BUILDING AN INTERNATIONAL REGULATORY REGIME IN SUBMARINE CABLES AND GLOBAL MARINE COMMUNICATIONS

by
Amy Min-Jung Paik

A dissertation submitted to Johns Hopkins University in conformity with the requirements for the degree of Doctor of International Affairs.

Baltimore, Maryland
December 2022

Abstract

About 95 percent of worldwide Internet traffic travels from one continent to another through submarine communication cables working around the clock, while only the remaining 5 percent relies on satellite for communication (Coffey 2014, 28; van Ouderaren 2021). Thus, what seems to keep military officers and national security strategists in many states awake at night is the possibility that some military submarines have the capability of cutting submarine communication cables. For example, it is known that a Chinese submarine, *Jiaolong*, has such capability (Kim 2012, 68) as well as a Russian submarine Yantar (Fuller 2021).

A concern here is that in international waters there are not effective laws to hold the attacker responsible when the submarine cables are physically damaged as a result of physical attack by a state.

The purpose of this study is to find out which international legal regime applies to submarine communication cables and global marine communications. It also suggests some modifications for improving the current international legal system so that sensitive information, such as our email exchanges and health records, and the cables that carry this information can be better protected. To explore these questions, I have chosen to employ a historical approach, case studies, and insights from experts to inform my study.

In this dissertation, I apply the theory of international cooperative regime-building to the submarine communication cable industry and emphasize the South Korean government's

potential role as a catalyst in developing new norms. As one of the leading suppliers of fiber optic cables (Kim 2020), South Korea can play a crucial role in developing an international regime--and identifying the challenges to the current regulatory regime for submarine communication cables.

During this process, I intend to test a hypothesis that submarine cables are not being adequately regulated under the current international legal regime. Where I identify gaps in international law currently protecting submarine cables, I also offer policy recommendations to improve the regulatory regime, such as the idea of granting the right to punish an attacker under the cable owner's jurisdiction rather than that of the attacker's jurisdiction when the cable is laid in high seas—the position that UNCLOS currently takes according to Article 113.

DIA Committee Members

Chair and Primary Reader: Professor Kent E. Calder, JHU SAIS

Secondary Reader: Professor Steven M. Schneebaum, JHU SAIS

Third Reader: Professor Thomas E. Kellogg, Georgetown University Law Center

Acknowledgments

I am grateful to God who has given me life, bestowed upon me wonderful and supportive family members, friends, and professors. Thank you Lord for watching over me and allowing me to grow in your love.

Table of Contents

List of Figures

Acronyms

ACE Cable	Africa Coast to Europe Cable
ILC	International Law Commission
IRB	Institutional Review Board
LS Cable	LS Cable & System
NBR	National Bureau of Asian Research
ROK	Republic of Korea
PEACE	Pakistan and East Africa Connecting Europe Network
UNGA	United Nations General Assembly
UNCLOS	United Nations Convention on the Law of the Sea

1. Introduction: Recognizing the Geo-Economic and Strategic Importance of Submarine Cables

The Africa Coast to Europe (ACE) submarine cable,[1] an internet highway between the African coast and Europe, was cut in April 2018, causing a two-day blackout for internet users. No one knows for sure why or how the submarine communication cable was cut, although it has been reported that a country in West Africa, Sierra Leone, appears to have approached the ACE cable. Unlike a missile attack, whose action is easily observable, the cut on submarine communication cables laid on the seabed takes place underseas, making the victim state less able to hold the attacker responsible. Having the attacker state admit responsibility for its action is a challenge.

The government officials in various nations live with the fear that a hostile foreign power may cut submarine communication cables intentionally, causing visible sabotage (Edwards 2018). The April 2018 incident affected at least 10 states. For example, direct effects were felt in Guinea, Senegal, and Liberia in Africa, where millions of people lost access to the internet (Baynes 2018).

Being in darkness causes not only inconvenience but also financial loss for internet

[1] The ACE cable network is twelve thousand km-long and connects eighteen states, including France, Portugal, Spain, Senegal, Nigeria, and Mali. It is owned by the ACE Consortium made up of France Telecom Orange and its subsidiaries, including Orange Mali and Sonatel (Capacity 2012).

users because the present-day global economy runs on the existence of online trading platforms. Any stoppage in the trading market due to a cut in submarine communication cables would cause tremendous financial loss. The latest figures show that financial transactions worth a total of $10 trillion are made daily via submarine cables (Wall 2021). A platform shutdown due to an intentional cut in submarine communication cables could cause a disaster in the global financial industry.

As this example illustrates, international society relies on submarine communication cables now more than ever. Even when coronavirus hit the world in 2019, our lives went on. The digital infrastructure let us continue our business with Zoom, Amazon, and online banking (Hillman 2021). Also, we were able to continue school during the pandemic, thanks to the technology that let us stay connected through the internet. As data from the Asia-Pacific Economic Cooperative Forum suggests, submarine communication cables carry about 95 percent of our data; the rest is transferred via satellite (Edwards 2018; Coffey 2014, 28; van Ouderaren 2021).

Communication through the internet began with the invention of a stable submarine communication cable network, but long before the age of the open-source internet arrived in 1991, the telegraph cable was invented in 1844. Made of a 5mm copper wire core wrapped in a protective casing of tar, hemp, and steel, the telegraph cable was developed by Samuel F.B. Morse. It carried Morse code, predating the age of the telephone. Morse inaugurated the first

telegraph cable in 1844, connecting Washington, D.C., and Baltimore. The U.S. and Britain laid the first telegraph cable underseas in 1858 (Little 2021).

The first message that went underseas was from Queen Victoria to President Buchanan, congratulating the two nations' success in completing this project in connecting two nations underseas (Gillian 2000). Then, Alexander Graham Bell invented the telephone cable, composed of copper in 1881. It went through the advancement process by instituting a tensile steel wire strand at the center, which allowed it to be laid underseas safely in 1956.

The large gap between 1881, when the telephone cable was invented and used on one continent, and 1956, when the cable was laid underseas, exists because of a variety of technical failures. For example, whether copper should be used as a proper component for cable, or where the cable should be landed, and many other issues were being debated by multiple parties for years, which delayed the whole development process (Fermandez 2022).

The first telephone cable, called the Transatlantic Telephone Cable System (TAT-1), went underseas to connect the continents in 1956. In addition, the fiber-optic submarine cable was introduced in 1956 (Matis 32, 2012). German physicist, Manfred Borner created it for communication (Little 2021).

Figure 1. Development of submarine communication cables (Source: Davenport. 2021. "International Interference with Submarine Cable Systems in Peacetime: Gaps in International Law," Center for International Law, National University of Singapore)

Telegraph Cables (1844-1950s)	Telephone Cables (1956-1986)	Fiber-Optic Cables (1986-present)

The change in core material from steel to fiber-optic cable hastened the internet revolution. Telephone cables were originally designed only for voice transmissions and had a limited bandwidth, or cable capacity.[2] Fiber-optic cables[3] with their larger bandwidths carry more data than telephone cables. Furthermore, fiber-optic cables can transmit data more quickly than telephone cables. Fiber-optic cables carry signals at speeds up to the speed of light,

[2] The cable capacity is the maximum rate of data transfer, measured in gigabits per second (Swinhoe 2021).

[3] Dr. Narinder Singh Kapany, a UK-based physicist discovered fiber-optic cables in 1952 (Stephen 2020).

equivalent to 2,000 megabytes per second (Mbps), unlike telephone cables, which carry signals at 280 megabytes per second (Mbps).

This technology allows us to download a movie within a few minutes and join stable videoconferences via Zoom or Microsoft Teams with one click from our computers (Cheong 2013). The internet speed via fiber-optic submarine communication cable networks is far faster than the average speed of satellite internet service, which is between 12 and 100 Mbps (Anders 2021; Balakrishanan 2014).

According to the Cisco submarine cable market forecast, the bandwidth demand worldwide is expected to double every two years, as our global data consumption continues to increase (Cisco 2019, 33) dramatically since the outbreak of COVID-19. The term bandwidth refers to cable capacity—a range of frequencies within a given band used for transmitting signals. As the demand for internet increases, more submarine cables are in demand to provide the necessary stability. The demand for submarine communication cables has been rising, as people's use of cloud services, mobile devices, and mobile technology such as 5G upon which submarine communication cables rely for operation increases (Kim 2022).

Another merit of fiber-optic cables is that they can carry signals much farther than the average copper cable, which can only carry signals 328 feet. With fiber optic cables, digital signals can be carried 132,000 feet, equivalent to 25 miles. Long distance is not a problem in communication, thanks to the invention of fiber-optic submarine cables. Now, meetings can

take place remotely on Zoom, thanks to advancement in submarine cable technology. Participants are connected across long distances, saving the costs of international business trips.

In addition, submarine communication cables are widely used and dominate the communication technology industry due to their superior pricing and speed compared to those of satellites (Burnett 2021, 1066). The figures suggest that satellite internet costs about twice as much as cable internet. Satellite internet costs more, for example, $250 for 100 Mbps, than does submarine communication-based internet service, which costs $80 for 500 Mbps, meaning that submarine cables provide faster internet at a lower price (Koeppel 2019). Therefore, the general public rarely uses satellite communication because of the associated high price of calls. Only some government officials, military members, or people in large businesses can make better use of satellites than of submarine communication cables (Wakefield 2021).

The thought of one state attacking a submarine communication cable that connects at least two other states has become an international topic, as more states have started discussing this matter publicly. Under the leadership of Captain Ashley Roach, representing the U.S., as chair, 22 international law scholars from 14 nations are currently participating in a committee on submarine cables and pipelines in the International Law Association (Roach 2022). The topic of submarine cables and international law has been discussed in the UN as well.

In December 2021, a draft resolution titled, “Oceans and the Law of the Sea,” with parts

addressing submarine cables, was adopted with 131 UN member states in favor; 4 abstentions from Columbia, el Salvador, Nigeria, and Venezuela; and 1 "against" vote from Turkey (UN 2021). Building on this international interest in submarine cables and law, I also began wondering about international law in the context of protecting submarine communication cables. My research question in this study is "How are submarine communication cables regulated from the perspective of international law?"

1.1. Methodology

The purpose of the study is to test a hypothesis regarding whether submarine cables are adequately regulated under the current international law. My research questions are, "What is the current structure of the international law for submarine communication cables and global marine communications? Are they adequately regulated or protected in the case of an intended attack focused on one state's cables and from physical damage[4]?" With that in mind, I have delved into the research to determine what international law governs submarine communication cables and global marine communications and to suggest some modifications for improving the current international legal system.

I have chosen to employ a historical approach, case studies, and insights from experts

[4] The physical damage here means the damage on a cable from one state to another, caused by an attack initiated by a state.

to inform my study. I apply the theory of international cooperative regime building by Prof. Kenneth Oye at MIT, and I emphasize the Republic of Korea (ROK) government's potential role as a catalyst in developing new international norms. The research scope is limited to submarine communication cables that transmit data; power cables that carry electricity (Worzyk 2009, v) are beyond the research scope.

Six documents were my primary sources for research on regulating submarine cables that carry international data, video, voice, and internet traffic. These are the 1884 Convention for the Protection of Submarine Telegraph Cables; the 1958 Geneva Convention on the High Seas; the 1958 Geneva Convention on the Continental Shelf; the 1982 United Nations Convention on the Law of the Sea (UNCLOS); the 2021 ICPC Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables; and the 2021 76th Session of the UN General Assembly Draft Resolution on Oceans and the Law of the Sea.

2. The Submarine Cable Industry as a Potential G-2[5] Battleground

Cyberspace is considered the fifth domain to defend in the 21st century. The U.S. Department of Defense officially incorporated it as a new war domain, in addition to land, maritime, air, and space, in 2011 (Welch 2011). What people often forget is that unlike other

[5] Fred Bergsten introduced the term, "G2" in 2005. It is used to refer to two global partners, usually the U.S. and China (Hill 2020). Bergsten coined the term to promote the prior agreements between the U.S. and China, whose cooperation is essential for progress in almost all international economic issues (Bergsten 2009).

war domains, cyberspace is not a natural but a human-invented battleground. Because of the "sneaky nature" of the cyber domain, it is difficult to know who is attacking whom. Cases have occurred in which either espionage or destruction of data took place, but the breach was not discovered until later.

In fact, such an event occurred in South Korea. A breach in the South Korean military intranet, which occurred in December 2016, was discovered two months later. The media reported that the ROK Defense Minister Min-koo Han's computer was hacked, leaking confidential and critical information, which would lead South Korea to rewrite its military operation plans (Kim 2017). This is one of the incidents in which the victim did not know that information was being stolen.

In addition to being invisible and sneaky, the cyber war domain is unique because cyber operations between states can occur constantly, regardless of whether the victim state realizes the damage being done. This is not true in other domains where people can clearly observe an attack, such as a missile strike in the air or one state's troops crossing another state's border without warning.

The cyber war domain cannot operate alone, meaning that it heavily relies, for example, on the maritime domain to function. The submarine cables laid on the seabed create a pathway for the data transfer between continents; a severe cut in submarines cable can cause the internet to shut down, affecting internet users in various countries. Before I delved into this study on

submarine cables, I, too, had a misconception that internet access is possible mostly because of satellites. However, satellite communication only makes up about 5 percent of global data transfer; about 95 percent of internet communication relies on submarine communication cables (Coffey 2014, 28; van Ouderaren 2021).

If a state cuts the submarine communication cables in another state's territorial sea on purpose, it commits a violation under United Nations Convention on the Law of the Sea (UNCLOS)[6]. However, many times when a cable is cut by accident, it is because of a natural disaster, such as the Tonga volcano eruption that occurred on January 4, 2022. This incident caught the media's attention since the only submarine communication cable, named the Tonga Cable System, which brought internet to Tonga by connecting Fiji and Tonga underseas, was cut because of a volcano eruption. In addition, fishing is considered a threat to submarine communication cables. It has been reported that about 70 percent of damage to submarine cables occurs due to fishing equipment, such as trawl nets and dredges (Scott 2022).

The implication from this 2021 Tonga volcano eruption is that not all cable cuts are intentional, but when a state cuts a submarine cable as an attack, it becomes a problem. For example, if the internet was shut down as a result of an attack, the conflict automatically

[6] UNCLOS stands for the United Nations Convention on the Law of the Sea. It is a legal framework for all marine activities. Unlike China, the US has not signed and ratified UNCLOS, although the US recognizes UNCLOS as a part of international customary law. As of June 2016, 167 countries including European Union and South Korea serve as parties to UNCLOS (Murphy 2019, 323~324). North Korea is a signatory state. However, it has not ratified UNCLOS (Shin 2009).

involves the maritime domain. The fact that the cut took place in the victim state's territorial sea automatically involves the victim state's navy, which is responsible for defending its territorial sea.

In this study, the location of the submarine cable is critical. This is because UNCLOS's standing on how to protect cables in a given country's territorial sea is clear. Yet I wonder whether international law properly protects them, even when they are laid in other parts of the sea, such as the high sea, which is beyond a country's territorial sea. Because cyber operation involves at least two war domains, government leaders of many countries are paying attention to submarine cables' ownership and the power dynamics in this industry, which has been identified as a potential battleground among states, especially China and the U.S., as competition over state ownership increases (Kim 2020).

It has often been predicted that whomever has more information underseas will have more power. If China ends up having "better intelligence," having more power by having more information, it can threaten the U.S.'s leadership in the world. Other countries have not "dared" to develop their own undersea networks, but since China is actively building its own undersea network and their espionage skill is increasing rapidly, it is becoming a threat to the U.S. and its allies.

My argument is that not only will G-2 rise as leaders in the submarine cable industry, but also the world will soon fall into the bipolar setting, in which the U.S.'s vision of a Clean

Network competes with China's initiative to build a Digital Silk Road.

The U.S. State Department introduced the Clean Network concept on April 29, 2020. It was meant to build a secure internet highway for all 5G traffic entering and exiting U.S. diplomatic facilities. The underlying assumptions behind this approach are that China has been eavesdropping to steal the data being transferred between the U.S. and its allies or partner nations, and that Deng Xiaoping's concept of "copism," coming up with ways to legalize its technologies copied from foreign technologies, was gaining popularity. In addition, CEO Ren Zhengfei of Huawei, a Chinese technology company, carried out this vision and even dedicated an R&D team to "copism", angering many nations with advanced technology, especially the U.S. (Hilman 2021, 35). This is why in the Clean Network Initiative, using components made by Chinese companies to build the submarine communication cables is forbidden.

What seems to bother the U.S. is the malicious actors' growing espionage abilities regarding submarine communication cables. The U.S. does not want any involvement from untrusted IT vendors in the construction of its undersea network. The U.S. fears using any construction materials, even a screw, from "the untrusted vendors" because doing so might help malicious actors steal critical data from the owner. As an attempt to "safeguard the U.S.'s assets…from aggressive intrusions by malign actors, such as the Chinese Communist Party," then-Secretary of State Mike Pompeo announced a list of the clean 5G telecommunications companies and forbade the "untrusted IT vendors" with a tie to the Chinese Communist Party

from participating in the U.S.-led Clean Network.

Figure 2. 5G Clean Telecommunications Companies (Source: US Department of State. 2020. <https://2017-2021.state.gov/the-clean-network/index.html>).

In my opinion, there is probably a reason why the U.S. only released a list of its "trusted vendors." Five of them--Chunghwa Telecom, Taiwan Mobile, T Star, GT', and FET--are from Taiwan. Four of them--Soft Bank, Rakuten, Jio, and KDDI--are from Japan. The company called "One" is from Hungary. Elisa is from Finland. Orange is from France. O2 is from UK. T-Mobile is from Germany. KT and SK Telecom belong to South Korea. Telstra and OPTUS are from Australia. The list goes further; companies like Telefonica and NTT are from Spain. Bell, Rogers, and Telus are from Canada. Telenor and ice are from Norway. Telia is from

Sweden, while “plus+” is from Poland. GCI, Sprint, AT&T, and Version are American telecommunication companies.

My observation is that the ones under the trusted vendor category share some similarities; for example, most of them come from U.S.-allied or economic partner nations with long histories. Thus, they are likely to be the ones verified and trusted by the FBI subgroup to make it to the list (Le Monde diplomatique 2021).

On the other hand, my analysis regarding the Digital Silk Road is that there probably is a reason why the names of the untrusted IT vendors are not specified. This is because changing the name of a company is easy. For example, Huawei Marine, who had a team dedicated to copying other states’ technologies, now operates under another name, HMN Technologies. Announcing that the U.S. forbids having companies with a tie to the Chinese Communist Party is more effective in deterring their involvement in the Clean Network Initiative than continuously making efforts to follow an industry where the companies may change names frequently to disguise their identity.

Unlike satellite communication, with which the military can acquire its own satellite bandwidth (Gao 2021) for high-level security, a separate submarine cable communication for the public sector does not exist. A so-called secure military line does not exist in submarine cable communication (Hillman 2021, 158). This is another reason the Clean Network Initiative emphasizes the importance of guarding the data inside submarine communication cables. A key

takeaway from Secretary Pompeo's statement is that the U.S. is not shy in identifying information thieves. It is strengthening its guard, especially where China is involved, by designating the Chinese Communist Party as a malicious actor that the U.S. claims is hurting the international order by stealing others' information (Pompeo 2020).

Even under the Biden Administration in 2022, the U.S.'s Clean Network Initiative from the Trump Administration is still being practiced. In 2020, Google and Meta planned to use a network cable in Hong Kong. However, after considering China's access to the cable, the U.S. government shut down this proposal so that such an act of creating a back door to provide the U.S. data to China is prevented in the first place (Hendel and Swan 2020).

However, from China's perspective, the U.S. poses a threat because the U.S. has tried to spy on China, stealing data from China's cables, as was revealed by Edward Snowden's leak in 2013. He revealed the U.S. National Security Agency's espionage through submarine cables to exploit Huawei's technology (BBC 2014b).

China's attempt to counter the U.S.'s Clean Network Initiative is to come up with its own initiative called the Digital Silk Road (DSR). It involves companies, including Huawei and Hengtong, building their own submarine communication cable networks in regions like Africa and Asia (Le Monde diplomatique 2021). The Digital Silk Road is one of the core components of China's foreign policy, whose goal is to connect China to major Eurasian and African states through infrastructure building, such as submarine communication cable

construction (Shen 2018).

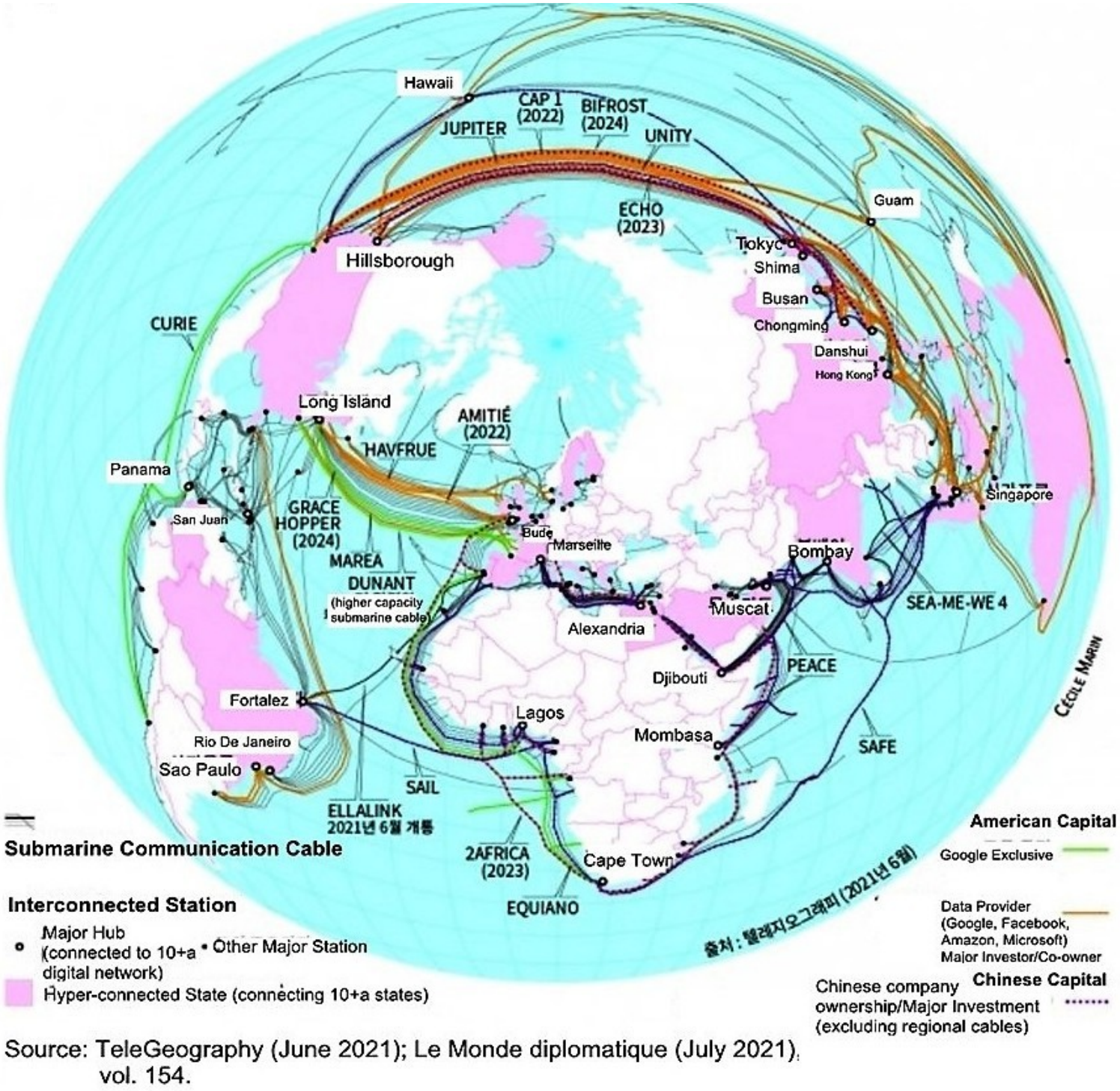

Figure 3. Map of submarine cables from the bipolar perspective translated from Korean to English by the Author (Source: Telegeography 2021; Le Monde diplomatique 2021.

<http://www.ilemonde.com/news/articleViewAmp.html?idxno=14729>).

The purple dotted line in Figure 3 shows how China is expanding its fiber-optic cable network to explore its influence in the Asian Pacific. Furthermore, China has been working hard to become the leader in communication technology in Africa and the Middle East. Huawei and ZTE are currently constructing fiber-optic cables in Belize, Ecuador, Guinea, and the Solomon Islands (Cheney 2019, 5). This move by China is considered an effort to team up with the developing countries to build a submarine cable network under its Digital Silk Road vision, completing the bipolar scene in which the U.S. and China are competing in the field of submarine cables.

In Figure 3, the solid green line represents the U.S. capital connections, where companies such as Google and Meta are helping to build a submarine cable network. The dotted line represents cables that fall under China's umbrella; they are either owned by a Chinese company or controlled by China. A state's intelligence capacity and espionage abilities via submarine communication cables have recently become indicators of its influence in geopolitics, and China's growing power in this industry seems to concern U.S. officials (Hillman 2021, 16).

In his speech regarding the U.S. strategy toward China in May of 2022, Secretary of State Blinken discussed China's surveillance technology and how China has been partnering

with other nations by exporting such technology to more than 80 countries (Blinken 2022). According to a report issued by U.S. Senate Permanent Subcommittee on Investigations Homeland Security and Government Affairs, China hijacked the emails that the U.S. Senate, the DoD, the Department of Commerce, and NASA sent and received for 18 minutes on April 8, 2010 (Robertson 2021). The Biden administration believes it is unjust that as China emerges as a global leader, it benefits from active undersea espionage. The U.S.'s Clean Network Initiative stands in order to prevent espionage like the above incident as much as possible.

Furthermore, China is pressuring corporations inside China to share their information. China has been pressuring public corporations, pushing them to give the government control of the physical layer of cyberspace (the physical medium that transports data to other systems) known as the submarine cable network. The Chinese government occupies an important position in the Asian consortium, which is led by China Mobile, China Telecom, and China Unicom.

With the increase in traffic to Asia, Asian countries such as China, Thailand, and Singapore have been relying more on submarine communication cables. "Since 2010, an average of 9 percent of China's investments have been in submarine cables. That figure used to be only 1 percent from 1987 to 2010," said Dr. Felix Blanc, an expert in submarine cable governance, raising an alarm about China's growing influence in this field (Le Monde diplomatique 2021).

China wields influence beyond Asia and invests heavily in projects in strategic locations such as the Nicaragua Canal (Scobell 2018, 307). This project concerns not only the construction of internet cables but also the first fiber-optic cable to connect Asia and Europe with Marseilles as a foothold, also known as the Pakistan & East Africa Connecting Europe (PEACE) cable. From 2016 to 2019, Chinese companies participated in 20 percent of the world's cable construction projects, with more than half of them taking place around developing countries right outside the South China Sea (Lee 2017).

China's active movement to rise as a G-2 power, and as one of the investor states in the industry of submarine communication cables, seems to put the U.S. at unease because controlling communication technology is considered a source of power in international society. Those with more information have an advantage. China's rising status in the G-2 for the submarine communication cable industry reflects its global status as one of two great powers, equipped to influence the information to which some nations, including developing countries, are exposed via their cables.

Regarding the PEACE, the U.S. has shared its heavy concerns with France, pointing out the fact that PEACE is owned by a Chinese company, Hengtong Group, whose investor is HMN Tech, formerly known as Huawei Marine. In October 2020, Director Peter Berkowitz of the U.S. State Department's Policy Planning Staff met with the French president's advisors and representatives from the foreign and defense ministries. In this meeting, they passed on a report

warning of China's ambition to install submarine communication cables around the world and the espionage risks that effort entailed (Allen 2019). On this matter, Paul Triolo, who was in charge of the geo-technology division of the Eurasia Group, stated that it was natural for the U.S. to share its concerns (U.S. Department of State 2020).

According to Dr. Camille Morel at Jean Moulin Lyon 3 University, the U.S. is intervening more extensively in the cable sector with its ongoing trade war with China (Le Monde diplomatique 2021). She stated that the U.S. had already pressured Australia to abort a project that would have installed a cable between Sydney and the Solomon Islands with Huawei Finance in 2018 (Dreyer 2021). This intervention was a part of the Clean Network program led by then-U.S. Secretary of State Michael R. Pompeo. The program, which still continues, prohibits the use of Chinese mobile telecom operators (China Telecom) and certain apps (with then-President Trump singling out TikTok) in the U.S., reduces the amount of data stored in China, and aims to maintain the cable network and keep it "clean" by excluding Chinese companies (Williams 2020).

Dr. Namhoon Cho, a senior research fellow at Korea Institute for Defense Analyses, also stated that the U.S. initially owned the internet. Regarding the U.S.'s concern over China's espionage capabilities, he pointed out the fear factor. He warned about the U.S.'s attitude toward China, stating that U.S. officials tend to overestimate China's espionage capabilities (Cho 2018), and implying that the U.S. is still the superpower in cyber space. However, in 2022,

Secretary of State Blinken directly challenged scholars like Dr. Cho, who claims that the technology gap between the U.S. and China is still huge.

According to Secretary Blinken, although the U.S. invented the internet, the authoritarian nature of China's political system makes it easier for China to collect data upon which surveillance technology can thrive, as China can monitor the sensitive information not just of its citizens but also of people in other states, which is what prompts the U.S.'s concern. Now, the U.S. must compete to maintain its superiority, because in cyber security the U.S.'s monolithic power is no longer guaranteed (Blinken 2022).

On the other hand, I find it important to point out that the U.S. also monitors other states, including China. With New Zealand's Security Intelligence Service, the U.S. hacked the submarine cable passing through the Chinese consulate in Auckland on behalf of the NSA (Kuehn 2016). In my opinion, the core of the U.S.'s concerns is that the submarine cable industry may become an area in which the theory of asymmetric conflict applies (Arreguin-Toft 2005, 200). The following shows that the weaker country in this bipolar power dynamic, China, which began as a follower and an imitator in the high-tech industry, may end up on top, defeating the U.S. not just in information technology but also in other fields in the future.

As even Secretary of State Blinken pointed out in his recent speech at George Washington University in May of 2022, this is a possible scenario as long as China continues to invest in the technological infrastructure inside and outside of its territorial sea (Simmons

2021). Statia Lee, a researcher in the Department of Political Science at the University of Washington, elaborated on this point. She explained that China Unicom invested in a project titled, "The Cameroon-Brazil Underwater Optical Fibre Project"—to establish a cable between Cameroon and Brazil in exchange for access to fishing areas. The site for this project is Beachman Haul, the connecting point between the Brazil-Cameroon underwater cable (Lee 2017).

Paul Triolo from Eurasia Group also observed that China's initial cable strategy was to satisfy domestic demand, but its digital economy has gradually expanded to other countries, including Africa and Asia. He called this network the Digital Silk Road (Triolo 2020). As much as the U.S. strongly expresses its desire not to have the Chinese companies in its cable network, according to the Clean Network Initiative, China also disfavors the U.S. companies' involvement in building its own vision, the Digital Silk Road.

It has been reported that China canceled a project to install three cables connecting Hong Kong to Japan, Singapore, and the Philippines when it discovered that Google had made a partial investment (Le Monde diplomatique 2021). This cancelation shows that as much as we talk about the U.S. being concerned about China's espionage, China also seems to hold the U.S. in check, attempting to avoid U.S. companies investing or becoming involved in building its submarine communication network.

Crozer said that the battle between the U.S. and China in this industry is not merely

possible but already happening. From 2016 to 2019, Chinese companies were involved in 20 percent of global cable construction projects (Le Monde diplomatique 2021; Lee 2017). Due to security concerns over hacking from the submarine communication cables, China's rapid growth as a provider of submarine communication cable infrastructure to the world is a growing challenge for many states.

The competition between the U.S. and China to expand their influence to other states' submarine cable networks by becoming involved in their projects has begun; the age of monolithic power, during which the U.S. enjoyed a hegemonic role is likely long gone (Moon 2022), as the bipolar scene in submarine communication networks becomes clearer every day.

2.1 Literature Review

About 475 submarine cables function as the world's information highway every day around the clock (Sherman 2021, 1). Chinese ownership comprised only 7 percent of the world market in 2012; by 2019, it had increased to 11 percent. It is now predicted that the Chinese presence in the submarine cable market could reach 20 percent by 2025. This trend is troubling to the U.S., which until now has maintained its status as the world's leading hub in the industry (Mayville 2021 26:22).

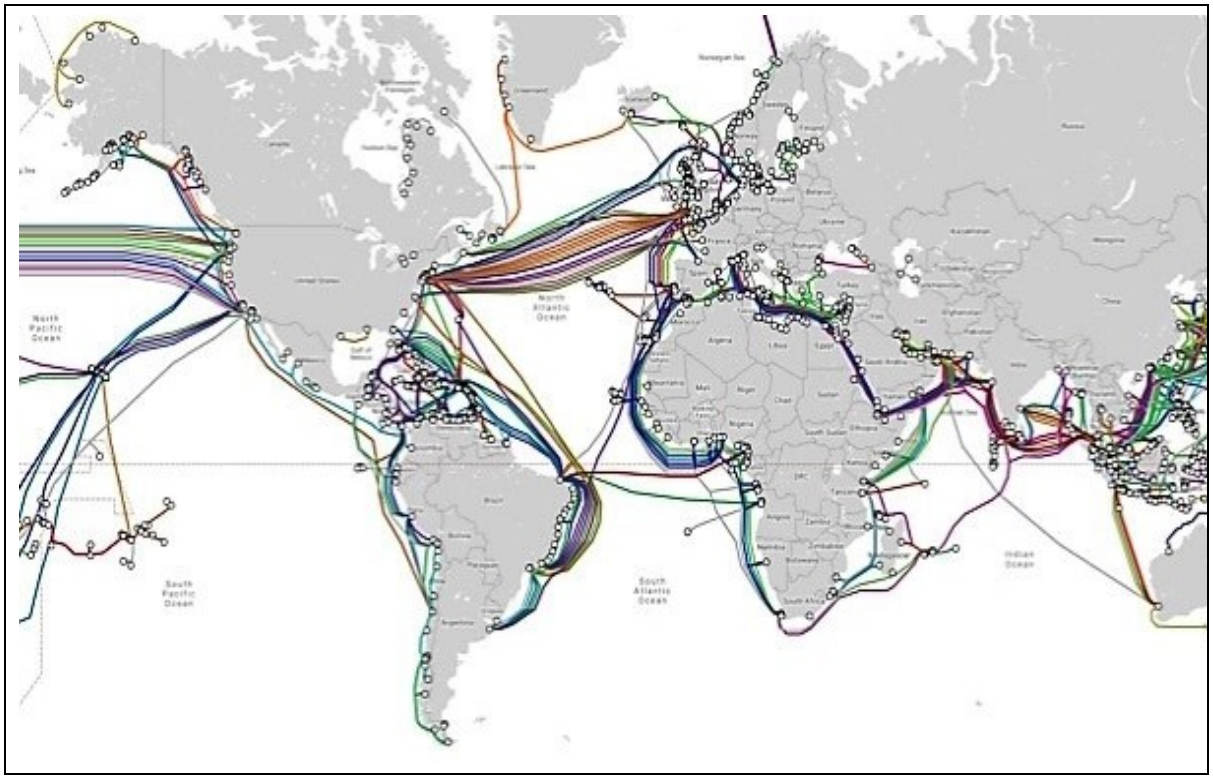

Figure 4. Global map of submarine cables. (Source: TeleGeography. 2021. "Global Map of Submarine Cables." 2021, <https://www.submarinecablemap.com>).

Under UNCLOS and customary international law, coastal states are entitled to adopt laws and regulations on innocent passage[7] through their territorial seas. The challenge is that coastal states are not required to enact such laws under UNCLOS, unlike under the 1884 Convention. UNCLOS does not contain a provision that allows a state to board vessels suspected of engaging in criminal acts involving submarine cables beyond its territorial seas. It remains unclear whether such a right is recognized in customary international law. Another

[7] Innocent passage is a concept in the law of the sea that allows for a vessel to pass through the territorial sea under UNCLOS Article 17. Passage is innocent so long as it is not prejudicial to the peace, good order or security of the coastal state (Ballester 2014).

issue is that because private companies rather than states own submarine cables, UNCLOS's authority to oversee the protection of cables is rather limited (Sunak 2017, 6).

The legal basis for the freedom to lay and maintain submarine cables comes from UNCLOS (Burnett 2017, 1). It is binding on states that are parties to it. Some nonparty states such as the U.S. have accepted UNCLOS as customary international law. However, the actors involved in the submarine cable industry are not only states but also the cables' owners and the companies that produce and maintain them.

The 1982 UNCLOS Commentary, compiled by scholars at University of Virginia Law School, suggests that the phrase "all states" should not be read strictly in the UNCLOS context; instead, it should be understood to refer to states or their nationals that lay cables or pipelines (quoted in Davenport 2015, 71). After Facebook proposed creating its own submarine communication cables, after its "worst" blackout in fifteen years in October 2021, this issue of private companies' ownership of submarine cables and the challenges in this field have been widely discussed (Prinsloo 2021).

Furthermore, in her 2015 article, "Submarine Cables, Cybersecurity and International Law: An International Analysis," Tara Davenport highlighted some incidents that might be considered breaches of international law for the failure to protect data or the cables themselves. She questioned whether the act of placing a recording device on undersea cables or tapping into them to collect the data that pass through them would be considered legal from the

perspective of international law. Neither the Law of War nor the Law of the Sea has provisions calling such espionage illegitimate (Paik 2020, 2).

However, distorting information inside a submarine cable qualifies as an "internationally wrongful act" (International Law Commission 2001). Nevertheless, the methodology for enforcing punishment against a state for such a wrongful act is a missing piece in international law. Davenport called the existing legal framework—which includes UNCLOS and the 1884 Cable Convention—fragmented and identified its limitations (Davenport 2015, 82).

Furthermore, Elizabeth O'Connor emphasized that the existing international law regulating submarine communication cables does not reflect the revolution in technology, as it began with the current generation's widespread use of the internet. She pointed out that international law relating to submarine communication cables has not been augmented since the mid-twentieth century when telegraphs and telephone calls connected the world rather than fiber-optic cables (O'Connor 2019, 42).

Blair Shepherd (2020) evaluated whether the existing regulatory regimes were prepared to deal with situations in which, for example, an unmanned submarine deliberately cuts cables or an unmanned aerial vehicle attacks them to manipulate the data inside them. It is worth exploring this line of thought to prepare legally to deal with these situations, should

North Korea, which is actively building its asymmetric capacity to counter the big powers in international politics, execute such actions in the future.

Because attacks on submarine cables would have crucial effects on people's everyday lives due to the increased reliance on the internet, the U.S. treats one state's malicious actions against another state's submarine cables as an armed attack. U.S. Presidents have said they treat it as if it were a physical attack. This is against international law because under international law, retaliation is only allowed when the attack meets all the conditions to be considered a clear physical attack—causing some visual physical damage. But under the U.S. Law of War Manual, a cyber attack is regarded as a physical attack, even when it is unclear whether the attack has caused some physical damage (Koh 2012, 3).

Shepherd explained that the U.S. has argued that the international society should also view actions, such as physically destroying submarine cables or harming the data inside them via cyber operations, as armed attacks and as justifications for self-defense, even when the threshold provided in Article 51 of the UN Charter has not been met (Shepherd 2020, 219-220).

3. Geopolitics of Cable Competition

From the early days in 1858, the U.S. and U.K. have been enjoying a cooperative relationship in building submarine communication cables. This meant that they made collective efforts to lay down a first transatlantic telegraph cable between the U.S. and the U.K, titled the

Atlantic. Upon the completion of the project, Queen Victoria and President Buchanan of the U.S. talked, using this newly established submarine communication cable in the Atlantic. Before this cable, it was all about just sending Morse code through the cables. This event establishing the first transatlantic telegraph cable over the Atlantic, connecting the U.S. and U.K., was significant because now people in two nations could live in an age where they could talk and listen to each other, relying on the submarine communication cable (PBS 2022).

The Atlantic Telegraph Company, led by an American businessman, Cyrus W. Field, was able to initiate this 1858 project. Ever since then, such cables as TAT-14, TGN-Atlantic, and Atlantic Crossing 2, also known as AC-2, were laid in the Atlantic out of the collective efforts between the U.S. and the U.K. These have been considered a monopoly, in other words representing the British hegemony in the submarine cable industry (Burns 2013). Right now, the two big players are America and China, but before, the two big players were America and Britain, as the history shows.

The first cable, TAT-14, lasted from 2001 to 2020. This cable system used four fiber cables—having two stay active and reserving the others for emergency backup. Unlike the other cables mentioned above, TAT-14 was built in a self-healing ring system. These bundled cables together connected the E.U. (U.K., France, Germany, Denmark, and Netherlands) with the U.S. This was possible, having the data flow in a ring shape, as depicted in Figure 5 below.

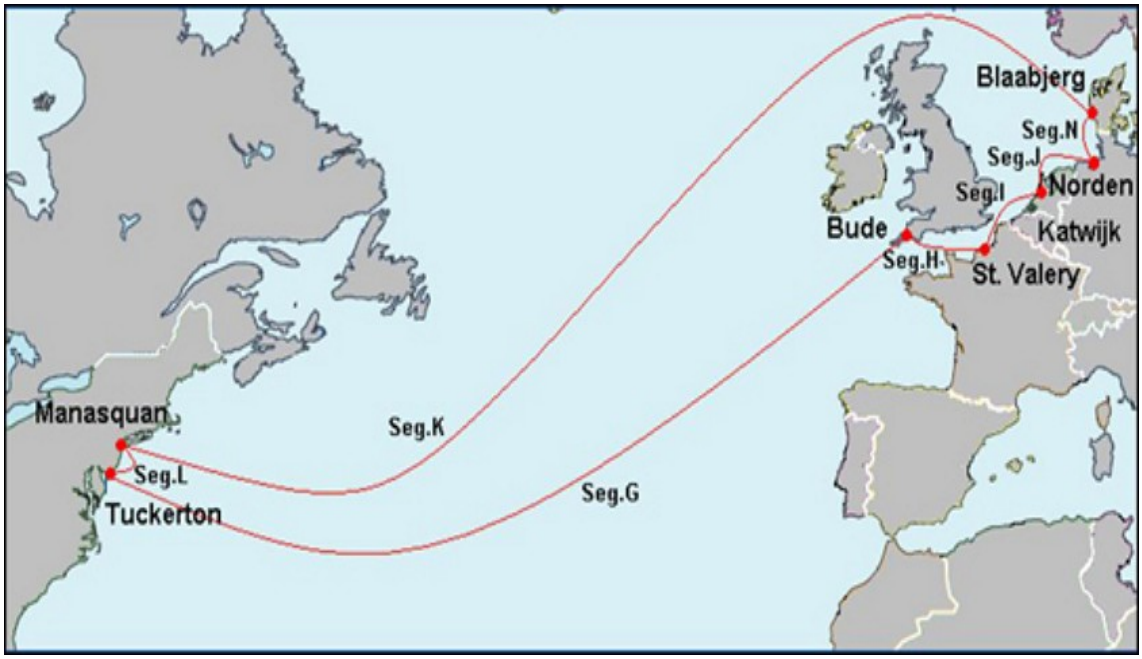

Figure 5. TAT-14 Landing Station Map. (Source: Submarine Cable Networks. 2022. "TAT-14 Landing Station Map." 2022, <https://www.submarinenetworks.com/system/trans-atlantic/tat-14>).

As history shows, this ring system soon was retired, giving its place to point to point "mesh architecture," since the act of building two cables in parallel was considered redundant and inefficient (Burnett 2021 1662). The second cable in the Atlantic is the TGN Atlantic. It has been operating since June 2001, and now it is expected to expire in June 2026. This cable connects the U.S. and the U.K. in mesh architecture. Originally, it was established by an American company, Tyco International. Currently, TGN Atlantic is owned by an Indian company, Tata Communication, based in Virginia (Glover 2022). Thirdly, the Atlantic Crossing 2, a.k.a. AC-2, was first introduced in November of 2000. It is 6,400 km-long

submarine cable linking the U.S. and the U.K. After going through several acquisitions, AC-2 is now wholly owned by Century Link, a part of an American telecommunication company, Lumen Technologies (Submarine Cable Networks 2022).

However, this Anglo-American monopoly seemed to begin breaking down in 2001, when France started laying cables in the Atlantic. For example, FLAG Atlantic 1, a 14,500-km cable, linked the U.K., the U.S. and France, and this was a change since this cable was owned and operated by a French company, Global Cloud Xchange—no longer an Anglo-American company (Nielson 2021, 58). Even after September 8, 2022, when the 77th UN General Assembly took place in New York and Queen Elizabeth II passed away and the world mourned, the U.S.-U.K. relationship remains solid as rock.

In President Biden's words, it represents an example of the bedrock alliance (Biden 2022). To me, this trusting relationship between the U.S. and the U.K. over the years is the forte that keeps the cables in the Atlantic up and running, despite the possibility for espionage among the nations who have a foot in submarine cables. In a way, allies or partner nations have built an underseas network, sharing information only among themselves by linking themselves via submarine cables. Comparing this U.S.-U.K. rather cooperative relationship in the submarine communication industry to the U.S.-China relationship in the same sector, I realize that not many similarities can be found. Far from being cooperative, the U.S. doesn't seem comfortable sharing submarine cables with its competitor nation, China. The revival of geopolitical

competition in the field of submarine cable is already here, although President Biden has said in the 77th General Assembly that "[The U.S. doesn't] seek another Cold War with China" in all matters (Biden 2022).

In my opinion, the fact that President Biden mentioned the words Cold War in his speech is hinting that an age of a new Cold War between the U.S. and China is possible. Especially in the field of technology, China may flourish over the U.S. because of China's authoritarianism (Ryan-Mosley 2022). This system makes it easier for China to gather sufficient data essential to develop China's surveillance technology in the future (Blinken 2022), unlike in the U.S., where people's privacy has a higher protection than China.

About 475 submarine cables function as the world's information highway every day (Sherman 2021, 1). Chinese ownership comprised only 7 percent of the world market in 2012; by 2019, it had increased to 11 percent. It is now predicted that the Chinese presence in the submarine cable market could reach 20 percent by 2025. This trend is troubling to the U.S., which until now has maintained its status as the world's leading hub in the industry (Mayville 2021 26:22). This data shows China's increasing involvement in the submarine cable industry, which also can be considered a bold step towards becoming a world power.

This is the reason why, when Google and Meta planned on using an existing submarine communication cable that passes through the territorial sea of Hong Kong, part of mainland China, it put the U.S. government at unease. The U.S. government asked Google and Meta to

avoid including Hong Kong in their submarine cable communication route. In other words, it blocked an end to the construction project proposed by Google and Meta initiated under the Trump administration (Hendel and Swan 2020).

However, the project gained momentum once the submarine communication route in the proposal changed from Hong Kong to Taiwan (once U.S.'s ally, now an economic partner nation) and Philippines (current U.S. ally nation). Under the Biden administration, both Google and Meta got permission to pursue their projects to use a submarine communication cable to handle the increasing data in Asia. Meta's proposal now includes the Philippines, while Google is teaming up with Taiwan (Shepardson 2021).

4. Identifying Deficiencies in Current International Law

4.1.1. Review of Existing Institutions: Brief History of the Regulation of Submarine Cables

In this chapter, I first review the existing international law for protecting submarine communication cables, and later identify the challenges in developing an effective system of international law, especially to address instances in which cables are physically damaged in another state's deliberate attack.

The 1884 Convention for the Protection of Submarine Telegraph Cables states in Article 4 that "The owner of a cable, who on laying or repairing his own cable breaks or injures another

cable must bear the cost of repairing the breakage or injury without prejudice to the application, if need by of Article 2 of the present Convention." Even though the 1884 Convention thus provides a punishable offense for those who damage submarine cables, some scholars, such as Jason Petty, have argued that the scope of Article 2 is limited to telegraphic wires and that fiber-optic cables are outside the scope of the 1884 Convention. The fiber-optic cables that we use today for internet communication were not available in 1884 and thus are outside of the Convention's scope.

The 1884 Convention for the Protection of Submarine Telegraph Cables is currently in force for 36 countries, including the U.S. (National Oceanic and Atmosphere Administration Office of General Counsel, 2019). This treaty is historically important, being the first multilateral treaty recognizing the importance of protecting submarine communication cables (Petty 2021, 272). It can be said that the 1884 Convention is considered a historical relic, limited to protecting telegraph cables.

The second treaty of relevance is the 1958 Geneva Convention on the High Seas. It codifies the rules of international law regarding the high seas, also known as international waters. The high seas are the international common space, which all states and their citizens are allowed to use lawfully (Lee 1983). Article 26.1 of the 1958 Geneva Convention on the High Seas provides that "all states" shall be entitled to lay submarine cables on the bed of the high seas. This means that presumably no state may impede their laying or maintenance. The

definition of high seas is provided in Article 1.[8] It means all parts of the sea that are not included in the territorial sea or internal water, as Figure 6 shows.

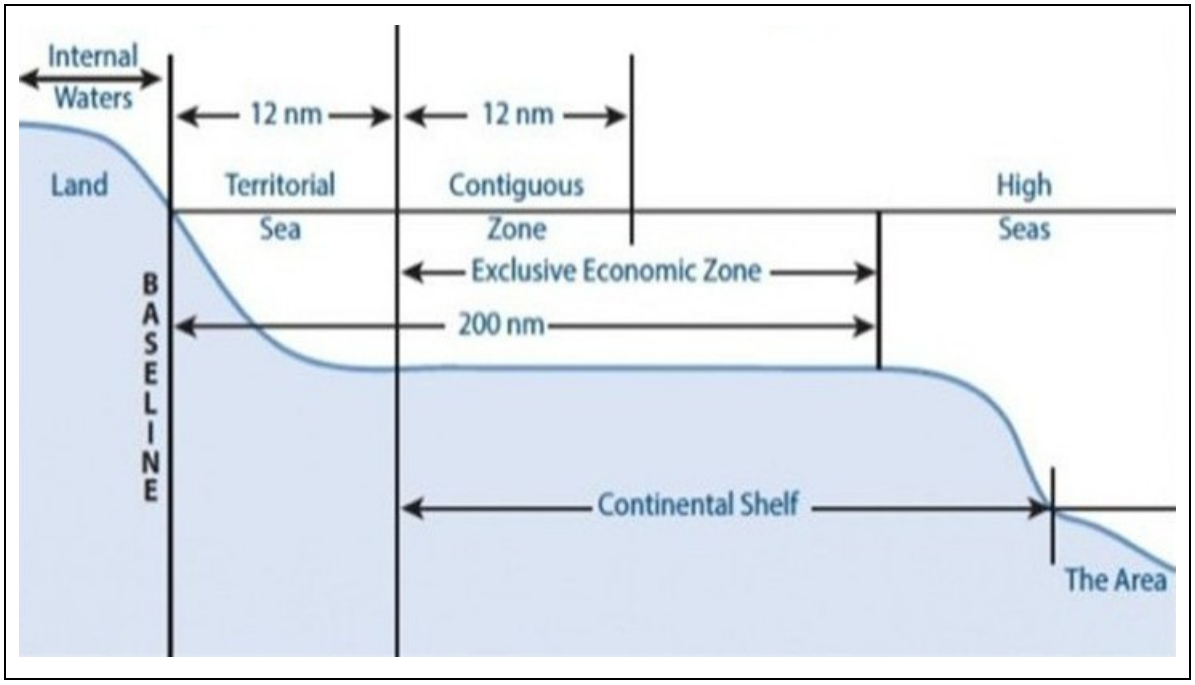

Figure 6. Legal boundaries of the ocean (Source: Tufts University, 2017. "Law of the Sea: A Policy Primer," <https://sites.tufts.edu/lawofthesea/chapter-two/>).

In 1984, the third treaty, the United Nations Convention on the Law of the Sea (UNCLOS), became effective. As of today, it is widely accepted, having 167 states parties. China signed and ratified UNCLOS in 1996; the U.S. has not ratified it because of opposition from Republicans in the Senate, where treaties must be approved by a two-thirds vote. Although the U.S. has not ratified UNCLOS, it still abides by it, treating it as customary

[8] By 2013, the 1958 Convention on the High Seas was ratified by 63 states, including most NATO bloc and Soviet bloc states but excluding states like Syria, Jordan, Egypt, Saudi Arabia, Iran, China, North Kora and South Korea (United Nations Treaty Collection 2022).

international law.

The 1958 Geneva Convention on the High Seas is no longer in force (Davenport 2015, 67). It is overridden by UNCLOS, which includes a new concept of the Exclusive Economic Zone (EEZ). It is an area beyond and adjacent to the territorial sea, subject to a specific legal regime, under which the rights and jurisdiction of the coastal state and the rights and freedoms of other states are governed by the relevant provisions of UNCLOS (Article 55). As illustrated in Figure 6, the EEZ does not extend beyond 200 nautical miles (370 kilometers) from the baselines from which the breadth of the territorial sea is measured (UNCLOS Article 57).

In summary, the rights guaranteed by UNCLOS are as follows: All states may install submarine cables on the continental shelf but must have due regard for cables already in position. The possibility of repairing existing cables shall not be prejudiced (UNCLOS Art. 79.5). And the specific positioning of the cables is subject to the consent of the coastal state (UNCLOS Art. 79.3). Left unregulated are submarine cables located in the high seas, which are outside a coastal state's internal waters, territorial waters and EEZ (UNCLOS Art. 86) (Bressie 2016, 10). Article 87.1.c of UNCLOS provides for the freedom of the high seas and refers to all states' rights to install submarine cables.

On the topic of injury of a submarine cable, Article 113 requires that:

> Every State shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its

> jurisdiction of a submarine cable beneath the high seas done willfully or thorough culpable negligence in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offense. This provision shall apply also to conduct calculated or likely to result in such breaking or injury. However, it shall not apply to any break or injury caused by persons who acted merely with the legitimate object of saving their lives or their ships, after having taken all necessary precautions to avoid such break or injury.

4.1.2. UNCLOS Provisions on Submarine Cables in the Territorial Sea

According to UNCLOS Article 3, a coastal state may establish its territorial sea to a limit not extending more than 12 nautical miles (nm) measured from the baseline, and which is precisely the same as the 1958 Geneva Convention on the High Seas. The coastal state has sovereignty up to this 12-nm line, based on UNCLOS Article 2.1, which states, "The sovereignty of a coastal State extends beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea." This means that no entity may lay cables in someone else's territorial sea without permission.

UNCLOS Article 21 states, "The coastal state may adopt laws and regulations, in conformity with the provisions of this Convention and other rules of international law, relating to innocent passage through the territorial sea in respect of…(c) the protection of cables and pipelines." The following can be said: A costal state has sovereign rights in the territorial sea

although these rights are subject to certain limitations such as the obligation to permit innocent passage. Vessels can come and go, but they cannot hurt the cables.

4.1.3. UNCLOS Provisions on Submarine Cables in the Contiguous Zone

According to UNCLOS Article 33.2 and as shown in Figure 6 above, a contiguous zone may not extend beyond 24 nautical miles from the baselines from which the breadth of the territorial sea is measured. It is not part of the high seas; the contiguous zone refers to the intermediary zone between the territorial sea and the high seas.

Inside the contiguous zone, a coastal state has the authority to exercise the control necessary to prevent infringement of its customs, fiscal, immigration, or sanitary laws and regulations to the same degree as within its territory or territorial sea (UNCLOS Art. 33.1.a). Among other restrictions, this means that no entity can come and lay a cable in a coastal state's contiguous zone without permission.

4.1.4 UNCLOS Provisions on Protecting Submarine Cables in the EEZ

From the line where the territorial sea ends, anyone can lay cables even in the exclusive economic zone (EEZ) (UNCLOS Article 58). The EEZ extends no more than 200 nm from the territorial sea baseline and is adjacent to the 12nm territorial sea of a coastal state (UNCLOS Articles 82 and 86).

Within a costal state's EEZ, UNCLOS guarantees to all states the freedom to lay submarine cables. Article 58 of UNCLOS provides as follows: "In the EEZ, all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in Article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention."

4.1.5 UNCLOS Provisions on Protecting Submarine Cables in the Continental Shelf

From the line where the territorial sea ends, while anyone can lay cables in the exclusive economic zone (EEZ), they cannot do so on the continental shelf of a coastal state without permission (UNCLOS Article 87). The continental shelf is the edge of the land mass that extends under the ocean from the coastline to a drop-off point called the shelf break (National Geographic Resource Library 2022).

Part IV of UNCLOS reiterates this right in Article 79.1 providing that "All States are entitled to lay submarine cables and pipelines on the continental shelf, in accordance with the provisions of this article." This needs to be read along with UNCLOS Article 79.3, which provides that "The delineation of the course for the laying of such pipelines on the continental shelf is subject to the consent of the coastal State." Thus, the right is not unrestricted. State A

may have a right in principle to lay a cable on State B's shelf, but it must discuss the details with B, and ultimately, needs B's permission to proceed.

4.1.6. UNCLOS Provisions on Protecting Submarine Cables in the High Seas

In cases in which submarine cables are willfully or through culpable negligence broken or damaged by a ship or by a person, the state under whose flag the ship operates or that of the person's citizenship has jurisdiction to address the injury (UNCLOS Article 113). Currently, UNCLOS does not provide for the jurisdiction of the cable owner's state.

UNCLOS Article 113.1 provides that "Every State shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done willfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offense." The problem is that because that is all the treaty says, when it comes down to the implementation, enforcement is lacking because the treaty places jurisdiction in the attacker's state, not the cable owner's state. If the jurisdiction were in both the cable owner's state and the attacker's state, enforcement could be stronger.

4.2. Deficiencies in the Regulation of Submarine Cables

Here, some challenges are unresolved by UNCLOS. Article 113 is insufficient to provide security to submarine communication cables. First, many states that are parties to UNCLOS have not implemented their obligation to enact domestic laws to protect submarine cables in the high seas (Davenport 2015, 83), meaning that they have not enacted the laws required by Article 113, and thus are in breach of UNCLOS. Furthermore, international law by nature lacks a strong enforcement mechanism. It relies on states' voluntary compliance.

Overall, the gap in UNCLOS is in respect not to laying but to protecting submarine cables before they are damaged. Under the current structure, because a number of individual countries have not adapted domestic laws to protect submarine cables, the cables in some parts of the ocean, like in the EEZ and the high seas, have been left "ungoverned."

UNCLOS is binding on the states that are parties to it. Some nonparty states, such as the U.S., also abide by UNCLOS, respecting it as customary international law (Burnett 2017,1). However, experts have pointed out that a hole exists in UNCLOS in terms of protecting submarine cables in the high seas. The problem I address here is that the jurisdiction can be exercised under the nationality of the owner of the ship, not under the jurisdiction of the cable owner. The nationality of the owner of the ship may not be interested in protecting the cables but in harming cables. Unless there is a monitor or a neutral enforcement mechanism outside the state of the attacker, the problem in the current legal regime will continue.

5. Real World Manifestations: ACE Cable and Beyond

The purpose of this chapter is to look for the cases in which one state's core infrastructure, a submarine communication cable, was damaged by another state's intentional attack. Only two cases have publicly been identified that fit into this category, and one of them is the ACE cable case. Those cases involve Russia and China, both of which have the technology to eavesdrop on what happens inside the submarine communication cables. The fact that they have this technology is bothersome because they can attack cables as a military tactic (Sutton 2020).

According to the statistics released by European Parliament, about 200 cases of damage to submarine communication cables occur per year (Bueser 2022, 70). Only a few of them are due to a natural disaster, like the recent one in Tonga on January 4, 2022. It was because of a volcanic eruption, which cut the fiber optic cable connecting Tonga to Fiji. Until the repair on the submarine cable was completed after five weeks, Tongans struggled, missing the fast and reliable submarine communication cable-based network (Nikkei Asia 2022). However, cuts in submarine cables are rarely because of natural disasters, and people losing internet access for almost five weeks because of a volcano eruption damaging the cables is extremely unusual.

As we have observed, 90 percent of the physical damage to submarine communication cables is caused by fishing nets and anchors (Kazaz 2022). However, these incidents are outside of my research scope; they do not qualify as intentional physical attacks by one state against

another state's infrastructure, such as a submarine communication cable. Intended attacks, which are within the scope of my case study, are rare, but they have happened. One example is the Africa Coast to Europe (ACE) cable case.

The ACE cable case arose on April 8, 2018. On that day, the ACE submarine cable was cut, and as a result people in 18 states, including France, Portugal, Spain, Senegal, Nigeria, and Mali, lost their access to the internet for 48 hours. The damage was severe because it meant that the business transactions in and out of 18 states literally stopped for two days, causing both financial loss and inconvenience to many people. Physically, the ACE cable is located in the west coast of Africa, spanning 12,000 km, as illustrated in Figure 7.

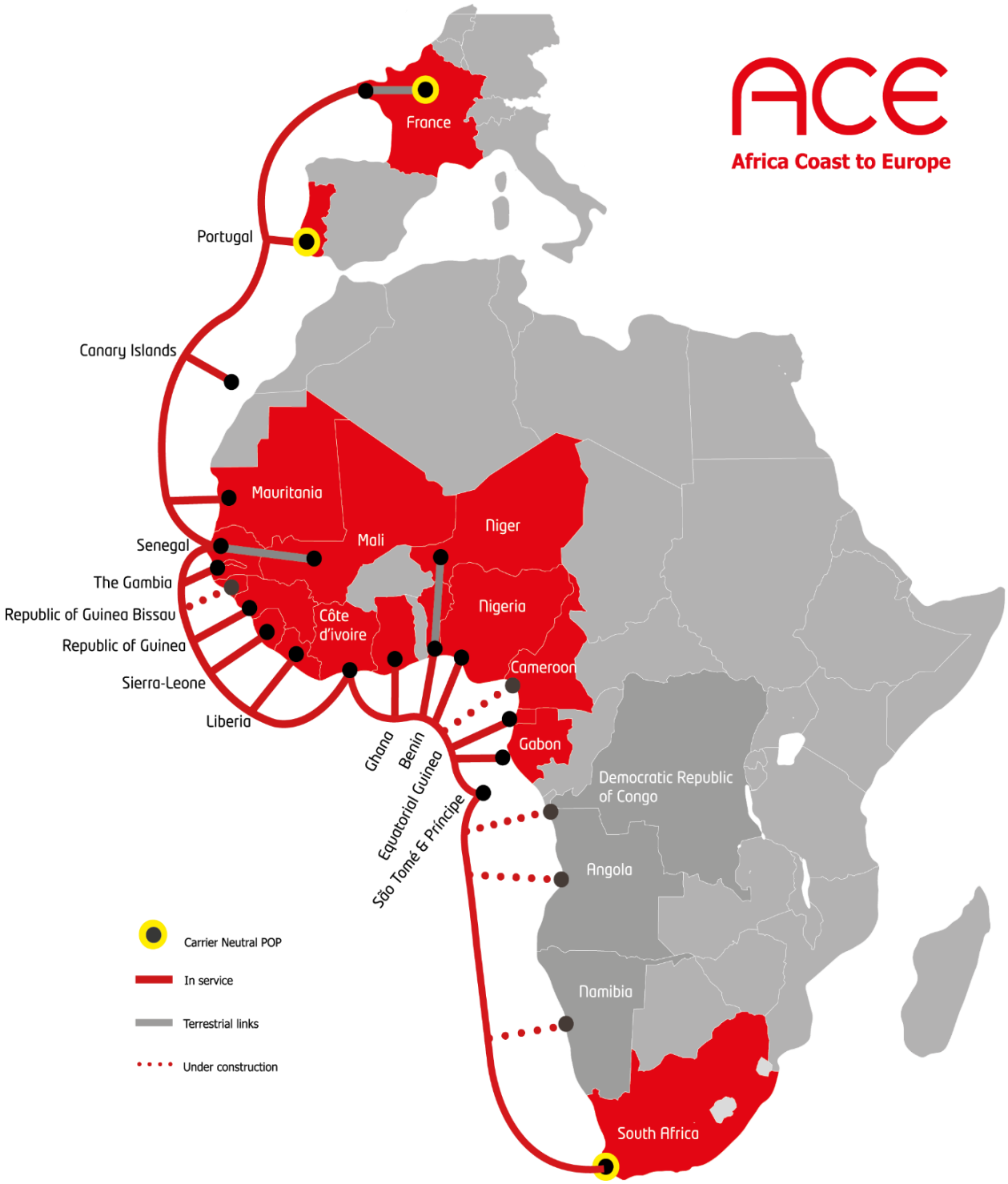

Figure 7. ACE Submarine Cable. (Source: ACE Submarine Cable, 2022. <https://acesubmarinecable.com/en/submarine-cable/>).

The ACE Cable is financed by ACE Consortium, made up of France Telecom Orange

and its subsidiaries, such as Orange Mali. France Telecom Orange is a company 23 % owned by the French government; the rest is in the hands of public investors. Orange Mali is a telecommunication company affiliated with France Telecom Orange (Submarine Cable Networks, 2018).

Whether the break in the ACE cable was an intended attack or just an accident is still not clear. The challenge here is the issue of attribution. Experts say that the ACE cable was cut off and no one knows the reason behind it, although Russia has the ability to cut the cable, suggesting that it may have done it as a physical attack (Edwards 2018).

Another case that also raises the attribution issue as a challenge is the *Losharik* spy submarine accident, which occurred on July 1, 2019 near the naval base of Severomorsk, a town in Russia. According to the Russian Defense Ministry, a fire happened on the *Losharik* while the vessel was measuring the depth of the seabed. However, the Russian newspaper Novaya Gazeta suspected that a nuclear-powered vessel, *Losharik*, might have cut Norwegian submarine cables located 60 nautical miles east of Norway, resulting in some physical damage done to the cables.

Contemplating the cause, some security experts, like H. I. Sutton, disagree with the official position of the Russian Defense Ministry. He suspects that the *Losharik* may have cut the Norwegian submarine communication cables because Russia has the capability to cut cables in hard-to-fix places. The *Losharik* dives up to 20,000 feet, 10 times deeper than the depth where

crewed American submarines operate (Glanz 2020).

This may have concerned the U.S., because according to the media, the U.S. USS Jimmy Carter only has the capability to eavesdrop the data inside the submarine communication cables, but not to cut them (Axe 2020). This is the only U.S. submarine publicly discussed in this way, but it likely represents general U.S. submarine capabilities. As this example shows, in the submarine sector, Russia appears to have more advanced capabilities than the U.S.

Figure 8. The pattern of submarine operation on submarine cables. (Source: Forbes., 2020.

"How Russian Spy Submarines Can Interfere with Undersea Internet Cables." 2020, <https://www.forbes.com/sites/Hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/?sh=7fc147543b04 >).

A British Member of Parliament, Rishi Sutton, who is not related to H.I. Sutton, explains his idea about how the operation probably worked on July 1, 2019 as follows: Three Russian submarines worked together. In Figure 8, (A) a nuclear-powered mini-submarine on a mission to cut the submarine communication cable approached the cable. (B) A large host submarine patrolled above, prepared to bring back the small submarine. (C) The nuclear-powered attack submarine performed the overwatch (Sutton 2020), watching to make sure no one interrupted the smaller vessel.

Figure 8 shows the general pattern of the operation that is likely to have been conducted by the Russian submarine against the cables. Despite this speculation, because Russia has not admitted its act in public and Norway has been passive, neither discussing the incident nor providing evidence to point fingers to Russia for causing the damage, Russia has not been accused of an illegal act, for example, in the International Tribunal for the Law of the Sea (Sutton 2020).

Interestingly, according to *The New York Times*, published on April 21, 2020 by Glanz James and Thomas Nilsen, "fewer still want to talk about what the (Russian sailors) were doing

off Norway's waters" (Glanz 2020). While unstated, the implication here is that Norway is aware that Russia probably cut the cable, but Norway didn't make a big deal about it because it didn't want to start a war over this incident.

Cutting the submarine cables as an attack can be considered a use of force. However, the Norwegian government probably concluded that provoking an international incident, turning Russia to be a foe over some damage to a cable, was not advisable, at least at the time.

In addition, the Chinese submarine *Jiaolong* also possesses the capability to cut submarine communication cables, which has made it a rising national security concern for the past decade (Kim 2012, 68). This was just mentioned briefly in Kim's article. There is not a lot of publicly available information about the *Jiaolong,* but the fact that China also has the capability to cut cables is troubling.

In summary, at least two countries have the capability to go deep enough to cut submarine communication cables. And, considering our heavy reliance on those cables, the threat to the security of the cable is not just a concern to the government officers but to almost all global citizens who have become more dependent on the internet since the pandemic hit the world in 2019.

6. Policy Implications: Suggestions Regarding South Korea's Role as a Catalyst in Developing a New International Norm

I intend to rely on concepts from the theory of international cooperation regime building as I approach this topic from the perspective of international relations and international law. The theory of international cooperation stems from the idea that international regulatory regimes help develop new norms and reduce uncertainty among participants (Oye 1986, 250).

International cooperation builds on the notion that governments can move toward a "better-coordinated future." It assumes that governments can see the benefits in orchestrating harmony, rather than devolving into anarchy (Oye 1986, 254). Tara Davenport shows how, just as in other areas, international cooperation theory can be applied in the submarine cable industry. The basic concept of international cooperation theory is that institutions can pursue and maintain cooperation when they have strong common interests (Dai 2017). In her opinion, building cooperation, not just among states but also in state-to-cable company relations, is indeed possible and essential to protecting submarine cables (Davenport 2012, 224).

As a middle power country, South Korea is positioned to become a leader in creating a new regime that regulates the submarine cable industry. As one of the world's largest fiber-optic cable suppliers, South Korea may engage other countries more and exert its influence in protecting submarine cables in the future. LS Cable & System, South Korea's largest supplier, is a leading global player in long-distance and high-pressure cables (Bae 2020). Even during the COVID-19 pandemic, LS Cable & System has successfully signed contracts for submarine cables with the Netherlands, the U.S., Singapore, and Bahrain (Kim 2020). LS Cable & System

is ranked sixth among the major submarine cable market vendors worldwide (Technavio 2020).

The prospect of positioning the country as a focal point in the submarine cable industry should garner more interest and discussion from the South Korean government—that is, when it decides to engage more with other countries and set the agenda for discussion. In my opinion, South Korea can act as a catalyst in an organization such as the International Cable Protection Committee (ICPC)[9] or the International Maritime Organization (IMO) by promoting discussions in venues such as the UN on the topic of developing an international regulatory regime.

One motivation for South Korea to fulfill such a role would be to build a mechanism with which to counter North Korea's efforts to become an asymmetrical power, and to make clear that, for example, a North Korean attack on submarine cables would be considered an internationally wrongful act in the eyes of international law. I suggest that submarine cables can be treated as a public good. Kaye agrees with this idea, stating that the deep seabed is part of the of the common heritage of mankind (Kaye 2007, 70). This places underwater submarine communication cables in the global commons. Therefore, these cables would be placed under customs and practices governing the high seas, limiting jurisdiction by states and their vessels except in specific circumstances (UNCLOS Article 113).

[9] The International Cable Protection Committee is a non-profit organization formed in 1958 to promote the protection of international telecommunications and submarine cables. As of May 2022, 65 states among 185 members, including cable owners, operators, manufacturers, as well as service providers have joined the ICPC (ICPC 2022).

As an intergovernmental organization (IGO), the International Telecommunication Union (ITU) can also contribute to developing international law, for example, by promoting its commitment to protecting submarine communication cables. This builds on the ITU's idea from its 2010 publication to utilize submarine communication cables for multiple purposes, not just to deliver data but also to monitor climate change. South Korea can champion the broader uses of cables as one of the reasons it is appropriate to call a submarine communication cable a public good.

There are three places where South Korea can share its vision in developing international law on protecting submarine communication cables. As discussed, one is the ITU. Another is the ICPC. And the issue of providing better protection for submarine communication cables can be a topic for discussion even at UN General Assembly. The argument here can be that since we can utilize submarine cables for a common purpose to monitor climate change, it is essential that we make efforts to protect them better than how UNCLOS currently operates.

As a middle-power country with a good relationship with all P5 states (China, France, Russia, the U.K., and the U.S.), South Korea can propose a UN General Assembly resolution to protect submarine communication cables better, thus recognizing their importance as a public good. My rationale behind this argument is that besides being one of the core infrastructures on which global citizens rely every day for internet communication, submarine communication cables can also be utilized for the common good. For example, they are capable of monitoring climate change while providing internet, fulfilling a dual purpose.

South Korea can raise its voice in overseeing submarine communication cables, even when they are located beyond its territorial sea, in working with an IGO (i.e. the International Maritime Organization [IMO]). An IGO's role is to set agendas and encourage states to help craft international norms. Currently, the secretary-general of the IMO is South Korean. Kitack Lim has been in office since 2005 and will serve until December 2023. The fact that Lim is a South Korean government official, and has become secretary-general of the IMO he had to compete for the position (Park 2018), indicates that South Korea cares deeply about maritime issues.

Another idea is to revive the discussion of reforms to IMO rules and regulations so as to better protect submarine communication cables. Supportive leadership can be an asset to South Korea if its agenda encourages a more sophisticated international norm and if it decides to use the IMO as a forum to achieve its goal. South Korea is in a good position to serve as a catalyst to raise its voice in developing an international norm to regulate submarine cables.

The "Draft Resolution on Oceans and the Law of the Sea" was published in November 2021, while the UN General Assembly was in session. The Permanent Mission of the Republic of Korea to the UN has shown great interest in giving its opinion in the future, especially regarding submarine cables, when the resolution undergoes revision. I learned this fact in my direct encounter with the Permanent Mission on February 18, 2022, when I conducted my field research interview for this study.

Although Figure 9 shows that the 2021 UN General Assembly (UNGA) Draft Resolution on Oceans & Law of the Sea does not contain anything new but repeats what has been already stated in UNCLOS regarding submarine cables, it was still a discovery for me to learn that submarine cables are a topic included in the Draft Resolution. Having a highly-ranked South Korean official bring the existence of this open source material, a draft resolution, to my attention helped give me more confidence that the South Korean government is indeed interested in playing a larger role in this field in the future.

2021 UNGA Draft Resolution on Oceans & Law of the Sea	**Author's Suggestions to Add for Revision**
- States are called to take measures to protect fiber optic submarine cables and to fully address issues relating to these cables, in accordance with international law, as reflected in the Convention (para 184).	- The courts of the country of the cable owner's citizenship should be open to **civil actions** brought by the owner against someone who allegedly damaged that cable, regardless of any other connection that the defendant might have to that jurisdiction.
- Also encourages the adoption by States of laws and regulations regarding the breaking or injury of submarine cables or pipelines beneath the high seas done willfully or through culpable negligence by a ship flying its flag or by a person subject to its jurisdiction, in accordance with international law, as	- The country of the owner's citizenship should be permitted to **prosecute** the party alleged to have caused the damage in its domestic courts just as UNCLOS provides in the perpetrator's state.

reflected in the Convention (para186).	

Figure 9. Suggestion made by the author to revise the provisions in the 2021 UNGA Draft Resolution on Oceans and Law of the Sea.

The suggestions provided above would establish a regime that not only punishes people who damage cables after the fact but would create a deterrence mechanism to reduce the risk of such misbehavior. First, the availability of a civil remedy is made explicit, compared to the UNGA resolution; the language I suggest for revision is more specific. Second, in UNCLOS Art. 113, it is clear that the courts of the flag state, in other words of the perpetrator, have exclusive jurisdiction to hear civil and criminal cases. I suggest that permitting prosecution in the jurisdiction of the submarine communication cable owner, in addition to that of the perpetrator, would also have the deterrent effects, so that submarine communication cables are less likely to be destroyed intentionally.

More thought should be given to how submarine communication cables are mentioned in the 2021 UNGA Draft Resolution on Oceans & Law of the Sea. Not noticing any differences between the language of UNCLOS and the UNGA Draft Resolution, I thought no progress was being made towards developing international law regarding submarine cables. Then, I realized that there probably was a vital reason why, despite the existence of UNCLOS, states gathered at UNGA and reiterated the importance of "adoption by States of laws….the breaking or injury of submarine cables beneath the high seas done willfully or through culpable negligence by a

ship flying its flag or by a person subject to its jurisdiction, in accordance with international law, as reflected in the Convention," as stated in UNCLOS.

This suggests that submarine communication cables are being cut more frequently than is being reported to us by the media. And this probably is the reason why a number of states at the UN General Assembly felt the need to re-write the clauses of UNCLOS in the UNGA Draft Resolution, to give a warning to perpetrator states that in fact they are violating existing international law, UNCLOS. Doing this at the UN table and having states pass a resolution could add more pressure on potentially responsible states, adding a deterrent effect to discourage them from destroying submarine communication cables in the high seas.

7. Conclusion

In today's world, the security of submarine communication cables seems important beyond our imagination. As much as ninety five percent of internet traffic moves via submarine cables (van Ouderaren 2021). Because of their price competitiveness over satellites, cables are dominating the industry. In this dissertation, I tested a hypothesis that submarine cables are inadequately protected under the current international legal regime. The regime applied, UNCLOS, is examined throughout the dissertation.

The answer to the question on the current structure of the international regulatory regime can be summarized as follows: Submarine communication cables are inadequately

regulated, and international law on this subject is considered outdated. Beneath the high seas, the only state that is legally able to take action against a vessel or individual that breaks a cable is the vessel's flag state or the state of citizenship of the responsible person. The problem here is that a state with an interest in the cable--because of ownership or due to the fact that the cable connects to the shore--is not usually able to take any legal action against a vessel cutting the cable (Scott 2022).

As more people have begun paying attention to this field of submarine communication cables and international law, the submarine communication cable industry has been identified as a potential battleground among states. So far, the U.S. has maintained its status as a world-leading hub. However, China's ownership of cables, which was seven percent of the world's total in 2012, is now predicted to be twenty percent by 2025 (Mayville 2021, 26:22). This reflects China's keen interest in cable investment.

Another expert's finding also supports my argument. Jonathan E. Hillman from the Center for Strategic and International Studies (CSIS) argues that China has turned its position from a dependent to a controller of submarine cables within a decade (Hillman 2021, 12). Now, it is the fourth major provider of submarine cables after the U.S., Europe, and Japan (Hillman 2021, xii). According to the statistics from 2019, South Korea has nine submarine communication cables, and used to be ranked first in Asia and the Pacific (O'Malley 2019, 387). According to the record from 2021, other Asian countries like China and Japan have been

actively building their state-owned communication cables lately, taking over what was South Korea's place in this industry. It now ranks sixth in the major submarine communication cable provider countries worldwide (Technavio 2020).

Western countries often call China's state-sponsored hacking an internationally wrongful act. However, Edward Snowden exposed that the U.S. and the U.K. have also been tapping into submarine communication cables, thus eavesdropping on other states. For example, it has been reported that the USS Jimmy Carter was built with an hourglass-shaped section that makes it possible not only to listen to submarine communication cables but also to plant listening devices on the ocean floor (Axe 2020). The possibility of espionage or a state's kinetic attack on a critical cable infrastructure is a common and rising international concern to be monitored, as declared by the UN General Assembly in 2010 (UNGA Resolution 65/31 para 121, December 6, 2010).

From the perspective of South Korea, if the U.S. and China disagree on how to protect submarine communication cables at an international level and continue the New Cold War (Brands and Gaddis 2021, 10; Bremmer 2021, 127), South Korea may find itself caught up in a dilemma—of being asked to pick a side, while also being sandwiched by powerful nations.

As a UN agency, the International Telecommunication Union (ITU) can contribute to the development of international law, for example, by promoting its commitment to protecting submarine communication cables. This approach was developed because of the use of cables

not only to deliver data but also to monitor climate change, as indicated in the ITU's 2010 publication (ITU 2010, 2). South Korea can champion broader uses of submarine communication cables, as it may argue that a submarine communication cable can be considered a public good (Kaye 2007).

Another possibility for South Korea to play a catalyst role in developing a new norm regarding submarine cables is through its influence in the International Maritime Organization (IMO). The IMO's role is to set agendas and encourage states to participate in crafting international norms in matters relating to the sea. Currently, the secretary-general of the IMO is South Korean (IMO 2021). Under this circumstance, the idea I am proposing here is to utilize the IMO by reviving the discussion of reforms to IMO rules and resolutions so as to better protect submarine communication cables.

The 2011 version of IMO Rules and Regulations on Protecting Submarine Cables speaks of how the Automatic Identification System (AIS) operates to provide conclusive proof for some faults. An example of such a clause states that an anchor is released as a result of becoming loose in heavy weather. Having such technology available to better differentiate accidents from deliberate attacks can contribute to developing an international norm to protect submarine communication cables eventually since such technology can help eliminate the non-attack cases of submarine cables.

Some suggestions on improving the IMO rules made by the Vice Chairman of the ICPC,

Mike Green, are the following: 1. Wider port inspections, to meet the higher maritime security measures, set by, for example, the IMO code of practice, are needed to avoid submarine cable failures because of anchors. 2. Introducing an interlock on anchors is necessary when secured for sea passage with an alarm on the bridge of a ship (Green 2011). This would reduce the likelihood of accidental deployment.

The IMO rules are about detecting accidents, using the advanced technology to sort out the accidents that make up about seventy percent of global damage to submarine cables caused by fishing or anchoring (ICPC 2021, 2). It is worthwhile to rely on the IMO rules and the technology listed in the rules because, if they detect a cut in a submarine cable was an accident caused by an anchor, then the challenge on attribution is solved and the damage done on the submarine communication cable can be narrowed down to be under the attack category from the perspective of international law.

The rules discussed above are from the International Telecommunication Union (ITU), dedicated to distinguishing what kind of accidents took place by their measurements. Another way to develop international law to better protect submarine communication cables is through the International Maritime Organization (IMO). In other words, receiving leadership support from the IMO could be an asset to South Korea if its agenda urges a more sophisticated international norm, and if South Korea decides to use the IMO as a forum to achieve this goal.

Daily, ninety-five percent of worldwide internet traffic is transmitted from one

continent to another via submarine communication cables rather than satellites. Because of this, more people are paying attention to the security of submarine cables and the sensitive information flowing through them. The research question asked in this study is which international legal regime applies to submarine communication cables and global marine communications? The study disregards damage caused by accidents or by activities such as fishing (Roach 543, 2021), and focuses on intentional kinetic cuts to submarine communication cables, for example, by a military submarine. When this occurs, the treaties and customary international laws available to protect those submarine cables and the information inside them are examined.

After the limits of current international law are acknowledged, the theory of international cooperative regime development is applied and some recommendations are offered on the role the South Korean government can play as a catalyst in developing new norms in this field. Here, the underlying assumption is that as one of the leading suppliers of fiber-optic cables, South Korea can voice its opinion on how to improve the protection of submarine communication cables and the information they carry, thus uniting with likeminded countries. Several ways that South Korea can pursue this vision on the international stage are through the ITU, the IMO, and the UNGA.

Furthermore, as part of the efforts to borrow some ideas to fill the void in international law, the newly issued 2021 ICPC Government Practices for Protecting and Promoting Resilience of

Submarine Communication Cable has been reviewed. The fact that the Permanent Mission of the ROK to the UN is willing to offer its opinion on the submarine cable section of the Draft Resolution on Oceans and the Law of the Sea, as it undergoes the finalizing stage in 2022, supports my argument that South Korea is capable of playing a significant role in this field, serving as a catalyst to build an international regulatory regime—an idea that comes from the theory of international cooperative regime building.

8. Recommendations for Future Study

The topics for future study consist of the following: The latest technology in communication is Elon Musk's Starlink, which helped Ukrainians stay online while internet connections failed in November of 2021, during the Russian invasion. Although only one percent of our data traveled via communication satellite as of 2021, the latest move in the commercial sector is to invest more in this business. The prediction is that in addition to the 18,000 satellites already existing, tens of thousands of satellites are likely to be launched in the next decade (Hillman 2021, 188), following Musk's lead.

The scope for my dissertation included discovering which international law applies to protect submarine cables, one highway for information. Communication technology is advancing quickly; we are living in a world where our data are not just traveling via submarine cables but via a method like Starlink, using satellites in a low orbit.

This dissertation looked at whether any effective international law exists to address physical damage done to submarine cables laid beneath the high seas willfully or through culpable negligence by a ship flying its flag or by a person subject to its jurisdiction, in accordance with international law, as reflected in UNCLOS.

More topics to be explored from the international law perspective as relates to the high seas include questions like what if when an attacker of a submarine cable is not a state but a non-state actor like a terrorist group? Another question to be explored is what if the attack on a submarine communication cable in the high seas is not a kinetic attack, meaning an attack that can be visually observed? I am still curious to learn the international legal consequences if a cyber-attack like stealing money from another state's or civilian's account is conducted through submarine communication cables while the funds were being transferred from one continent to another.

9. Appendix: Section on Submarine Cables, 2021 UN General Assembly Draft Resolution on Oceans and the Law of the Sea Section on Submarine Cables

Recognizing that fiber optic submarine cables transmit most of the world's data and communications and hence are vitally important to the global economy and the national security of all States, conscious that these cables are susceptible to intentional and accidental damage from shipping and other activities and that the maintenance, including the repair, of these cables is important, noting that these matters have been brought to the attention of Stat es at various workshops and seminars, and conscious of the need for States to adopt national laws and regulations to protect submarine cables and render their willful damage or damage by culpable negligence punishable offences ,

PP40. Noting the importance of the delineation of the outer limits of the continental shelf beyond 200 nautical miles an d that it is in the broader interest of the international community that coastal States with a continental shelf beyond 200 nautical miles submit information on the outer limits of the continental shelf beyond 200 nautical miles to the Commission on the Limits of the Continental Shelf (the Commission), and welcoming the submissions to the Commission by a considerable number of States Parties to the Convention on the outer limits of their continental shelf beyond 200 nautical miles, that the Commission has continued to fulfil its role, including of making recommendations to coastal States, and that the summaries of recommendations are being made publicly available,

PP41. Noting also that some coastal States may continue to face particular challenges in relation to preparing and presenting submissions to the Commission,

PP42. Noting further that financial and technical assistance may be sought by developing countries for activities in relation to preparing and presenting submissions to the Commission, including additional information with respect to submissions and revised or new submissions, including through the voluntary trust fund established by the General Assembly in its resolution 55/7 of 30 October 2000 for the purpose of facilitating the preparation of submission s to the Commission for developing States, in particular the least developed countries and small island developing States, and compliance with article 76 of the Convention, as well as other accessible international assistance,

PP43. … Para184. Also calls upon States to take measures to protect fiber optic submarine cables and to fully address issues relating to these cables, in accordance with international law, as reflected in the Convention; 185. Encourages greater dialogue and cooperation among States and the relevant regional and global organizations through workshops and seminars on the protection and maintenance of fiber optic submarine cables to promote the security of such critical communications infrastructure; 186. Also encourages the adoption by States of laws and regulations addressing the breaking or injury of submarine cables or pipelines beneath the high seas done willfully or through culpable negligence by a ship flying its flag or by a person subject to its jurisdiction, in accordance with international law, as reflected in the Convention;

187. Affirms the importance of maintenance, including the repair, of submarine cables, undertaken in conformity with international law, as reflected in the Convention.

References

Ace Submarine Cable. 2022. https://acesubmarinecable.com/en/submarine-cable/

Allen, Gregory. 2019. "Chinese Strategic Intentions: a Deep Dive into China's Worldwide Activities: a Strategic Multilayer Assessment (SMA)." White Paper, December, 2019.

Anders, David. 2021. "Cable, Fiber, 5G and More: The Different Internet Connection Types and How They Work." CNET., September 13, 2021, https://www.cnet.com/home/internet/internet-connection-types/.

Arreguin-Toft, Ivan. 2006. *"How the Weak Win Wars: A Theory of Asymmetrical Conflict."* Cambridge University Press, January 2, 2006.

Axe, David. 2020. "We Now Have Details on the USS Jimmy Carter Spy Submarine Secret Mission." *The National Interest*. March 4, 2020.

Bae, Hyunjung. 2020. "LS C&C Wins Extensive Submarine Cable Deal Worth W200B."

Korea Herald, December 17, 2020.,

https://www.koreaherald.com/view.php?ud=20201217000843.

Balakrishanan, Chandrasekaran. 2014. "The Internet at the Speed of Light.," 13th ACM Workshop, October 2014.

Barrett, Jonathan. 2020. "Exclusive: US Warns Pacific Islands about Chinese Bid for Undersea Cable Project.," *Technology News*, December 17, 2020.

Baynes, Chris. 2018. "Entire Country Taken Offline for Two Days after Undersea Internet Cable Cut.", *Independent*, April 11, 2018.

BBC. 2020. "US-China Row Moves Underwater in Cable Tangle.", June 18, 2020., http://www.bbc.com/news/world-asia-53088302.

BBC. 2014. "Transatlantic Telegraph Cable 1866", http://w.bbc.co.uk/ahistoryoftheworld/objects/nV6cNBDYRuS_SE5uxGdxwg

BBC. 2014b. "Edward Snowden: Leaks that Exposed US Spy Program." BBC, January 17

2014, https://www.bbc.com/news/world-us-canada-23123964.

Bergsten, Fred. 2009. “Two’s Company.” Foreign Affairs, September/October, 2009., https://www.foreignaffairs.com/articles/americas/2009-09-01/twos-company

Berkowitz, Peter. 2020. “The Elements of China Challenge”, Policy Planning Staff, Office of the Secretary of State, December 2020., https://www.state.gov/wp-content/uploads/2020/11/20-02832/2020/11/20-02832-Elements-of-China-Challenge-508.pdf

Bhattacherjee, et al. 2022. “cISP: A Speed-of-Light Provider.” USENIX: The Advanced Computing System. 2022. http://www.state.gov/wp-content/uploads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf

Biden, Joe. 2022. “Statement of President Joe Biden and First Lady Jill Biden on the Death of Queen Elizabeth II.” The White House, September 8, 2022., https://www.whitehouse.gov/briefing-room/statementsreleases/2022/09/08/statement-of-president-joe-biden-and-first-lady-jill-biden-on-the-death-of-queen-elizabeth-ii/.

Bill, Burns. 2013. “History of the Atlantic Cable & Undersea Communications from the First Submarine Cable of 1850 to the Worldwide Fiber Optic Network.” https://atlantic-cable.com/Cables/1956TAT-1/

Blinken, Antony J. 2022. “The Administration’s Approach to the People’s Republic of China.” US Department of State, May 26, 2022.

Bocetta, Sam. 2017. “Chinese State Sponsored Hacking: It’s Time to Reach an Effective and Lasting Bilateral Agreement on Cyberwarfare,” *The Strategy Bridge,* https://thestrategybridge.org/the-bridge/2017/11/23/chinese-state-sponsored-hacking-its-time-to-reach-an-effective-and-lasting-bilateral-agreement-on-cyberwarfare

Brands, Hal and John Lewis Gaddis. 2021. “The New Cold War: America, China, and the Echoes of History.” Foreign Affairs. 2021., https://www.foreignaffairs.com/articles/united-states/2021-10-19/new-cold-war.

Bremmer, Ian. 2021. “The Technopolar Moment: How Digital Powers Will Reshape the Global Order.” *Foreign Affairs*, https://foreignaffairs.com/articles/world/2021-10-19/

/ian-bremmer-big-tech-global-order.

Bressie, Kent. 2016. “Marine Jurisdictional Problems for Submarine Cables.”, *In SubOptic.* Washington DC: Harris, Wiltshire & Grannis LLP.

Brown, Caroline E. 2020. “Team Telecom Opposes US-Hong Kong Communications Link”, 2020, Washington DC: Crowell & Morning LLP.

Bueser, Christian. 2022., “Security Threats to Undersea Communications Cables and Infrastructure Consequences for the EU.,” European Parliament, April 2022.

Burnett, Douglas R. 2006. “The Importance of the United Nations Law of the Sea Convention to the Cable Industry.,” Submarine Telecoms Forum. May 26, 2006.

Burnett, Douglas R. 2014a. *Submarine Cables in the Sargasso Sea: Legal and Environmental Issues in Areas beyond National Jurisdiction: The Legal Framework under UNCLOS.* Washington, DC: George Washington University Law School.

Burnett, Douglas R, ed. 2014b. *Submarine Cables: The Handbook of Law and Policy*. Boston:

Martius Nihoff Publishers.

Burnett, Douglas R. 2016. *"Submarine Cables and the UNCLOS*." Squire Pattons Boggs LLP, 2016.

Burnett, Douglas R., et. al., 2017. "International Submarine Cables and Biodiversity of Areas beyond National Jurisdiction: The Cloud beneath the Sea.", 2017, http://www.jstor.org/stable/pdf/10.1163/j.ctt1w76vr5.4.pdf.

Burnett, Douglas R. 2021. "Submarine Cable Security & International Law." *International Law Studies,* Stockholm Center for International Law.

Capacity. 2012. "ACE Launches in 13 Countries." https://www.capacitymedia.com/article/29ot5fqcgf5jpfdigi1hc/news/ace-launches-in-13-countries.

Chae, Saerom. 2021. "Facebook Down, Emphasis on Connecting the Internet …150,000km Submarine Cable under Construction." *Yonhap News Agency*, October 7, 2021.

Chong, Heongju, et al. 2013. “Optics vs. Copper: from the Perspective of Thunderbolt Interconnect Technology,” *SPIE OPTO*, February 27, 2013.

Cheney, Clayton. 2019. “China’s Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism.” Issues & Insights Working Paper, Vol. 19. WP8, July 2019. Pacific Forum, CSIS, July 2019.

Cho, Namhoon. 2018. *Defense Policy 2040: Northeast Asia Security Order Prospects and Response Strategy.*, Seoul: Korea Institute for Defense Analyses, 2018.

Cisco. 2019. “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2017-2022.”, Cisco, February 2019., http://media.mediapost.com/uploads/CiscoForecast.pdf

Coffey, Valerie C, 2014. The Challenges Facing Submarine Optical Communications, *Optics & Photonics News,* March 2014.

Convention for the Protection of Submarine Telegraph Cables, 1884.

Convention on the High Seas, 1958.

Dai, Xinyuan, et al., 2017. “International Cooperation Theory and International Institutions.” International Studies, November 20, 2017.

Davenport, Tara, 2012. “Submarine Communication Cables and Law of the Sea: Problems in Law and Practice.,” *Oceans Development and International Law,* 43,3, (July), https://doi.org/10.1080/00908320.2012.698922

Davenport, Tara. 2015. “Submarine Cables, Cybersecurity and International Law: An International Analysis.” *The Catholic University Journal of Law and Technology.* 24, no.1: 57-109.

Davenport, Tara. 2021. “International Interference with Submarine Cable Systems in Peacetime: Gaps in International Law.” Center for International Law, National University of Singapore.

Dreyer, June Teufel. 2021. “AUKUS, Australia and China,” *The Asan Forum*, The Asan Institute.

Edwards, Jim. 2018. “The Internet’s Worst-Case Scenario Finally Happened in Real Life: An

Entire Country Was Taken Offline, and No One Knows Why." *Business Insider*, April 10, 2018.

Federal Communications Commission, Fukushima, Akiko. 2021. "Promises and Challenges of Digital Connectivity," European University Institute., https://cadmus.eui.eu/handle/1814/71620

Fernandez, Jay A. "Sundance Audience Shaken by Brutal 'Killer'.", Reuters, January 26, 2010.

Fuller, Alice. 2021. "Russian Spy Ship That Can Cut Undersea Cables Spotted in English Channel.", *New York Post*, September 13 2021.

Gillian, Cookson. 2000. "The Transatlantic Telegraph Cable: Eighth Wonder of the World.," *History Today*, 50, 3 (March).

Glanz, James, et al. "A Deep-Diving Sub. A Deadly Fire. And Russia's Secret Undersea Agenda.," *New York Times*, April 21, 2020.

Glover, Bill. 2022. “Atlantic Cable: 1856-2018.,” *The Atlantic Cable*, https://atlantic-cable.com/Cables/CableTimeLine/atlantic.htm.

Green, Mick. “CIL-ICPC Workshop on Submarine Cables Session #5: Using IMO Rules and Regulations to Protect Submarine Cables.” ICPC, April 14-15, 2011.

Gresh, Geoffrey F. 2020. To Rule Eurasia’s Waves: The New Great Power Competition at Sea. New Haven: Yale University Press, 2020.

Grieco, Joseph M. 1988. “Anarchy and the Limits of Cooperation: A Realist Critique of the Newest Liberal Institutionalism.” International Organization 42 (3):1-14.

Han Kyoreh, 2022, https://english.hani.co.kr/arti/english_edition/english_editorials/1044987.html

Han, Seung-soo. 2007. *Beyond the Shadow of 9/11: a Year at the United Nations General Assembly*. Washington DC: JHU SAIS Reischauer Center for East Asian Studies.

Harbin, Dennis E. 2021. “Targeting Submarine Cables: New Approaches to the Law of Armed

Conflict in Modern Warfare." *Military Law Review*, 229, no. (3).

He, Yujia. 2019. "Connecting the Emerging Markets: China's Growing Role in Global Digital Infrastructure."

HKUST IEMS, 2019, https://iems.ust.hk/publications/thought-leadership-briefs/he-connecting-the-emerging-markets-china-s-growing-role-in-global-digital-Infrastructure.

Hendel and Swan. 2020. "Justice Department Opposes Google, Facebook Cable Link to Hong Kong," Politico, June 17, 2020., https://www.politico.com/news/2020/06/17/justice-department-hong-kong-google-facebook-cable-326688.

Hillman, Jonathan E. 2021. "Securing the Subsea Network: A Primer for Policymakers." CSIS, March 2021., https://www.csis.org/analysis/securing-subsea-network-primer-policymakers

Hillman, Jonathan E. 2021. "US at Risk of Losing Cloud Computing Edge to China." Politico, August 26, 2021., https://www.politico.com/newsletterspolitico-china-

watcher/2021/08/26/us-at-risk-of-losing-cloud-computing-edge-to-china-494105

Hillman, Jonathan E. 2021. *The Digital Silk Road: China's Quest to Wire the World and Win the Future.* New York: Harper Collins.

Hinct, Garret. 2017. "Cutting the Cord: The Legal Regime Protecting Undersea Cables." Lawfare (blog),. November 21, 2017. http://www.lawfareblog.com/cutting-cord-legal- legal-regime-protecting-undersea-cables.

Hinct, Garret. 2018. "Evaluating the Russian Threat to Undersea Cables." Lawfare (blog),. March 5, 2018., https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

Honniball, Arron N. 2016. "The Exclusive Jurisdiction of Flag States: a Limitation on Pro-active Port States?", *The International Journal of Marine and Coastal Law*, 31: 499-530.

International Cable Protection Committee. 2022. "About ICPC," November 11, 2022., htpps://www.iscpc.org/about-the-icpc/

International Cable Protection Committee. 2021. *Government Best Practices for Protecting and Promoting the Resilience of Submarine Telecommunications Cables*.

International Law Commission. 2001. *Report of the International Law Commission on the Work of Its Fifty Third Session.,* https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

International Maritime Organization. 2021., https://www.imo.org/en/MediaCentre/PressBriefings/Pages/30-SG-election.aspx. https://www.imo.org/en/About/Pages/Default.aspx International Telecommunication Union.

ITU. 2010. "ITU-T Technology Watch Report.," https://www.itu.int/oth/T0B1500000C/en.

International Telecommunication Union. 2021. Accessed January 14, 2022, https://www.itu.int/en/about/Pages/vision.aspx.

Kaye, Stuart. 2007. "Threats from the Global Commons: Problems of Jurisdiction and

Enforcement." *International Law Studies*, 83: 69-81.

Kazaz, Nicholas. 2022. "Are Laws Regulating Subsea Cables Outdated?." *Submarine Telecoms Forum*, March 29, 2022.

Keohane, Robert O. 1982. "The Demand for International Regimes." International Organization 36 (2): 325-55, 1982.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton: Princeton University Press.

Keohane, Robert O., and Lisa L. Martin. 1995. "The Promise of Institutional Theory," International Security, 20 (1): 39-51.

Keoppel, Dan. 2019. "Moving to the Woods Killed My Internet. Here's What I Did about It." *New York Times,* September 11, 2019.

Kim, Chai-Hyung. 2017. "Legal Regime of International Society concerning Laying and Use of Submarine Cables." *Maritime Law Review*, March 2017.

Kim, Youngman. 2017. “Expert Warns of North Korea’s Growing Cyberwar Capabilities.” Voice of America, October 14, 2017.

Kim, Jonathan. 2022. “Submarine Cables: the Invisible Fiber Link Enabling the Internet.” Dgtl Infra, May 4, 2022, https://dgtlinfra.com/submarine-cables-fiber-link-internet/#:~:text=Submarine%20cables%20connect%20continents%20and,States%20and%20the%20United%20Kingdom.

Kim, Hyun-bin. 2020. “LS Possible Acquisition of KT Submarine Could Generate Synergy.” *Korea Times*, October 21, 2020., https://www.koreatimes.co.kr/www/tech/2021/02/515_297891.html.

Kim, Minsoo. 2012. “Trends of Legal Systems for Protecting Submarine Cables and Implications.” *Dokdo Research Journal.* 16 :68-75.

Kim, Sangbae. 2020. “Data Security and Digital Hegemony Competition: from the Perspective of Emerging Security and Complex Geopolitics.,” *National Strategy*. 26 (2): 5-34.

Koh, Harold Hongju. 2012. “International Law in Cyberspace,” *Harvard Law Journal* 54.

Koeppel, Dan. “Moving to the Woods Killed My Internet. Here’s What I Did about It.” New York Times, September 11, 2019.

Kraska, James. “The Law of Maritime Neutrality and Submarine Cables.” *EJIL: TALK*, July 29, 2020, https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/.

Kuehn, Kathleen. 2016. The Post-Snowden Era: Mass Surveillance and Privacy in New Zealand., Wellington, New Zealand: Bridget Williams Books.

Le Monde diplomatique. 2021. “Geopolitical Competition of Submarine Cables, US and Intermediate Network Infrastructure.”

Lee, Luke T. 1983. “The Law of the Sea Convention and Third States.” The American Journal of International Law, 77, no 3.

Lee, Stacia. 2017. “The Cybersecurity Implications of Chinese Undersea Cable Investment,” East Asia Center, University of Washington, February 6, 2017., https://jsis.washington.edu/news/cybersecurity-implications-chinese-undersea-cable-

investment/

Lee, Kibum. 2020. “Protecting Submarine Cables and International Law.” Navy Brief, Asan Institute for Policy Studies, December 14, 2020.

Liu, Coco.2020. “Cloud over Alibaba and Tencent as US raises pressure on China Tech.” Nikkei Asia, August 8, 2020, https://asia.nikkei.com/Business/Technology/Cloud-over-Alibaba-and-Tencent-as-US-raises-pressure-on-China-tech Maritime Zone

Little, Becky. 2021., “The First Transatlantic Telegraph Cable Was a Bold, Short-Lived Success.,” *History,* October 28, 2021., https://www.history.com/news/first-transatlantic-telegraph-cable.

Nielson, Wayne. 2021. “Global Outlook,” Submarine Telecoms Forum, Issue 116, January 2021.

Nikkei Asia, “Tonga Re-connects to World as Submarine Cable Restored after Tsunami,” February 22, 2022.

Pompeo, Michael R. 2022. “The US Protects National Security and Integrity of 5G Networks.,” US Department of State, May 15, 2020.

Prisloo, Loni. 2021. “Facebook to Expand Planned Undersea Network in Africa” *Bloomberg,* August 16, 2021.

Schematic, Tufts University., 2017. “Law of the Sea: A Policy Primer.” http://sites.tufts.edu/lawofthesea/chapter-two.

Shepardson, David. 2021. “U.S. Recommends Approving Google, Meta Undersea Data Cable to Asia.,” *Reuters*, December 17, 2021.

Shin, Beomchul. 2008. “International Law and the Use of Force: Shaping the UN Charter’s Regime and Its Evolution.,” Korea Institute for Defense Analyses Press.

Submarine Cable Networks. 2011. “AC-2/Yellow.”, February 15, 2011. https://www.submarinenetworks.com/systems/trans-atlantic/ac-2

Capacity. 2012. “ACE Launches in 13 Countries.”,

https://ww.capacitymedia.com/article/29ot5fqcgf5jpfdigi1hc/news/ace-launches-in-13-countries.

Sutton, H I, "How Russian Spy Submarines Can Interfere with Undersea Internet Cables." *Forbes*, August 19, 2020.

Technavio, 2020. "Submarine Fiber Cable Market by Investment Source and Geography-Forecast and Analysis 2020-2024."

The Independent. April 11, 2018., http://www.independent.co.uk/tech/mauritiana-internet-cut-underwater-cable- offline-days-west-africa-a8298551.html.

The Strategy Bridge, November 23, 2017., https://thestrategybridge.org/the-bridge/2017/11/23/chinese-state-sponsored-hacking-its-time-to-reach-an-effective-and-lasting-bilateral-agreement-on-cyberwarfare.

Matis, MS. 2012. "The Protection of Undersea Cables: a Global Security Threat.," Defense Technical Information Center, https://apps.dtic.mil/sti/citations/ADA561426.

Mayville, William C., et al. 2021. “Securing the Subset Network.” CSIS Webinar. April 8, 2021. http://www.youtube.com/watch?v=bWWd6emoFhI.

Moon, Jungin. 2022. “America’s Shaky Leadership Makes for Uneasy Global Order.,” *The Hankyoreh*, May 29, 2022, https://m.hani.co.kr/arti/opinion/column/1044812.html

Murphy, Sean. 2019. “International Law, Cases and Materials.” *West Academic Publishing,* 7 ed., March 6, 2019.

NATO Cooperative Cyber Defense Centre of Excellence. 2019. “Strategic Importance of, and Dependence on, Undersea Cables.,” https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.

National Geographic Resource Library, “Continental Shelf.”, https://www.nationalgeographic.org/encyclopedia/continental-shelf/ (last visited on April 28, 2022).

National Oceanic and Atmosphere Administration Office of General Council. 2019. “Submarine Cables: International Framework.”,

http://www.gc.noaa.gov/gcil_submarine_cables_international.html.

O'Malley, Sean. 2019. "Assessing Threats to South Korea's Undersea Communications Cable Infrastructure.", *Korean Journal of International Studies*, December 31, 2019.

UNCLOS 1982 Commentary. Leiden: Brill, 1995.

US Government Accountability Office. 2021. "Satellite Communications: DOD Should Explore Options to Meet User Needs for Narrowband Capabilities," September 2, 2021.

Nordquist, Myron H., et al. *UNCLOS 1982 Commentary Supplementary Documents*. Leiden: Martinus Nijhoff Publishers, 2012.

O'Connor, Elizabeth A. 2019. "Underwater Fiberoptic Cables: A Customary International Law Approach to Solving the Gaps in the International Law Framework." Medford: Tufts University.

O'Keeffe, Kate, et al. 2019. "National Security Concerns Threaten Undersea Data Link Backed

by Google, Facebook." *Wall Street Journal*, August 28, 2019.

Oye, Kenneth A. 1986. *Corporations under Anarchy*. Princeton: Princeton University Press.

Oxford Research Encyclopedia of International Studies. Oxford: Oxford University Press, 2021. Accessed March 16, 2021., https://doi.org/10.1094/acrefore/9780190846616.013.93.

Paik, Min Jung. 2020. "US's Position in Cyber Operation: Analysis in the Eye of International Law." Korea Institute for Defense Analyses., https://kida.re.kr/frt/board/frtNormalBoardDetail.do?sidx=2184&idx=693&depth=2&searchCondition=&searchKeyword=&pageIndex=3&lang=kr.

Public Broadcasting Service. 2022. "How the Early Cable Was Used." https://www.pbs.org/wgbh/americanexperience/features/cable-how-early-cable-was-used/.

Petty, Jason. 2021. "How Hackers of Submarine Cables May Be Held Liable under the Law of the Sea." *Chicago Journal of International Law*, 22, no. 1.

https://chicagounbound.uchicago.edu/cjil/vol22/iss1/18.

Reuters, 2020. “Exclusive: US Warns Pacific Islands about Chinese Bid for Undersea Cable Project.”, December 17, 2020, https://www.reuters.com/article/us-china-pacific-exclusive/exclusive-u-s-warns-pacific-islands-about-chinese-bid-for-undersea-cable-project-sources idUSKBN28R0L2.

Roach, Ashley. *Excessive Maritime Claims.,* Leiden, Netherlands: Brill, 2021.

Roach, Ashley, et al. 2020. “Submarine Cables and Pipelines under International Law Interim Report 2020.” International Law Association.

Roach, Ashley, et al. 2022. “Table of National Legislation on Submarine Cables and Pipelines.” International Law Association, January 15 2022, https://www.ila-hq.org/en_GB/documents/submar-2.

Robertson, Jordan. 2021. “The Long Hack: How China Exploited a US Tech Supplier.”, *Bloomberg.* February 21, 2021., https://www.bloomberg.com/features/2021-supermicro/.

Ryan-Mosley, Tate. 2022. “The World Is Moving Closer to a New Cold War Fought with Authoritarian Tech.,” *MIT Technology Review*, September 22, 2022.

United Nations General Assembly, “Seventy-sixth session of the UN General Assembly on Oceans and the Law of the Sea Draft Resolution on Oceans and the Law of the Sea.”, November 23, 2021., http://www.un.org/depts/los/general_assembly/general_assembly_resolutions.html.

Scobell, Andrew. 2018. “At the Dawn of Belt and Road: China in the Developing World.” Rand. https://www.rand.org/pubs/research_reports/RR2273.html.

Scott, Karen. 2022. “Outdated Laws Governing Undersea Cables Need Modernizing” gCaptain Forum, January 30, 2022., https://gcaptain.com/outdated-laws-governing-undersea/cables-need-modernizing/.

Shen, Hong. 2018. “Building a Digital Silk Road? Situating the Internet in China’s Belt and Road Initiative.”, *International Journal of Communication,* University of Southern California.

Sherman, Justin. 2021. “Cyber Defense across the Ocean Floor: The Geopolitics of Submarine Cable Security.”, The Cyber Statecraft Initiative, September 2021., https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf.

Sherman, Justin. 2020. “The Politics of Internet Security: Private Industry and the Future of the Web.”, Atlantic Council, October 5, 2020., https://www.atlanticcouncil.org/in-depth-research-reports/report/the-politics-of-internet-securityprivate-industry-and-the-future-of-the-web/.

Shepherd, Blair. 2020. “Cutting Submarine Cables: The Legality of the Use of Force in Self-Defense.,” *Duke Journal of Comparative and International Law*, https//scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1571&context=djcil

Simmons, Blake. 2021. “China is Financing Infrastructure Projects around the World—Many Could Harm Nature and Indigenous Communities.,” *The Conversation*, September 20, 2021, https://theconversation.com/china-is-financinginfrastructure-projects-around-the-world-many-could-harm-nature-and-indigenous-communities-168060

"Sixty-fifth session of the UNGA Resolution Adopted by the General Assembly." December 6, 2010., https://international.vlex.com/vid/res-65-31-resolution-861189011.

Slaughter, J. Matthew., et. al. 2021. "Data is Power: Washington Needs to Craft New Rules for the Digital Age." *Foreign Affairs*, April 16, 2021., https//www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital- age

Submarine Telecom Forum., 2021. "ICPC Releases Cable Protection Recommendations: Best Practices for Cable Protection and Resilience as Resource for Governments", July 14, 2021.

Sunak, Rishi. 2017. *Undersea Cables: Indispensable, Insecure*. Westminster: Policy Exchange.

Sutton, H.I. 2020. "How Russian Spy Submarines Can Interfere with Undersea Internet Cables." *Forbes*, August 19, 2020., https://www.forbes.com/sites/hisutton/2020/08/19/how russian-spy-submarines-can-interfere-with-underseainternet-cables/?sh=70f5fdd63b04.

Swinhoe, Dan. 2021. “What Is a Submarine Cable? Subsea Fiber Explained: Our Wireless World Depends on a Few Hundred Fiber Cables Laid on the Ocean Floor.” Data Center Dynamics, August 26, 2021., https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiberexplained/#:~:text=Subsea%20or%20submarine%20cables%20are,from%20one%20point%20to%20another.

TeleGeography. 2021. “Global Map of Submarine Cables.”, Accessed October 12 2021. https://www.submarinecablemap.com.

The National Interest., March 4, 2020, https://nationalinterest.org/blog/buzz/we-now-have-details-uss-jimmy-carter-spy-submarines-secret-mission-129272

Triolo, Paul. 2020. “The Digital Silk Road: Expanding China’s Digital Footprint,” *Eurasia Group*, April 8, 2020, https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint.pdf.

Trujillo, Clorina. 2014. “The Limits of Cyberspace Deterrence”, *Joint Forces Quarterly*,

National Defense University., ttps://ndupress.ndu.edu/JFQ/ Joint-Force-Quarterly-75 /Article/577560/the-limits-of-cyberspace-deterrence.

Tufts University. 2017. “Law of the Sea: A Policy Primer.”, https://sites.tufts.edu/lawofthesea/chapter-two.

United Nations Convention on the Law of the Sea, 1982.

United Nations Treaty Collection 2022. “1958 Convention on the High Seas,” April 29, 1958.

US Department of State, 2020. “The Elements of the China Challenge” Office of Policy Planning.

Van Oudenaren. John S., et al. 2021. “Submarine Cables: Backgrounder for Maritime Awareness Project.”

Veal, Robert, et al. 2019. “The Legal Status and Operation of Unmanned Maritime Vehicles.” *Ocean Development and International Law*, 50, no 1, (January).

National Bureau of Asian Research., Accessed February 23, 2021, https://www.nbr.org/publication/submarine-cables.

Wall, Colin. 2021. “Invisible and Vital: Undersea Cables and Transatlantic Security.,” Center for Strategic and International Studies, June 11, 2021.

Wall Street Journal. 2011. “China’s Milestone Dive.” July 27, 2011, https://www.wsj.com/articles/SB10001424053111903591104576470883731065002.

Wakefield, Jane. 2021. “How Will Tonga’s Broken Internet Cable Be Mended?” BBC News, January 24, 2022., https://www.bbc.com/news/technology-60069066

Welch, Larry D. 2011. “Cyber Space—the Fifth Operational Domain.” *Research Notes*, Institute for Defense Analyses, February 20, 2011.

Williams, Robert. 2020. “Untangling U.S. Concerns over Chinese Tech Companies and Digital Security,” PTC Center, University of Pennsylvania.

Worzyk, Thomas. *Submarine Power Cables Design, Installation, Repair, Environmental*

Aspects, Sweden: Springer, 2009.

Zaheer. 2021. “Wires That Run the World.” *The Economic Times*, September 17, 2021., http://economictimes.inidatimes.com/tech/newsletter.ettech-unwrapped/wires-that-run-theworld/articleshow/86311425.cms?from=mdr.