Ships, and Trust

Repairs are essential to the protection of the subsea cable network against physical attacks by state or nonstate actors. My recommendations under the repair prong for building a more resilient subsea cable network is twofold. Frist, when I recommend the importance of ensuring the United States has repair capabilities, I am discussing the resource to repair physical cables that have been sabotaged by state actors. Second prong, under repair that I am recommending is, repair the broken trust after the Snowden revelation that has allowed China to expand its espionage campaign in our broken relations with many international countries.

Cable repairs are likely more complicated than one might think, beyond the initial barriers of expense to repair subsea cables, they take place out at sea. Poor weather can leave a boat stranded waiting for better weather so it can carry out the repair. Beyond expense and poor weather, crossing through the ocean in a zone that is not the high sea but off a costal state you might be required to wait for a permit by that coast state's government. The United States Department of Transportation (DoT) has authorized the Cable Security Fleet consisting for two government authorized privately owned ships to be on standby to repairs damages to cables affecting United States national security that may or may not be touching United States Boarder in the National Defense Authorization Act for Fiscal Year 2023.[167] Thus, I recommend that the United States should push its private owned entity cable owners to join the International Cable Protection Committee (ICPC), to ensure access to more resources to repair cables. The ICPC is made up of 170 members and accounts for 97% ownership of the world's subsea cables.[168] The entity pools resources and helps with coordinating fleets of ships to repair subsea cables when necessary. Quick and well executed repairs have, the capacity to secure our subsea cable network from sabotage. While it is unrealistic to patrol the high seas for malicious actors, responding quickly and repairing intentional cutting and damaging to the cables defeats the purpose behind the attack by limiting the total disruption that occurs.

Following the Snowden disclosures that revealed that the United States had been tapping subsea cables, many countries grew hesitant about their nations data and communications passing through the United States subsea cable network. China

---

[167] *National Defense Authorization Act for Fiscal Year 2023*, at 1710, (Dec. 7, 2022), https://docs.house.gov/billsthisweek/20221205/BILLS-117hres_-SUS.pdf

[168] Kevin Frazier, *On Protecting the Undersea Cable System*, Lawfare https://www.lawfareblog.com/protecting-undersea-cable-system.

capitalized on this distrust and offered its Digital Silk Road plan to build its subsea cable network out that allowed for greater access to large volumes of data that allows them to carry out espionage campaigns by siphoning data to its mainland. If the United States wants to protect its data from ending up in China's hands, it must take a global approach to ensure its allies and partners are not using subsea cables built by Chinese backing or with Chinese entity ownership. For subsea cables are vulnerable to the weakest link approach that being if one cable is under a Chinese espionage campaign, all data is vulnerable. My recommendation to protect United States reliance on the subsea cable network from espionage is to build trust with nations aboard so they come back to using United States subsea cables and reduce China's growing control over the subsea cable network. Building trust between nations is hard but common practices used in other areas of international law is sharing best practices to build dialogue between nations and offering capacity building with no strings attached.

Part VI: Conclusion

There is no denying that as a society we have become increasingly dependent on the global internet and data communication network for everyday activities such as work, school, banking, social media, and watching tv. Additionally, our national and global institutions such as the banking and financial sector of our economy, as well as the military have become increasingly dependent on this subsea cable network. Based on above evidence the United States needs to take a more proactive approach to securing the nation's data. By using the 3 R's, the country will be better protected from being cut off from cables and data ending up in the wrong hands which, is not a question of if but, when.