JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOL. 13 • NO. 1 • 2021 – 2022

POLICY PROPOSALS FOR THE UNITED STATES TO PROTECT THE UNDERSEA CABLE SYSTEM

Kevin Frazier

The protection of the undersea cable system, which carries the vast majority of the world's Internet traffic, requires a new policy approach from the United States government. Old vulnerabilities and new threats have placed this critical piece of international infrastructure under increased threat of disruption and sabotage. Old vulnerabilities include the inherent difficulties associated with defending cables that lay along the open seafloor across international waters and the fragility of the cables themselves--often no larger than a garden hose. New threats come from climate change and changes in geopolitics. For example, Russia, among other nations, has made investments in offensive military equipment tailored to breaking undersea cables.

Though disruptions to Internet traffic through the undersea cable system can be diverted to satellites, that alternative comes with significant financial and temporal costs. Therefore, proactive policies to prevent cable breaks should receive substantial attention from political leaders. The weeks and millions of dollars required to repair broken cables further justify the prioritization of proactive policies to reduce the frequency of breaks.

This article explores why current international and domestic laws and policies meant to protect undersea cables fall short of what is needed to ensure the longevity and security of the undersea cable system. After an analysis of these various laws and policies, the article offers a series of steps the Biden Administration can take to improve the resilience of the undersea cable system, at least the parts of it connected to the United States.

These steps make theoretical sense and have received support from policy leaders on this topic--actually taking the steps, though, will require significant political capital. The majority of the undersea cable system is owned and operated by private stakeholders. The protection of the system necessitates extensive collaboration between private and public stakeholders. Because collaboration takes time and trust, this article comes at a critical moment -- it can help direct political energy toward this time-sensitive endeavor.

CONTENTS

I. Introduction – A Vulnerable, Critical System

Picture this hypothetical: in the dark cloud of night, several Russian submariners prep for a world-changing mission. Covered by an even darker sea, the submarines sail west to the coast of California; more specifically, the submarines target a small slice of the coast—the approximate 200 miles between Morro Bay and Redondo Beach in which seventeen different undersea cables lay unprotected on the ocean floor.[1] After decades of investment in its Pacific Fleet,[2] the Russian government is ready to reap a return in the form of disrupting the Internet.

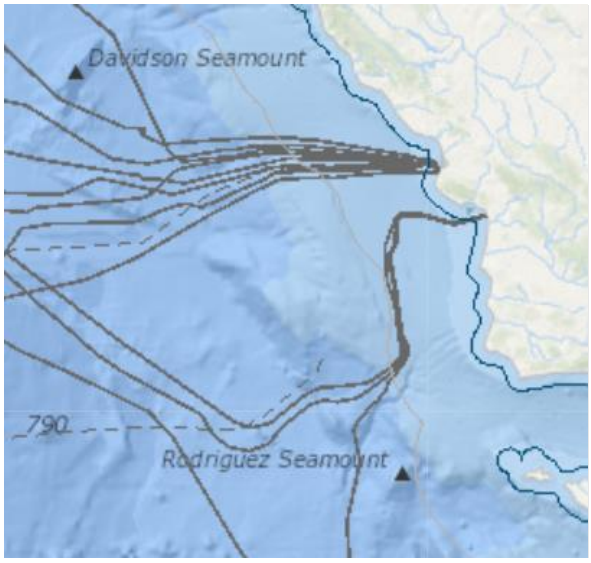

FIGURE 1: Depiction of the undersea cables off the coast of California.[3]

Once in place, the submarines begin their operation. Designed to perform technical work on the ocean floor, these machines are equipped for the task at

[1] TELEGEOGRAPHY (visual count of cables taken on Jan. 22, 2021), https://www.submarinecablemap.com/multiselect/landing-point?ids=morro-bay-ca-united-states,redondo-beach-ca-united-states,hawaii-kai-hi-united-states,lurin-peru [https://perma.cc/9Q38-FMJV].

[2] Peter Suciu, *Russia's Pacific Fleet Is Getting Stronger. Here's Why That Matters*, NAT'L INT. (June 2, 2020), https://nationalinterest.org/blog/buzz/russias-pacific-fleet-getting-stronger-heres-why-matters-159506 [perma.cc/9HCC-QSDM].

[3] *Marine Cadastre National Viewer*, OFF. COASTAL MGMT. (Jan. 22, 2021), https://marinecadastre.gov/nationalviewer/.

hand:[4] cutting the undersea cables—not that it is especially hard given that the cables are comparable in size to garden hoses.[5]

The small breaks in each of the cables amount to large disruptions to Internet access at both ends of the cables—the contiguous United States, where the cables launch, and the respective end destinations of the cables, including Hawaii, Japan, the Philippines, and Peru.[6] Internet service continues in each of these places but at much slower speeds. The undersea cable system is fairly redundant[7]—meaning that multiple cables often land at a single destination to prevent a single cable break from causing too much disruption.[8] However, a geographically-specific attack such as this one would force more Internet traffic to travel through satellites because the redundancy of the system would become a bug, rather than a feature. The high number of cables in close proximity would allow for a few submarines to knock out many cables. The resulting shift in traffic would result in lower quality, less reliability, less security, and more expensive Internet service.[9] Undersea cables, made up of fiber optic cores, "transfer data five times faster than satellites [and] do so at a vastly lower cost," according to Rishi Sunak, British Parliamentarian and author of a report on undersea cables.[10]

With Americans tweeting, albeit with less speed, about their sluggish Internet, the *USNS Zeus*, the U.S. Navy's lone cable repair ship,[11] mobilizes . . .

---

[4] Magnus Nordenman, *Russian Subs Are Sniffing Around Transatlantic Cables. Here's What to Do About It*, DEF. ONE (Jan. 17, 2018), https://www.defenseone.com/ideas/2018/01/russian-subs-are-sniffing-around-transatlantic-cables-heres-what-do-about-it/145241/.

[5] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, STRATEGIC IMPORTANCE OF, AND DEPENDENCE ON, UNDERSEA CABLES 1 (Nov. 2019), https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf [hereinafter CCDCOE].

[6] TELEGEOGRAPHY, *supra* note 1.

[7] *See* Garrett Hinck, *Evaluating the Russian Threat to Undersea Cables*, LAWFARE BLOG (Mar. 5, 2018, 7:00 AM), https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables [https://perma.cc/63R3-7XRQ] (outlining the redundancy of the undersea cable network by pointing out that "[c]utting the United States off from the rest of the world would require severing a large number of cables: at least 18 in the North Atlantic alone . . .").

[8] *Id.*

[9] THE COMMUNICATIONS SEC., RELIABILITY AND INTEROPERABILITY COUNCIL IV, WORKING GROUP 8 SUBMARINE CABLE ROUTING AND LANDING 1 (Dec. 2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf [https://perma.cc/39ZA-AABG] [hereinafter WORKING GROUP REPORT].

[10] RISHI SUNAK, UNDERSEA CABLES: INDISPENSABLE, INSECURE 13 (Dec. 1, 2017), https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf.

[11] *See* Hinck, *supra* note 7 (noting that "Congress authorized $250 million for a new ship that can lay and repair cables" in the U.S. defense authorization bill for fiscal 2018).

from Norfolk, Virginia . . . to respond to the threat in California.[12] Public and private actors demand a more expedient solution but receive an unsatisfactory response because the Navy has not outlined a plan for defending undersea cables.[13] Ultimately, the United States Federal Government calls on the International Cable Protection Committee (ICPC) for assistance. The ICPC, whose 170 members account for ownership of 97 percent of the world's undersea telecom cables,[14] coordinates a fleet of undersea cable repair ships. After several weeks and more than $17 million in repair costs,[15] the cables are restored.

This hypothetical is not far from reality. In 2008, an accidental cable break in the Mediterranean Sea diminished the reliability and quality of the Internet to such an extent that the United States military had to scale back its drone operations in the Middle East by an order of magnitude.[16] Similarly, when a cable connected to Vietnam failed in 2017, Internet customers in Ho Chi Minh briefly lost connectivity.[17] Intentional breaks of cables have also wreaked havoc on some nation states while advancing the aims of others and affiliated non-state actors.[18] As flagged by the think tank Chatham House and reported by the BBC, Ukrainian telecom providers noticed disruptions to an essential Internet exchange point as well as to cable connections in the midst of Russia's military action in the Crimean Peninsula in 2014.[19]

The under-discussed importance and vulnerability of the undersea cable system merit increased attention from, and action by United States policymakers. Society's increased reliance on the Internet justifies addressing the vulnerabilities of the system.[20] Additionally, absent action in the short-run, other activities in the

---

[12] *See generally* Voyage information of *USNS Zeus*, MARINETRAFFIC, https://www.marinetraffic.com/en/ais/details/ships/shipid:5430967/mmsi:367212000/imo:7932408/vessel:ZEUS#:~:text=ZEUS%20(IMO%3A%207932408)%20is,her%20width%20is%2022.25%20meters (documenting the various locations of the USNS Zeus, some of which are on or beyond the eastern coast of the United States) (last visited Nov. 7, 2021).

[13] Hinck, *supra* note 7.

[14] INT'L CABLE PROT. COMM., https://www.iscpc.org/ [hereinafter ICPC] (last visited Nov. 7, 2021).

[15] CCDCOE, *supra* note 5, at 3 (noting that it may take "several weeks and cost in excess of one million USD for a repair to be completed").

[16] Hinck, *supra* note 7.

[17] *Id.*

[18] *Id.*

[19] Chris Baraniuk, *Could Russian submarines cut off the internet?*, BBC (Oct. 26, 2015), https://www.bbc.com/news/technology-34639148 [https://perma.cc/25U6-R6HX] (quoting a representative of Chatham House as saying, "[Russia] can interfere with internet infrastructure in order to gain [complete] control of [the information available in] specific regions").

[20] WORKING GROUP REPORT, *supra* note 9, at 1.

sea will make future efforts to remedy the system even harder; increased exploration and exploitation of the seabed, for instance, is bringing new stakeholders into the proverbial arena and threatening to crowd out the interests of undersea cable operators.[21]

This paper contains six sections: a discussion of the importance of the undersea cable system to the Internet, an overview of the sources and severity of risks to that system, an assessment of the adequacy of the various legal frameworks and industry standards related to the system, a review of actions by other public and private actors to protect the system, an examination of the shortcomings of United States law and policy related to the system, and a proposal for policy responses by the United States.

Several issues are outside the scope of this paper. The impact of the undersea cable system on marine life and ecosystems will go uncovered. An authoritative report produced, in part, by the ICPC reports that the "laying of [undersea cables] on the surface of the ocean floor has a minor if not negligible one-off impact."[22] Nevertheless, some of the solutions discussed in Section VII may benefit marine life and ecosystems. Those secondary benefits will be left to others to fully examine.[23] This paper will also not provide a thorough examination of the issues related to cybersecurity and espionage associated with the undersea cable system. The decision to avoid these topics is based on the difficulty of eavesdropping via undersea cables and the ease of other means to accomplish the same objective.[24]

This paper instead is focused on raising awareness around the vulnerability of the undersea cable system during a time, in the midst of the COVID-19 pandemic, when Internet access is more important than ever.[25]

---

[21] *Id.* at 3.

[22] CARTER ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD 37 (UNEP-WCMC Biodiversity Series No. 31 2009).

[23] *See, e.g.*, Kingsley Ekwere, *Submarine Cables and the Marine Environment: Enhancing Sustainable and Harmonious Interactions*, 2016 CHINA OCEANS L. REV. 154, 161 (2016).

[24] *See, e.g.*, Richard Chirgwin, *Spies need superpowers to tap undersea cables*, THE REGISTER (Sept. 18, 2014), https://www.theregister.com/2014/09/18/spies_arent_superheroes/ [https://perma.cc/N9QQ-FUFW] (discussing the dangerous and resource intensive steps required to safely and effectively tap an undersea cable, noting that few nations possess the submarines requisite for such an activity, and pointing out three far easier means to get the same sort of information).

[25] Jessica Poiner, *In the midst of coronavirus, connectivity matters more than ever*, OHIO GADFLY DAILY (July 23, 2020), https://fordhaminstitute.org/ohio/commentary/midst-coronavirus-connectivity-matters-more-ever [https://perma.cc/6JEZ-4B99].

Furthermore, this paper aims to motivate action from Federal Government stakeholders in the wake of the transition to a new presidential administration; this transition presents an opportunity to reassess the current United States legal and policy approaches to the protection of the undersea cable system.

The paper will reveal the following conclusions: first, the protection of the undersea cable system is essential to a functioning Internet and, therefore, the economy, culture, and governance; second, intentional attacks by state and non-state actors and unintentional breaks by commercial actors pose the two greatest threats to the system; third, international law inadequately addresses those threats; fourth, United States domestic law also insufficiently addresses those threats; and, fifth, the United States Federal Government can most effectively and efficiently reduce the likelihood of those threats occurring and the severity of damage those threats could cause by partnering with the owners of the cables themselves to implement policy solutions.

II. The Undersea Cable System is Essential to a Fast and Reliable Internet

Undersea cables are foundational to a safe, reliable, and global Internet. Upwards of 97 percent of all Internet traffic travels on undersea cables.[26] "Submarine cables," as reported by The Working Group of the Communications Security, Reliability, and Interoperability Council, "provide the principle domestic connectivity between the contiguous United States" and its offshore states and territories (see Figure 2).[27] As of 2014, Internet cables carried more than 95 percent of United States Internet traffic, a percentage that is almost assuredly higher as of this writing.[28] Most of these cables have a series of fiber optic cables at their core; these cables are hair-thin strands of glass that allow for data to travel as wavelengths of light at speeds of approximately 180,000 miles per second.[29]

[26] CCDCOE, *supra* note 5, at 1.
[27] WORKING GROUP REPORT, *supra* note 9, at 1.
[28] *Id*.
[29] SUNAK, *supra* note 10, at 14.

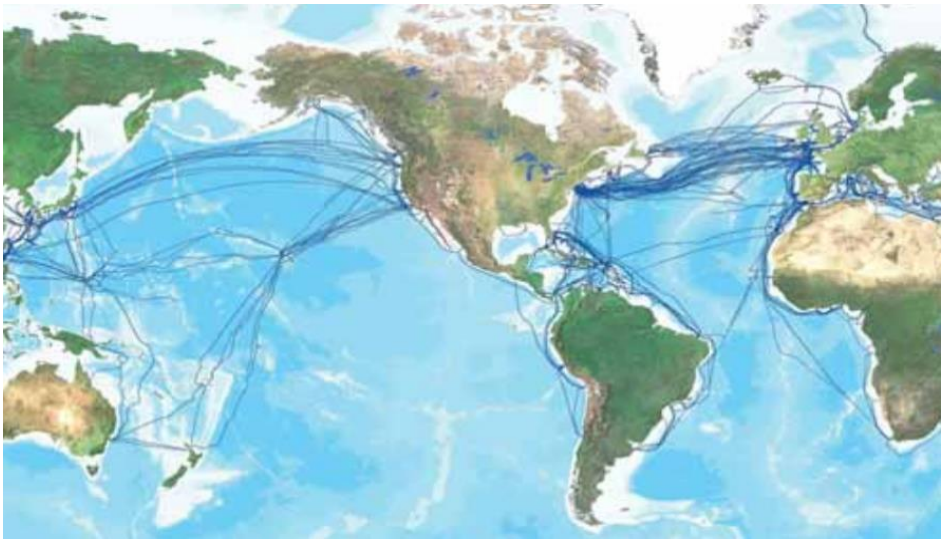

FIGURE 2: Undersea communications cables as of 2009.[30]

The private and public sectors rely almost exclusively on privately-owned cables to carry their Internet traffic. The importance of these cables to private and public interests qualifies them as "critical infrastructure" according to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).[31] Regular or persistent disruption to these cables could undermine modern society's ability to function.[32] The destruction of or disruption to an undersea cable may cut an entire area off from the Internet. Whether that area remains connected depends on the number of redundant cables and the existence of alternative routes for the Internet traffic, such as satellites.[33] What's more, as the number of people with Internet access increases around the world, the integrity of the cables will grow in importance due to the increase in the amount of data that will travel through the cable system.[34]

Despite the fact that undersea cables "carry the vast majority of civilian and military U.S. Government traffic, [as of 2014] the U.S. Government does not own and operate its own submarine cables."[35] The Federal Government has laid some of its own cables;[36] nevertheless, a Harvard report revealed that the agency

[30] CARTER ET AL., *supra* note 22, at 11.
[31] CCDCOE, *supra* note 5, at 1.
[32] *Id.* (comparing the cables to the "central nervous system" of the global Internet).
[33] *See id*. at 2.
[34] *Id.*
[35] WORKING GROUP REPORT, *supra* note 9, at 1.
[36] Hinck, *supra* note 7 (stating that the Pentagon has "publicly acknowledged [laying its own] cables connecting Miami to the naval base at Guantanamo Bay").

responsible for the Department of Defense's Internet networks depends on privately-owned cables for 95 percent of their strategic communications—indicating continued government reliance on private cables to carry even the most sensitive data.[37] This reliance on the undersea cable system means that "[d]amage to [the system] can pose grave risks to U.S. national security and the U.S. economy."[38] The number of cables running along the United States coastline further increases the importance of the integrity of the system to the United States military. Within the territorial sea, exclusive economic zone (EEZ), and outer continental shelf (OCS) of the United States there are at least 55 in-service submarine cable systems and at least a dozen have been proposed or are currently under construction.[39] These cables represent potential targets for foreign states, and non-state actors such as terrorist organizations.[40]

Private-sector entities likewise rely on the undersea cable system for fast, reliable Internet. "[A]n estimated $10 trillion in financial transfers and vast amounts of data pass through the seabed routes" on a daily basis.[41] The importance of the Internet to the economy has drawn the capital of some of the world's largest and most powerful companies. Though telecom carriers previously owned the majority of cables, their share of the system has decreased because of the entrance of Internet content providers, such as Facebook and Google, into the cable-laying business.[42]

Absent the undersea cable system, the public would experience slower Internet speeds.[43] Internet traffic routed through satellites is lower in quality, less reliable, less secure, and more expensive.[44] Consider that modern-day cables are engineered to the same "five-nines" standard as nuclear weapons and space shuttles—a standard which means they are reliable 99.999 percent of the time.[45] For all of its benefits, some aspects of the undersea cable system can raise the consternation of the public. Residents of a small town on the Oregon coast, for example, have decried Facebook's placement of a cable landing station ("CLS")

---

[37] *Id.*
[38] WORKING GROUP REPORT, *supra* note 9, at 2.
[39] *Id.* at 1.
[40] *See generally id.* at 2 (discussing how critical infrastructure is for both civilian and military purposes in the United States).
[41] Tim Johnson McClatchy, *Undersea Cables: Too Valuable to Leave Vulnerable?*, GOVTECH (Dec. 12, 2017), https://www.govtech.com/network/Undersea-Cables-Too-Valuable-to-Leave-Vulnerable.html [https://perma.cc/A3AU-7S4B].
[42] CCDCOE, *supra* note 5, at 1.
[43] WORKING GROUP REPORT, *supra* note 9, at 1.
[44] *Id.*
[45] SUNAK, *supra* note 10, at 15.

in the community.[46] Notwithstanding issues related to the land-based infrastructure of the undersea cable system, the public experiences tremendous benefits from the system.

III. Two Types of Threats Must be Addressed to Secure the Undersea Cable System

The physical characteristics of the undersea cables make them susceptible to intentional and unintentional disruption. Cables that connect continents or lands divided by open water rest on the ocean floor.[47] The average diameter of these cables is comparable to that of a garden hose.[48] The planned commercial lifespan of the cables is 25 years, though they often get used for longer periods of time.[49] Closer to the coast, the cables often have external steel wire rods for protection and, in some cases, are placed up to two meters beneath the surface.[50] CLS are also susceptible to natural and human-based threats, though threats to these sites will not be discussed here.

Most experts regard the breakage rate of undersea cables as "rare" given the scale of the system;[51] there are about 100 undersea cables breaks per year.[52] Though "rare," the frequency of breaks incentivizes cable owners as well as those reliant on cables to lay additional, seemingly redundant cables to increase the resiliency of the cable system.[53]

The high costs of repairs and difficult logistics of those repairs also incentivizes cable system owners to protect cables and lay extra ones. Timely repair of cables necessitates "ready and unfettered access for cable ships and equipment to the ocean surface, water column, and seabed around a submarine

---

[46] Nigel Jaquiss, *Mark Zuckerberg Is Despoiling a Tiny Coastal Village and Oregon's Natural Treasures. The State Invited Him.*, WILLAMETTE WEEK (Aug. 19, 2020), https://www.wweek.com/news/2020/08/19/mark-zuckerberg-is-despoiling-a-tiny-coastal-village-and-oregons-natural-treasures-the-state-invited-him/ [https://perma.cc/G57P-Y3KY].
[47] CCDCOE, *supra* note 5, at 1.
[48] *Id.*
[49] WORKING GROUP REPORT, *supra* note 9, at 1.
[50] *See id*.
[51] *Id*. (regarding the frequency of damage to submarine cables as "rare"); *See also* McClatchy, *supra* note 41 (estimating an average of 200 failures along cable routes per year along approximately 650,000 miles of active international commercial cables).
[52] CCDCOE, *supra* note 5, at 2.
[53] *See id*.; *see also* Hinck, *supra* note 7 (outlining the redundancy of the undersea cable network by pointing out that "[c]utting the United States off from the rest of the world would require severing a large number of cables: at least 18 in the North Atlantic alone . . .").

cable."[54] Obtaining such access requires extensive coordination and cooperation mechanisms, including, but not limited to, "cable spacing and crossing standards, cable awareness programs and outreach, coordinating with other users of marine and coastal areas, and marine special planning."[55] Cable ships need a lot of room in order to complete their repairs.[56] Objects such as "oil platforms, turbine towers, [and] submerged structures" all frustrate the timely repair of cables.[57]

FIGURE 3: "Diver Checking Underwater Protection of Cable"[58]

Unintentional events in waters shallower than 200 meters account for the majority of cable breaks.[59] Unintentional breaks include those caused by natural forces as well as some human-caused breaks.[60] Natural events, such as earthquakes along the Pacific Rim, regularly break undersea cables.[61] The

[54] WORKING GROUP REPORT, *supra* note 9, at 3.
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Driver Checking Underwater Protection of Cable* (photograph), *in* The Official CTBTO Photostream, FLICKR (Aug. 13, 2009), https://search.creati9vecommons.org/photos/b9d8b72a-3cb5-4405-a55c-b0c6a047ba17.
[59] CARTER ET AL., *supra* note 22, at 39.
[60] *Id.*
[61] *See, e.g.*, Winston Qiu, *Submarine Cables Cut by Taiwan Earthquake and Typhoon Morakot*, SUBMARINE CABLE NETWORKS (Mar. 19, 2011), https://www.submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006.

unintentional byproducts of human actions, such as commercial fishing activities including anchoring and fishing, are the most frequent cause of undersea cable breaks.[62] For example, in 2012, a ship off the coast of Mombasa accidentally dropped its anchor on the East African Marine System (TEAMS), a cable laid by the Government of Kenya to increase its connectivity to the rest of the Internet.[63] As a result, six African nations saw the normal flow of Internet traffic drop by 20 percent; the repair time was estimated to be three weeks, while costs were forecasted to reach $500 million.[64] This sort of damage and disruption, though, is not typical of the regular breaks that occur from unintentional breaks.[65]

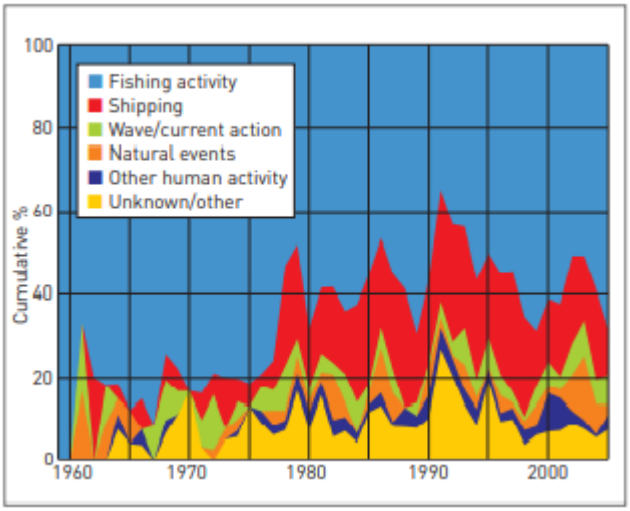

FIGURE 4: Types of cable breaks recorded between 1959 and 2000.[66]

Given that commercial activity causes the majority of cable breaks, any meaningful effort — be it legal or extralegal — to protect the undersea cable system must address these events. As the TEAMS example makes clear, the randomness of these commercially-induced breaks does not make for a straightforward policy response to reduce their frequency. The rarity of natural

[62] *See* CCDCOE, *supra* note 5, at 2.
[63] Curt Hopkins, *Ship's anchor cuts Internet access to six East African countries*, CHRISTIAN SCI. MONITOR (Feb. 29, 2012), https://www.csmonitor.com/World/Africa/2012/0229/Ship-s-anchor-cuts-Internet-access-to-six-East-African-countries.
[64] *See id*.
[65] WORKING GROUP REPORT, *supra* note 9, at 2; CCDCOE, *supra* note 5, at 2.
[66] Matthew P. Wood & Lionel Carter, *Whale Entanglements with Submarine Telecommunication Cables*, 33 IEEE J. OCEANIC ENG'G 445, 446, fig.1 (2008).

events causing breaks means that these events ought not to significantly influence policy decisions.[67]

A policy designed to ensure the integrity of the undersea cable system should also consider the threats posed by undersea cable system attackers. These actors have clear ample reason to target the undersea cable system as a means to injure an adversary. By way of example, an adversary who intentionally broke specific cables along the United States coast could "cause a significant network disruption that could hamper a United States military response in the opening hours of a major war," at least according to a former deputy director of the National Security Agency.[68] It appears as though nations such as Russia are increasingly investing in the resources necessary to cause such breaks.[69]

Non-state actors may also intentionally interfere with undersea cables for non-political reasons. The Vietnamese military responded to one such incident when local officials permitted fishermen in town to harvest copper from old cables off the Vietnam coast.[70] When doing so, the fishermen attempted to take resources from newer cables as well.[71] The resulting damage to the undersea cable system caused 82 percent of the Internet traffic to drop in the short run and, in the long run, cost US $5.8 million to restore to normal service.[72] Whatever motive instigates the intentional breaking of a cable, these deliberate and geographically-specific attacks can significantly disrupt Internet service.

Intentional threats, then, have the potential to be more disruptive than the more-frequent unintentional, commercial threats. That is precisely why policies focused on ensuring the integrity of the system should prioritize responding to intentional attacks and unintentional, commercial threats—the former is more disruptive, and the latter is more common.

---

[67] Not only are unintentional, natural events causing breaks infrequent, they are also more predictable. For instance, a nation may identify that a typhoon is coming and, to the extent possible, ready its private and government cable repair ships. Intentional breaks are likewise infrequent, but their unpredictability renders them a greater threat to the integrity of the undersea cable system because no such advanced preparation can take place.

[68] Hinck, *supra* note 7.

[69] *Id.*

[70] Mick P. Green & Douglass R. Burnett, *Security of International Submarine Cable Infrastructure: Time to Rethink?*, *in* LEGAL CHALLENGES IN MARITIME SECURITY 557, 561–62 (Myron H. Nordquist et al. eds., 2008).

[71] *Id.* at 562.

[72] MICHAEL SECHRIST, CYBERSPACE IN DEEP WATER: PROTECTING UNDERSEA COMMUNICATION CABLES BY CREATING AN INTERNATIONAL PUBLIC-PRIVATE PARTNERSHIP, BELFER CTR. 123 (Mar. 23, 2010), https://www.belfercenter.org/sites/default/files/legacy/files/PAE_final_draft_-_043010.pdf.

IV. Current Legal and Extralegal Frameworks do not Sufficiently Address the Threats to the Undersea Cable System

The international and national laws pertaining to the undersea cable system are outdated and insufficient.[73] Industry standards meant to coordinate the actions of the private cable owners also fall short.[74] These insufficiencies are not because of a lack of awareness surrounding the importance of the undersea cable system. Going as far back as 1884, undersea cables have received special protection under international laws.[75] Since then, international law pertaining to the cables has not substantially progressed. Some nations have opted to fill in the blanks left by the international regime; these efforts, though, have limited efficacy so long as the international regime fails to empower nations to take proactive acts to protect their cables, especially in international waters. This paper will not perform a full exploration of these laws, customs, and standards. Instead, this part will focus on the law as it is understood and applied today, particularly from the perspective of the United States.

Which laws, customs, and standards apply to the undersea cable system depends on the distance of the cable from the relevant coastal state.[76] Intuitively, as the distance from the coastal state increases, the legal rights of that coastal state diminish.

The first legal zone, the one most proximate to the coastal state, is the territorial sea.[77] According to the United Nations Convention on the Law of the Sea (UNCLOS), "[t]he sovereignty of a coastal State extends . . . to an adjacent belt of sea," known as the territorial sea.[78] Every State has the right to exercise such sovereignty in the seas within 12 nautical miles of their coast.[79]

---

[73] *See* UNCLOS DEBATE, *U.S. underseas cable industry needs UNCLOS protection*, https://www.unclosdebate.org/argument/708/us-underseas-cable-industry-needs-unclos-protection (last visited Sept. 15, 2021).
[74] WORKING GROUP REPORT, *supra* note 9, at 45–46.
[75] Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884 [hereinafter "1884 Convention"]; CCDCOE, *supra* note 5, at 4 (outlining some provisions of the Convention for the Protection of Submarine Telegraph Cables).
[76] *See generally* United Nations Convention on the Law of the Sea art. 2, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter "UNCLOS"] (establishing a legal framework for all marine and maritime activities).
[77] *Id.* at art. 2, ¶ 2.
[78] *Id.*
[79] *Id.* at art. 3, ¶ 1 (noting that the precise boundaries of the territorial sea depend on how the coastline is defined, the determination of which is specified in detail in the Convention).

The next legal zone is the EEZ, which may not extend further than 200 nautical miles from the coastal State.[80] In this zone, "all States enjoy the freedom of laying submarine cables . . . and other internationally lawful use of the seas related to this freedom, such as the operation of submarine cables," writes Kingsley Ekwere, Senior Lecturer at the University of Port Harcourt, Nigeria.[81]

The next legal zone is the continental shelf, which typically is up to a distance of 200 nautical miles from the relevant coastal State.[82] In this zone, all States may lay submarine cables.[83] Furthermore, no coastal State may interfere with the laying and maintenance of such cables in this zone.[84] To reinforce the importance of allowing all States to lay and repair cables in this zone, UNCLOS mandates that States have "due regard to cables . . . already in position."[85] Additionally, the "possibilities of repairing existing cables . . . shall not be prejudiced."[86]

On the high seas, the next zone, consideration of coastal State jurisdiction comes to an end because "[t]he high seas are open to all States," per Article 87 of the UNCLOS.[87] In this zone, coastal and land-locked States have the freedom to lay submarine cables.[88]

a. UNCLOS Fails to Mitigate Threats to the United States' Cables Because of Omissions in the Text of the Treaty and the Fact that United States is not a Formal Party to the Treaty

Even if the United States were a party to UNCLOS, the treaty would fall short of addressing the intentional and unintentional commercial activities most likely to cause significant disruption to the Internet. Firstly, UNCLOS sets too high of a threshold for what sort of activity can be punished. UNCLOS also does not empower States to take proactive action; the treaty's ambiguities and omissions leave some States wondering if their policy responses are permissible under international law.[89] Secondly, it is important to stress that because the majority of breaks take place within waters shallower than 200 meters, an

[80] *Id*. at art. 57.
[81] *See* Ekwere, *supra* note 23, at 165 (2016) (referring to art. 58, ¶ 1 of UNCLOS).
[82] UNCLOS, *supra* note 76, at art. 76, ¶ 1.
[83] *Id.* at art. 79, ¶ 1.
[84] *Id.* at art. 79, ¶ 2.
[85] *Id.* at art. 79, ¶ 5.
[86] *See id*.
[87] *See id.* at art. 87(1).
[88] *See id.* at art. 87(1)(c).
[89] *See id.* at art. 112–15.

international regime focused on deeper waters will have only limited efficacy with respect to protecting the undersea cable system.[90]

UNCLOS specifically addresses injuries, intentional or not, to submarine cables in Articles 113, 114, and 115.[91] The former, as interpreted by the CCDCOE, "implies that the breaking or injury of a cable need only be punished under domestic law if it is 'liable to interrupt or obstruct . . . communications.'"[92] This condition on interruption or obstruction means that attempted cable-breaking may not be punishable under Article 113. The Article has also been interpreted as allowing espionage based on the requirement for disruption to communication;[93] this interpretation could facilitate more intentional cable attacks. The Article also fails to specify that warships have the right to board vessels in international waters suspected of attempting to intentionally damage undersea cables; the result is that naval powers struggle to deter vessels from conducting attacks on cables.[94]

Article 114 specifies that States shall adopt laws to ensure that persons who "cause a break in or injury to another cable . . . bear the cost of the repairs."[95] Article 115 provides that States shall create laws to ensure that owners of ships who sacrifice an anchor, net, or other form of fishing to save a submarine cable are indemnified by the owner of the cable, so long as "the owner of the ship has taken all reasonable precautionary measures beforehand."[96] Note, however, that the indemnity does not include lost profits or catch.[97] This omission discourages fishermen from sacrificing their equipment, especially if they think that the cable break will not be attributed to them; they would rather increase the odds of keeping their catch, then face the certain losses associated with giving up equipment and more. This omission fails to adequately deter unintentional, commercial breaks. Furthermore, Articles 114 and 115 are contingent on States passing domestic legislation regarding the activities in question;[98] this presents another barrier to their enforcement.

---

[90] Wood & Carter, *supra* note 66, at 448.
[91] UNCLOS, *supra* note 76, at art. 113–15.
[92] *See* CCDCOE, *supra* note 5, at 3 (quoting Article 113, UNCLOS).
[93] *See id*. at 4 (tapping an undersea cable would not stop Internet traffic, but merely allow an unintended third party to review that traffic as well).
[94] SUNAK, *supra* note 10, at 17.
[95] UNCLOS, *supra* note 76, at art. 114.
[96] *Id*. at art. 114–15.
[97] *See* DOUGLAS R. BURNETT & LIONEL CARTER, INTERNATIONAL SUBMARINE CABLES AND BIODIVERSITY OF AREAS BEYOND NATIONAL JURISDICTION 22 (2017) (referring to cable protection zones as "generally comply[ing] with UNCLOS.").
[98] *See* UNCLOS, *supra* note 76, at art. 114–15.

The failure of UNCLOS to explicitly cover the extent to which its provisions pertain to non-state actors represents another gap in the treaty. Though UNCLOS refers to "States," a few scholars have read the term to encapsulate the private actors, such as those who control the vast majority of undersea cables.[99] Still, some scholars have interpreted UNCLOS as requiring national legislation for private actors to exercise the freedom to lay undersea cables.[100] Though international treaties generally do not apply to private parties, the exclusion of such parties is unacceptable in the context of an undersea cable system that is almost exclusively privately-owned.[101]

Other gaps in UNCLOS necessitate action by States to protect undersea cables. Robert Beckman, Director of the Center for International Law at the National University of Singapore, stated the protections afforded by UNCLOS to submarine cables in the high seas, in EEZs, and on continental shelves are "clearly inadequate."[102] The CCDCOE identified two such inadequacies. First, it is unclear if UNCLOS extends legal authority to States to create cable protection zones intended to safeguard the integrity of the undersea cable system.[103] This is problematic given that these zones are designed to prevent the unintentional, commercial breaks in relatively shallow water that account for such a high percentage of [104] Second, it is it is unclear if attempted damage to an undersea cable falls within the provisions of UNCLOS.[105] Note, however, that some stakeholders regard the prohibition against the infliction of damage to cables as a matter of customary law.[106] Third, UNCLOS fails to cover "the intentional theft of submarine cables in maritime zones outside of sovereignty."[107] That's why

---

[99] 3 MYRON NORDQUIST ET AL., UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY, 264 (Martinus Nijhoff et al. eds., 1995).
[100] *See* RAINER LAGONI, LEGAL ASPECTS OF SUBMARINE HIGH VOLTAGE DIRECT CURRENT (HVDC) CABLES 12–13 (1998).
[101] *See* ICPC, *supra* note 14.
[102] ROBERT BECKMAN, SUBMARINE CABLES–A CRITICALLY IMPORTANT BUT NEGLECTED AREA OF THE LAW OF THE SEA 13 (2010), https://cil.nus.edu.sg/wp-content/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables-rev-8-Jan-10.pdf.
[103] *See* CCDCOE, *supra* note 5, at 5; *see also* BECKMAN, *supra* note 102, (citing Article 21(1)(c) of UNCLOS and noting that "UNCLOS gives coastal States the power to impose restrictions on the right of innocent passage in order to protect submarine cables."); BURNETT & CARTER, *supra* note 97, at 21 (referring to cable protection zones as "generally comply[ing] with UNCLOS.").
[104] ICPC, *supra* note 14; *infra* Section V.
[105] *See* CCDCOE, *supra* note 5, at 3.
[106] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 252–53 (Michael N. Schmitt ed., 2017) [hereinafter "TALLINN MANUAL 2.0"].
[107] *See* BECKMAN, *supra* note 102, at 15.

Beckman calls on States to take it upon themselves to fill in the blanks left by UNCLOS;[108] some of his suggestions will be discussed in Sections V and VII.

The textual and scholarly analysis of UNCLOS reveals that it does not adequately address the two key threats identified in Section III. If UNCLOS definitively permitted cable protection zones, especially beyond sovereign seas, then States would have greater authority to reduce problematic commercial activity in more territory. The monitoring associated with enforcing cable protection zones, covered in more detail below, would likely also deter actors aiming to intentionally damage cables. These attackers would similarly be deterred by UNCLOS penalizing attempted damage of cables and by UNCLOS applying universal jurisdiction over breaking or attempting to break cables. However, universal jurisdiction to enforce those proposed provisions is unlikely because of the arduous process required to amend UNCLOS; any amendment to UNCLOS has to be ratified or acceded to by at least 60 State parties.[109] Even when that threshold is met, the amendment only enters into force for those who accept the amendment.[110] Shortfalls notwithstanding, UNCLOS marks an improvement on the prior reliance on customary law to protect the undersea cable system.

UNCLOS, amended or not, can only have a marginal effect on protecting the undersea cable system from the perspective of the United States. The nation has not ratified UNCLOS.[111] Consequently, scholars such as James Kraska of the U.S. Naval War College argue that the United States is missing out on an opportunity to have a more stable legal framework when acting in the continental shelf and beyond.[112] After all, UNCLOS and related conventions were developed in direct response to the uncertainties associated with customary law—"practices considered legally required by most nations," as defined by David B. Sandalow in a policy brief for the Brookings Institution[113]—to govern the oceans. Despite the United States Senate opting not to sign UNCLOS, President Reagan issued an Ocean Policy Statement indicating the nation's intent to generally follow the Convention.[114] Sandalow notes that President Reagan's intentions, as good as they

---

[108] *See id*. at 13.
[109] *See* UNCLOS, *supra* note 76, at art. 313(1).
[110] *See id*.
[111] *See* William Gallo, *Why Hasn't the US Signed the Law of the Sea Treaty?*, VOICE OF AM. (June 6, 2016, 7:00 PM), https://www.voanews.com/a/united-states-sign-law-sea-treaty/3364342.html [https://perma.cc/72NN-A8JT].
[112] *See id.*
[113] *Id.*
[114] *Id*.

may have been, still do not afford the United States all of the benefits made available to nations that have formally ratified UNCLOS.[115]

b. Other Sources of International Law and Norms Offer Only Limited Protection to the United States' Cable System Due to Being Outdated or Non-binding

Because the United States is not a party to UNCLOS, it may cite prior international agreements when seeking to protect the undersea cable system.[116] For instance, the United States may still invoke the Convention for the Protection of Submarine Telegraph Cables (1884 Convention).[117] The United States, as interpreted by the Working Group, regards the provisions of the 1884 Convention as customary law guaranteeing to all states "unique freedoms to lay, maintain, and repair submarine cables."[118] The 1884 Convention, though, provides comparatively fewer protections than UNCLOS; "[t]he [1884 C]onvention," as stated by the CCDCOE, "only focuses on undersea cables located in the high seas."[119] The 1884 Convention does make it a punishable crime "to break or injure a submarine cable, willfully or by culpable negligence, in such a manner as might interrupt or obstruct telegraphic communication."[120] However, the effect of this provision is limited because the 1884 Convention does not apply to situations of armed conflict; thus making it less responsive to threats posed by actors seeking to intentionally damage cables.[121]

This review of international law, as it pertains to the United States, reveals that the nation can only marginally rely on those conventions to combat threats to the undersea cable system. Ultimately the United States has a limited range of legal options from international law to reduce the occurrence of unintentional, commercial threats to the system and to stem the likelihood of actors intentionally attacking the system.

The Tallinn Manual 2.0 represents another international agreement that shapes norms pertaining to the undersea cable system. Developed by the Cooperative Cyber Defense Center of Excellence (CCDCE) within the North

---

[115] *See id.*
[116] CCDCOE, *supra* note 5, at 4 (noting that UNCLOS supersedes many aspects of the Submarine Cables Convention, but pointing out that "[s]tates not party to UNCLOS could, however, continue to invoke the Submarine Cable Convention").
[117] *See id.*
[118] WORKING GROUP REPORT, *supra* note 9, at 8.
[119] CCDCOE, *supra* note 5, at 4.
[120] 1884 Convention, *supra* note 75, at art. 2.
[121] *Id.* at art. 15.

Atlantic Treaty Organization (NATO), the Manual sets forth that customary international law prohibits the infliction of damage to an undersea cable; however, this prohibition would not apply in an armed conflict.[122] According to Garrett Hinck, the writers of the Tallinn Manual 2.0 have specified that States have the right to create cable protection zones within their territorial seas, but beyond that "there is no equivalent clear norm with respect to either the EEZ or continental shelf, and certainly not for the high seas."[123]

Notwithstanding the guidance the Tallinn Manual 2.0 provides, it has limited legal value. The Manual is not binding, but rather it "must be understood only as an expression of the opinions of the two International Groups of experts as to the state of the law," as expressed in the document's introduction.[124] Members of NATO are not bound by the Manual; the Manual does not even reflect NATO's official policies.[125] Instead, the Manual is thought of as a restatement of international laws related to cyberspace, informed by a broad range of international law scholars.[126]

In sum, the Manual does not formally bolster the means by which the United States can reduce unintentional, commercial activity and combat actors intentionally targeting cables.

c. Private Actors Have Proactively Tried to Respond to the Threats to the Undersea Cable System but Lack the Authority and Capacity to Fully Mitigate the Threats

Industry norms help fill some of the holes left by international agreements—especially in the context of unintentional, commercial activity. The ICPC, for instance, has offered several recommendations to reduce the vulnerability of the system. Sample recommendations include specifying the proper distance between cables, outlining the criteria for crossing cables and pipelines, and standards for repairing and installing cables.[127] Several countries have opted to make ICPC standards a formal part of their undersea cable governance. China and the United Kingdom, by way of example, have followed

---

[122] TALLINN MANUAL 2.0, *supra* note 106, at 252–53, 256.
[123] Hinck, *supra* note 7 (citing TALLINN MANUAL 2.0, *supra* note 107, at 256).
[124] TALLINN MANUAL 2.0, *supra* note 106, at 2–3.
[125] *See id.*
[126] Eric T. Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 738, 740 (2017) (citing TALLINN MANUAL 2.0).
[127] WORKING GROUP REPORT, *supra* note 9, at 8–9 (citing ICPC Recommendations 2 No. 10, 3 No. 10, 4 No. 8, 6 No. 8A).

ICPC standards and identified specific minimum separation distances to protect submarine cables.[128]

The North American Submarine Cable Association (NASCA) has also taken steps to support the undersea cable system. NASCA runs cable awareness programs that share the route position list data with commercial fishermen and government agencies; this list has the location information of undersea cables as a way to reduce anchoring- and fishing-related risks to the undersea cable system.[129] Representatives of NASCA further contribute to the security of the undersea cable system through presentations on policy ideas related to increased protection.[130]

Regional committees (such as NASCA) have stepped in to fill regulatory and legal gaps. These committees formed in the late 1990s and early 2000s in response to a "boom" in the undersea cable industry, as labeled by Robert Wargo, who served as President of NASCA.[131] Committees generally formed on a regional and as-needed basis; for instance, the Oceania Submarine Cable Association formed in 2010 and disbanded in 2011.[132] Committee memberships have typically included power and telecommunications cable owners, operators and suppliers; some also featured regulators and government officials.[133] As a result of insufficient government regulations, the committees formed, in part, "to ensure that no cable owner agreed to permit conditions that were technically infeasible and would then need to be agreed to by all others seeking approval at the same time."[134] Wargo noted that the committees also filled a gap left by ICPC in resolving local or domestic problems.[135] The United States is not a formal member of NASCA nor of any specific regional committee;[136] therefore, these outlets do not currently present an opportunity for a centralized response to the main threats to the undersea cable system in the United States.

Not all industry collaboration has necessarily advanced the integrity of the undersea cable system. Case in point, NASCA did not support efforts by the

---

[128] *Id.* at 10.
[129] *Id*. at 9.
[130] Robert Wargo, *The Role of Regional Cable Protection Committees in the Protection of Submarine Cables*, YUMPU, https://www.yumpu.com/en/document/read/18880804/undersea-cables-in-the-south-china-sea-centre-for-international (last visited Oct. 17, 2021).
[131] *Id.* at 1, 4.
[132] *Id.* at 2, 4, 6.
[133] *Id.* at 2.
[134] *Id.* at 4.
[135] *Id*.
[136] *Id.* at 2–3, 5.

Canadian government to group underseas cables and pipelines, even identifying the efforts as inconsistent with Canadian law and historical practices.[137] NASCA representatives have also exploited jurisdictional differences in regulations among states in the United States to pass "cable friendly" provisions.[138]

V. The United States Should Learn from the Undersea Cable Laws of Other Nations to Better Protect its own Portion of the System

Because of the inadequacies of UNCLOS, in particular, and the international legal and regulatory environment, in general, there is a need for affirmative action by the United States to protect the undersea cable system. Notably, the United States is not alone; according to Beekman "the laws and regulations of most states on the protection of submarine cables are inadequate."[139] A few states, however, have taken meaningful action against the two main threats. Laws and regulations adopted by Australia, New Zealand, and Sweden offer templates for the United States to consider.[140]

Due to the substantial number of cables along the US and the nation's complicated federal system, there is no peer country to study with respect to undersea cable policy. For instance, the policy lessons learned from New Zealand are of limited value because the country has fewer cables than the United States;[141] similarly, China's approach to undersea cable protection is of limited value to the United States because of the centralized structure of China's government and its more uniform approach to coastal and ocean law.[142] Consequently, the United States will have to glean only the most applicable lessons from other countries addressing the threats to the undersea cable system.

Australia and New Zealand created cable protection zones that prohibit certain activities from occurring around undersea cables. Australia created the first such zones in 2007.[143] In consultation with industry stakeholders, Australian authorities created zones near Sydney which prohibit activities of the highest risk

---

[137] *Id.* at 5.
[138] *Id.*
[139] BECKMAN, *supra* note 102, at 13.
[140] WORKING GROUP REPORT, *supra* note 9, at 10.
[141] *Id.* at 56.
[142] *See, e.g.*, Eli Huang, *China's cable strategy: exploring undersea cable dominance*, AUSTL. STRATEGIC POL'Y INST. (Dec. 4, 2017), https://www.aspistrategist.org.au/chinas-cable-strategy-exploring-global-undersea-dominance/ [https://perma.cc/RT3H-ZZ5Y].
[143] Australian Communications and Media Authority, *Protection Zones Declared for Submarine Telecommunications Cables off NSW Coast*, ACMASPHERE, Aug. 2007, at 8–9 [hereinafter ACMA]; s*ee also* Submarine Cables and Pipelines Protection Act 1996 (N.Z.).

to cables such as "sea-bottom trawl fishing, anchoring, sand-dredging and dumping."[144] Zones may only be created around cables that are of national significance.[145] In the case of the first zones, each contained "nationally significant high-capacity cables linking Australia to global communications systems," as described by the Australian Communications and Media Authority (ACMA).[146] Another zone off the coast of Perth has since been identified.[147]

Cable protection zones, however, do not guarantee that human activity will never disrupt or break a cable. Some limits to the efficacy of cable protection zones are inherent to the policy. The creation of cable zones increases awareness of cable location and, accordingly, allows attackers to more easily target the systems. Cable zones also increase the odds of unintentional breaks caused by placing more cables in a narrower geographic area.[148]

Cable corridors, which create protection zones for cables to be laid, rather than zones around pre-existing cables, suffer from a similar problem as that of protection zones. Another factor mitigating the effectiveness of cable protection zones and corridors is implementation. A lack of proactive monitoring and deterrence by legal authorities around the zones or corridors may render the intended protection moot. This lack of deterrence may have been worsened by the comments of the Australian Federal Police (AFP), explicitly stating that they did not have a responsibility to monitor, nor supervise, the safekeeping of the cable protection zones, and that they lacked the resources to do so.[149]

New Zealand has modeled and improved upon the Australian approach to cable protection zones. In contrast to Australia's three zones, New Zealand has created ten.[150] Unlike Australia, New Zealand has taken a proactive approach to

---

[144] ACMA, *supra* at 8–9; *see also Telecommunications Act 1997* (Cth) (Austl.).
[145] ACMA, *supra* note 144, at 8; *Telecommunications Act 1997* (Cth) (Austl.).
[146] ACMA, *supra* note 144, at 8.
[147] *See* APEC COMM. ON TRADE AND INVESTMENT, REPORT OF THE TRADE POLICY DIALOGUE ON THE TRADE BENEFITS FROM SUBMARINE CABLE PROTECTION 10 (2012), https://www.apec.org/-/media/APEC/Publications/2012/4/Report-of-the-Trade-Policy-Dialogue-on-the-Trade-Benefits-from-Submarine-Cable-Protection/2012_CTI_Trade-Policy_Dialogue_Submarine_Cables.pdf.
[148] *See, e.g.*, Jessica Woodall, *Australia's Vulnerable Submarine Cables*, AUSTL. STRATEGIC POL'Y INST. (May 31, 2013), https://www.aspistrategist.org.au/australias-vulnerable-submarinecables/.
[149] *See* AUSTRALIA COMM. AND MEDIA AUTHORITY, REPORT ON THE OPERATION OF THE SUBMARINE CABLE PROTECTION REGIME 15 (2010), https://apo.org.au/sites/default/files/resource-files/2010-09/apo-nid23392.pdf.
[150] *See Safety Update*, MARITIME N. Z. (Aug. 1996), https://www.maritimenz.govt.nz/commercial/safety/safety-updates/navigation-stability/cables-pipelines.asp (listing locations of ten New Zealand cable protection zones).

enforcing prohibitions related to the zones.[151] A report by the Australian Strategic Policy Institute commended the impressive enforcement regime employed by their neighbors: "Protection officers and Maritime Police [in New Zealand] not only patrol their zones with ships and helicopters, in some cases they operate for up to 24 hours a day."[152]

FIGURE 5: Map of a cable protection zone in New Zealand.[153]

Though these two nations have experienced success with their zones, zones and corridors are "not generally implemented [by countries around the world]," despite the fact that "they could reduce unintended cable damage."[154] Where zones have been instituted and effectively enforced, instances of cable breaks have decreased to near zero.[155] Given the success of these zones, it makes sense that the two oceanic nations are not alone in having adopted cable protection zones; other countries with zones include Denmark, Uruguay, and Colombia.[156]

---

[151] *See, e.g.*, Submarine Cables and Pipelines Protection Act 1996, pt. 3 (N.Z.) (approving of government purchases of additional maritime surveillance equipment to assist with enforcement of the act).
[152] Woodall, *supra* note 148.
[153] CARTER ET AL., *supra* note 22, at 37 (exhibiting cable protection zone map from Telecom New Zealand in Figure 5.7).
[154] CCDCOE, *supra* note 5, at 3.
[155] BURNETT & CARTER, *supra* note 97, at 21.
[156] *Id*. at 14.

Another approach to reduce the likelihood of cable damage is to increase the penalties for any such violation. Australia and New Zealand have modeled this approach by imposing stiff penalties for violating their cable protection zones, and for causing damage to an undersea cable. In Australia, for example, a person who "engages in conduct . . . that results in damage to a submarine cable [that is in a cable protection zone]" may be imprisoned for ten years.[157] Sweden has also imposed a legal structure likely to deter damage where owners of a cable that cause damages to another cable must cover the repair costs.[158] New Zealand has also imposed penalties with similar potential to deter damage.[159] And as Article 113 of UNCLOS provides criminal sanctions for those who willfully or with culpable negligence injure undersea cables, China has also adopted cable protection legislation. In contrast, however, this legislation has done little, if anything, to deter injurious behavior.[160] Both China's struggles with reducing breaks and the inadequacies of Australia's enforcement regime related to its cable protection zones suggest that effective enforcement is a necessary condition to protecting the undersea cable system.

Other less punitive policies to reduce the likelihood of damage to undersea cables include information-sharing regimes. For instance, Australia and New Zealand have tasked their governments with providing cable route information and coordinating with the fishing and maritime industries.[161] National security strategists, such as the Director of National Strategic Studies in the United States, have acknowledged the importance of information sharing.[162] In other maritime contexts, national security entities have set up an "unclassified, multinational, freely shared" automatic identification system to track merchant ships. A similar system for undersea cables would help reduce cable disruptions.[163]

---

[157] *Telecommunications Act 1997* (Cth) (Austl.).
[158] ACT ON THE OBLIGATION TO PAY COMPENSATION FOR DAMAGE TO SUBMARINE CABLES AND PIPELINES (Svensk författningssamling [SFS] 1996:518) (Swed.).
[159] WORKING GROUP REPORT, *supra* note 9, at 10.
[160] *See* BURNETT & CARTER, *supra* note 97, at 21, n.82 (reporting that "China in the years 2008–2015 [had] an average number of about 26 cable faults per year, the highest of any state").
[161] *Telecommunications Act 1997* (Cth) sch 3A pt 2 div 2 sub-div A para 8 (Austl.) (stating that the "Location of submarine cable to be specified in declaration"); Submarine Cables and Pipelines Protection Act 1996, pt 2 s 12 (N.Z.) (allowing cable protections to apply "differently in respect of specified methods of fishing").
[162] MICHAEL MATIS, THE PROTECTION OF UNDERSEA CABLES: A GLOBAL SECURITY THREAT 3 (U.S. Army War College 2012) (describing the importance of information-sharing in underwater cable protection and acknowledging Stephen Krotow, Director of National Strategic Studies Department, as project advisor).
[163] *Id.* at 26.

On the whole, laws, regulations, and norms surrounding protection of undersea cables reflect difficult trade-offs between commercial fishing, navigation, and undersea cables. Scholars David R. Burnett and Lionel Carter recommend that any tinkering with this balance be taken on with "[g]reat care, careful thought, and evidence justifying the need and the risk of intended consequences [associated with any change]."[164] This recommendation, though, likely does not apply to nations in desperate need of modern legislation and regulation, including the United States, which Burnett and Carter criticize for its antiquated "telegraph era statutes based on the 1884 Cable Convention that are historical relics with little practical utility."[165]

VI. The United States Legal Framework and its Policy Responses to System Threats are Insufficient

With limited options through international law, and having failed to implement best practices gleaned from policies implemented elsewhere, there is a tremendous amount of room for improvement in the United States' legal and regulatory framework pertaining to undersea cables. The time to realize these improvements is now. Increasing development in the United States coastal and marine areas threatens the integrity of the undersea cable system.[166] These activities, if left unregulated, threaten the installation of cables, threaten to limit the speed of effective and efficient cable repairs, and threaten to detrimentally alter the course of cables by effectively requiring that they cluster together, thereby "magnifying[ing] the risks of damage and communications outages across multiple systems due to particular natural or man-made events."[167]

a. The Manifold Federal Agencies with Partial Authority Over Undersea Cables Hinder the Development of a Comprehensive Protection Regime

United States laws and regulations fall short in four main ways. U.S. laws and regulations have fallen short by way of, first, a lack of clarity regarding which agency or agencies should lead on undersea cable protections; second, insufficient penalties to deter behavior likely to result in broken undersea cables; third, insufficient coordination among federal, state, and local governments regarding specifying and enforcing standards and regulations; and, fourth, as briefly

[164] BURNETT & CARTER, *supra* note 97, at 23.
[165] *Id.* at 21.
[166] WORKING GROUP REPORT, *supra* note 9, at 5.
[167] *Id.*

discussed above, private actors, such as Big Tech companies, bearing too much responsibility for protecting the undersea cable system.

Though the United States Federal Government has recognized the importance of undersea cables, no agency has taken ownership over the protection of the system. Importantly, the government has labeled undersea cables as critical infrastructure.[168] This designation suggests that the government would formalize its institutional response to protecting the system, yet the Working Group determined that "no U.S. federal agency has transposed th[e] finding [of undersea cables as critical infrastructure] in practical terms to adopt or enforce cable-protection standards or policies."[169] Instead, as noted by the Office of the General Counsel within the National Oceanic and Atmospheric Administration (NOAA), "a number of U.S. agencies have authority to regulate the laying and maintenance of cable off of [the] nation's shores."[170] This observation is important in two respects: first, it acknowledges that many agencies have a role in undersea cable regulations and laws; and, second, it specifies the existence of authority of several agencies over the undersea cable system, but not an obligation on any one agency to lead on policy formulation and implementation.

An exhaustive review of the role of each United States federal agency with ties to the undersea cable system is beyond the scope of this paper. Still, even a partial overview reveals the fragmented approach taken by the United States government. NOAA has the authority "to regulate whether and how proposed submarine cables may be installed in National Marine Sanctuaries."[171] NOAA, as discussed below, also plays a role in administering the Coastal Zone Management Act ("CZMA").[172]

The United States Army Corps of Engineers also has authority over undersea cable laying—at least on the seabed of the outer continental shelf—via section 10 of the Rivers and Harbors Appropriations Act of 1899.[173] This authority often entails weighing the national security implications of laying a specific cable.[174] Another agency, the Federal Energy Regulatory Commission, also has authority over some undersea cables proposed to rest on the continental

---

[168] *Id.* at 11.
[169] *Id.*
[170] NOAA Office of General Counsel, *Submarine Cables—Domestic Regulation*, NOAA (July 8, 2019), https://www.gc.noaa.gov/gcil_submarine_cables_domestic.html.
[171] *Id.* (citing 16 U.S.C. § 1435(a) (2000)).
[172] *See infra* Section VI(c).
[173] NOAA, *supra* note 170 (referring to 33 U.S.C. § 403, as amended by the Outer Continental Shelf Lands Act of 1953 (OCSLA), 43 U.S.C. § 1333(e)).
[174] 33 C.F.R. § 320.2; 33 C.F.R. § 320.4(j)(2).

shelf.[175] The Department of the Interior may also play a role in shaping the nature of a proposed cable; at times, its specific grant of authority may overlap with that of the Army Corps of Engineers.[176]

The Federal Communications Commission ("FCC") plays a pivotal role in undersea cable policy and regulation. It has the authority to issue licenses for "any submarine cable directly or indirectly connecting the United States with any foreign country, or connecting one portion of the United States with any other portion thereof."[177] Approval of an undersea sea cable license application is contingent upon the applicant providing information related to ownership of the cable, certain reporting requirements, and conditions imposed on each cable landing license.[178]

Occasionally, agencies or their sub-units act in informal capacities to assist initiatives meant to protect the undersea cable system. For example, the Bureau of Ocean Energy Management ("BOEM") has partnered with the U.S. Coast Guard to enforce an informal agreement barring installing wind energy structures within one nautical mile of a traffic separation scheme.[179] Additionally, at times, the U.S. Coast Guard will create safety zones around energy exploration and exploitation facilities on the OCS of the United States.[180]

This brief overview of the agencies with some stake in the undersea cable system reveals a series of overlapping authority. Absent more clarity around which agency is responsible for protecting the undersea cable system, it is likely that the current approach will fail to protect the system in the event of significant disruptions—regardless of the intentionality of the responsible party. At the federal level alone, overlapping jurisdictions make it harder to implement cable protection zones and other related legal responses to the threats posed by unintentional, commercial activity and intentional attacks.

b. Insufficient Penalties for Breaking Cables Fail to Deter Unintentional Breaks

Underneath the morass of potential agency regulations rests the federal law prohibiting certain activities related to undersea cables. The main law on the

[175] 16 U.S.C. § 792–823(a).
[176] 33 U.S.C. § 403; 43 U.S.C. § 1333(e).
[177] 47 U.S.C. § 34.
[178] 47 C.F.R. § 1.767.
[179] WORKING GROUP REPORT, *supra* note 9, at 10.
[180] *Id*.

books serves as an inadequate deterrent to problematic behavior from commercial actors and state and non-state attackers. According to the Submarine Cable Act, enacted in 1888, "[a]ny person who shall willfully and wrongfully break or injure, or attempt to break or injure . . . a submarine cable in such a manner as to interrupt or embarrass, in whole or in part, telegraphic communication" shall be liable for as many as two years in prison and/or a fine of up to $5,000.[181] As reported by the Working Group Report, the penalties associated with causing damage to a submarine cable are "unlikely to deter negligent or willful damage and do not even cover the cost of the repair."[182] The United States has not updated its penalty amount for cable damage for more than 125 years.[183] It is unlikely that attackers even weigh prison time and fees when planning their acts; this is even more likely to be the case when law enforcement has few means and a diminished incentive to effectuate enforcement.[184]

There are other laws related to damage caused by commercial actors to undersea cables lack sufficient deterrent power. Federal law holds fishing vessels accountable by subjecting fishermen who fail to keep their equipment from interfering with or damaging submarine cables to punishment;[185] the law specifies a fine of up to $250 and a prison term for as many as ten days for fishing-related damage. The law also obligates fishing vessels to remain a minimum distance from vessels engaged in laying cables or buoys indicating the position of a cable.[186]

c. Federalism Undermines a Comprehensive Approach to Undersea Cable Protection Because States Often have Policy Priorities that Conflict with Protecting the System

Coastal states influence undersea cable protections and regulations. As a consequence of the Submerged Lands Act, each coastal state has authority over the three nautical miles of seabed off their coast.[187] Nevertheless, many states have yet to take substantial action to protect undersea cable systems. As detailed by the Working Group Report, "no U.S. federal, state, or local government agency has promulgated laws or regulations establishing default or minimum separation distances," referring to the minimum separation distance between an

[181] 47 U.S.C. § 21.
[182] WORKING GROUP REPORT, *supra* note 9, at 8.
[183] *See id*. at 10.
[184] Scott Coffen-Smout & Glen J. Herbert, *Submarine Cables: A Challenge for Ocean Management*, 24 MARINE POL'Y 441, 444 (2000).
[185] *See* WORKING GROUP REPORT, *supra* note 9, at 8.
[186] *Id*.
[187] 43 U.S.C. §1301.

existing undersea cable and any other marine activity in the absence of "any mutual agreement to allow the activity in closer proximity to the submarine cable."[188] These mandated distances could reduce the frequency of commercial activities leading to cable breaks; for instance, submarine cables that are a part of the Internet would have sufficient berth from cables that may be relaying power from offshore wind farms.

Administered by NOAA, the CZMA also creates a role for states to play in undersea cable policy.[189] Under the CZMA, the nation's coastal resources ought to be balanced between economic development and coastal conversation.[190] Determining that balance must be done in coordination with the states: "no federal agency may grant a license to conduct an activity affecting a coastal area until a state concurs or is presumed to concur with the applicant's certification that a proposed activity is consistent with the state's coastal management plan."[191] This means that individual states could disrupt efforts by the Federal Government that either stem commercial activity or foster it. States could act as individual protectors of cables by creating coastal management plans that require certain protections for cables.

The ability of states to shape undersea cable policy is not lost on industry actors. States have become targets of industry groups for regulatory capture. Former NASCA President Wargo made that clear in a presentation that highlighted NASCA working with various states to "get more 'cable friendly' regulation."[192] As a counterpoint, some states have been more proactive than others in developing and enforcing spatial planning schemes.[193] Still, a state-by-state effort to address the threats posed by commercial actors to the undersea cable system likely falls short of the sort of comprehensive policy solution necessitated by infrastructure of this importance.

Notwithstanding the power held by states to affect policies related to commercial actors, they lack the sort of coordination to respond to the threats posed by attackers. Federal actors are better suited to determine the nation's plan to reduce breaks caused by attackers—a plan that necessarily raises the sort of foreign policy questions usually left to the Federal government. At this point,

---

[188] WORKING GROUP REPORT, *supra* note 9, at 9.
[189] NOAA, *supra* note 170, at 2.
[190] *Id.*
[191] *Id.* (referencing 16 U.S.C. § 1456(c)(3)(A)).
[192] *See* Wargo, *supra* note 130, at 8.
[193] *See* WORKING GROUP REPORT, *supra* note 9, at 11 (pointing to the Mid-Atlantic Council on the Ocean and the Northeast Regional Ocean Council).

though, even the Navy has yet to adopt a formal plan for the protection of the undersea cable system.[194]

d. Private-Sector Stakeholders Have Succeeded in Creating Patchwork Protections of the Undersea Cable System, but these Protections are far from Comprehensive

Insignificant legal protections have thus far forced private stakeholders, such as Big Tech companies like Google, to take the protection of the undersea system into their own hands. Submarine cable operators, for example, have had a relatively high degree of success in mitigating damage to cables by burying and armoring cables, instituting cable awareness campaigns, and compensating fishermen for any gear snagged by the cables.[195] Cumulatively, these tactics can reduce threatening commercial activity.

In a similar fashion, regional committees of fishermen and submarine cable owners have often reached agreements around how to divvy up the seabed.[196] Thanks to these agreements, cables in many areas have been placed outside of highly fished areas, thereby decreasing the risk of commercial damage to cables.[197] For example, the Oregon commercial trawl fisherman collaborated with numerous other private companies to create "the Oregon Fisherman's Undersea Cable Committee Agreement," which represented the first effort by two private stakeholder groups to "discuss, describe, and delineate their shared use of a community resource—the ocean."[198] Nevertheless, these "self-help" mechanisms, as described by the Working Group Report, have proven to be "wholly inadequate" for ensuring the protection required for such an important piece of the nation's infrastructure.[199] Moreover, to an even greater extent than states, private actors are limited in their ability to respond to attackers because they generally lack the authority to respond to attacks by foreign and non-state actors.[200]

---

[194] Hinck, *supra* note 7, at 2.
[195] *See* WORKING GROUP REPORT, *supra* note 9, at 5.
[196] *See id*. at 11.
[197] *See id*.
[198] *About OFCC, Or. Fisherman's Cable Comm*., OR.'S FISHER CABLE COMM., http://www.ofcc.com/about_ofcc.htm (last visited Sept. 19, 2021).
[199] *See* WORKING GROUP REPORT, *supra* note 9, at 12.
[200] Momentum may be building to allow private actors to more proactively engage with foreign and non-state actors. For instance, Congress has considered amendments to the Computer Fraud and Abuse Act that would allow private companies to "hack back" foreign and non-state actors that infiltrate private computers. Shannon Vavra, *Congress to take another stab at 'hack back'*

United States federal agencies have helped private actors with some cable protection projects and initiatives, but only on a reactive basis; it follows that the agencies, according to the Working Group, place "the burden on the submarine cable operator[s] to justify a particular method of protection."[201] These ad hoc and private measures should be replaced by a set of laws and regulations that ensure the integrity of the undersea cable system in a comprehensive manner—addressing both attackers and commercial actors.

VII. The New United States Presidential Administration Should Adopt Short- and Long-Run Responses to the Threats to the Undersea Cable System

An initial, speedy review of this paper and topic at large could lead one to believe that the United States could significantly contribute to the integrity of the undersea cable system simply by ratifying UNCLOS and creating cable protection zones. Ratifying UNCLOS would improve the regulatory and legal framework of the United States related to the system by affording the nation standing in conversations about amending the Convention as well as providing the nation with more legal authority to take actions related to the breaking of undersea cables. Creating cable protection zones, in theory, would indicate that the United States was adopting a best practice that has shown great results in reducing undersea cable breaks in nations such as New Zealand, where several zones have been created and where enforcement is high.

a. Neither Ratifying UNCLOS nor Creating Cable Protection Zones Will Adequately Address the Threats to the Undersea Cable System in the United States

In practice, neither ratifying UNCLOS nor attempting to adopt cable protection zones would make much of a difference in the occurrence of cable breaks caused by unintentional, commercial activities, or intentional activities in the United States. Even if the United States ratified UNCLOS and adopted legislation to implement Articles 113, 114, and 115, the efficacy of that legislation hinges on effective monitoring; as is the case with cable protection zones.[202] The United States, in the context of effectively monitoring cable break

legislation, CYBERSCOOP (Jun. 13, 2019), https://www.cyberscoop.com/hack-back-bill-tom-graves-offensive-cybersecurity/ (noting that some cybersecurity experts regard the authorization of private actors to "hack back" as a dangerous idea).

[201] WORKING GROUP REPORT, *supra* note 9, at 10–11.

[202] *See* BURNETT & CARTER, *supra* note 97, at 21.

activities, is much more akin to China than New Zealand. In other words, like China, the United States has too many cables and insufficient resources to effectively monitor cable-breaking activity;[203] on the other hand, New Zealand has three cables, which the nation relies on for all of its international data traffic.[204, 205]

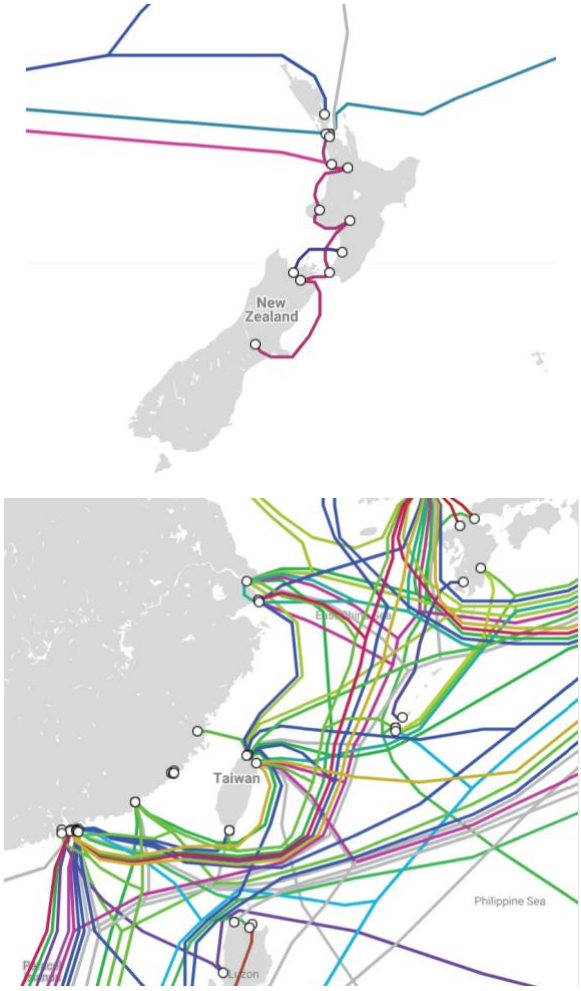

FIGURE 6: Undersea cables off of New Zealand (upper) and China (lower) as of January 24, 2021.[206]

[203] *See* WORKING GROUP REPORT, *supra* note 9, at 1.
[204] TELEGEOGRAPHY, *supra* note 1.
[205] SUNAK, *supra* note 10, at 18.
[206] TELEGEOGRAPHY, *supra* note 1.

The absence of effective enforcement via effective monitoring will render both UNCLOS-related legislation and cable protection zones insufficient to maintain and improve the integrity of the undersea cable system. What's more, unlike New Zealand, the United States holds a significant position in geopolitics. It follows that the United States must be far more attentive to the downside of openly sharing the location of its cables via cable protection zones; identifying the location of its cables could attract the attention of actors seeking to intentionally break cables. So, whether the cable protection zones were designed for pre-existing or future cables, the issue of actors seeking to cause intentional damage being notified of the location of the cables still proves problematic.

However, some of the shortfalls of cable protection zones could be remedied by scaling back the scope of the zones. For example, the British Parliamentarian Sunak has advocated for smaller zones around the most important cables and for targeting monitoring resources on these locations.[207] The United States may struggle to identify such narrow zones, given that the majority of cables are privately owned and the manifold cables lining the coast of the United States. What criteria would justify affording some cables greater protection than others? Some factors, such as the amount of Internet traffic carried on specific cables, may help identify the most important zones for protection. The process for creating a specific list of factors and outlining specific zones would likely be subject to costly and time-intensive litigation. The vulnerability of the undersea cable system to threats of unintentional, commercial, and intentional breaks requires a faster policy response.

Note also that this paper is not actively opposing the ratification of UNCLOS, but only suggests that doing so would have a limited impact on protecting the undersea cable system. The fact that U.S. states would still retain significant authority over the shallow waters prone to breaks caused by commercial activity reinforces the limited efficacy of UNCLOS.[208]

Finally, the politics of ratifying UNCLOS or adopting cable protection zones could impose a substantial barrier to realizing either goal. Though bipartisan support for ratifying UNCLOS has existed since at least the early 2000s,[209] oppositional political forces as well as political inertia have thwarted ratification. Similar political coalitions could likely mount a successful campaign

---

[207] SUNAK, *supra* note 10, at 18.
[208] *See* CARTER ET AL., *supra* note 22, at 44.
[209] *See, e.g.,* David D. Caron & Harry N. Scheiber, *The United States and the 1982 Law of the Sea Treaty*, AM. SOC'Y INT'L L. (June 11, 2007), https://www.asil.org/insights/volume/11/issue/16/united-states-and-1982-law-sea-treaty.

against cable protection zones as well. One such coalition member could be NASCA, which has already proven capable of pushing back against cable protections that did not meet its standards.[210]

b. Gathering and Sharing Information Related to Undersea Cable Threats Will Immediately Increase Deterrence by Making Attribution of Breaks Easier

Given the importance of the severity and likelihood of getting caught breaking a cable to reducing the frequency of breaks, the United States should review the remaining policy options through a lens that promises the greatest deterrent effect to actors likely to unintentionally or intentionally break cables. With that in mind, the United States should focus on three policy goals: information gathering, information sharing, and increasing penalties.

Regarding information gathering, the U.S. should institute a new requirement to include sensors on all undersea cables and should pursue international agreements and domestic regulations to monitor ship locations. Undersea cables are "located hundreds if not thousands of miles from anywhere or anything that can detect and monitor the presence of a hostile maritime actor," based on Sunak's research.[211] Consequently, Sunak recommends that nations mandate cable laying companies to "place relatively cheap sensors that detect sonar frequencies near key undersea infrastructure and along cable routes. If the sensors were tripped, they could alert nearby coast guard or navy assets."[212]

In the context of the United States, the FCC could realize this information gathering strategy by mandating that cable operators include their use of sensors in any license for an undersea cable. This small step would turn the agency's licensing process into an effective tool for improving the nation's response to the primary dual threats to the system; of course, there would need to be follow up efforts to ensure that license recipients installed the sensors when laying their cables. Private owners of these cables would likely comply with this sensor requirement if they knew that the resulting information would help them recover any costs associated with repairing a break in their cable.

---

[210] *See* Wargo, *supra* note 130, at 9.
[211] SUNAK, *supra* note 10, at 23.
[212] *Id.* at 35 (citing Robert Martinage, *The Vulnerability of the Commons*, FOREIGN AFFAIRS, January/February 2015); *see generally Telecommunications Act 1997* (Cth) (Austl.); Submarine Cables and Pipelines Protection Act 1996 (N.Z.).

In the event that the United States is unable to rally an international coalition to create an information gathering system or pass similar domestic legislation, the private sector may be able to adopt its own standards to achieve the same effect. The ICPC, for instance, could mandate that its members include sensors on their cables as a condition of their membership. Of course, the ICPC may seek federal funds to help cover the costs of such a requirement; asking Congress for money would likely be easier than asking the gridlocked body to pass meaningful legislation. This approach would benefit from being easier and faster to implement. However, an international treaty or domestic law would likely be easier for the state and federal authorities to enforce, which, as discussed in Section V, is imperative to an effective regime. With the protection of the undersea cable at stake, both short- and long-term solutions ought to be pursued.

However, the sensors are implemented, to ensure a high likelihood of identifying the person or entity responsible for a break observed by a cable's sensors, it is essential to locate the ship nearest to the cable at the time of the break. Australia and New Zealand offer a policy response that, if expanded, could supply that information. In those countries, ships within cable protection zones are required to broadcast their locations to the relevant Coast Guard.[213] This obligation ensures that the Coast Guard can effectively track when ships near and cross cables. The United States should expand this requirement to all boats within its territorial seas, EEZ, and continental shelf—doing so would not interfere with the rights or freedoms of any State to sail in such waters.[214]

On the high seas, the United States should reach agreements with other nations to delineate specific monitoring responsibilities; given that the vast majority of breaks occur within territorial seas and EEZs, it is most important that the United States work with other nations to observe their respective waters.[215]

With this sort of international monitoring, it would be possible to cross reference any break triggered by the cable sensors against the location database. The geographic and data-keeping responsibilities of nations in this monitoring arrangement could be specified in future trade agreements or through international bodies such as NATO or the UN.

---

[213] SUNAK, *supra* note 10, at 18.

[214] *See* BURNETT & CARTER, *supra* note 97, at 71 (indicating that of the four average annual repairs that took place in U.S. waters from 2008 to 2015 three were in the EEZ, and one was in the territorial waters).

[215] *See id*. (indicating that the average number of repairs per year, from 2008 to 2015, in the high seas was just 5; comparatively, China averaged 26 within its territorial waters and EEZ).

The exchange of sensitive information between private and public stakeholders will not be realized without an information sharing regime in place. By way of example, Congress passed the Cybersecurity Information Sharing Act to create a legal safe harbor for companies subjected to cyberattacks to exchange information with government stakeholders.[216] A similar piece of legislation could provide companies that share information related to their undersea cables with certain benefits, so as to increase the odds of them installing the sensors discussed above and sharing trigger events with the government in a timely fashion. For example, the legislation could make the provision of repair costs to the private owner of the cable from the party responsible for the break contingent upon the cable company being a part of the information sharing agreement.

This agreement would also provide the government with assurances that the private companies would not divulge government information collected via national security systems, such as information collected through the Integrated Undersea Surveillance System (IUSS). The IUSS is the Navy's "array of fixed and mobile acoustic arrays that provide its primary means for detecting submarines."[217] By placing the location of submarines and ships into a database with sensor-gathered information related to cables, the odds of identifying the culprit for any cable break would drastically increase. This extensive cooperation would make even the most sophisticated attacker think twice before intentionally breaking a cable and would give pause to commercial actors every time they considered dropping anchor. This legislative solution, though, would take time. It follows that congressional hearings on this topic should commence sooner rather than later.

With information gathering and sharing addressing the likelihood of being caught, increasing the fines associated with breaking a cable is the last remaining aspect of the deterrence equation. The United States must update the penalties associated with intentionally damaging, attempting to damage, and negligently damaging undersea cables. Consider that breaching undersea cable laws and regulations in New Zealand or Australia carries fines of more than US $68,410 and US $342,004, respectively.[218] Comparatively, the corresponding fine in the United States is just $5,000.[219] Although this increase will likely only add to the

---

[216] *See* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. F. CORP. GOVERNANCE (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/#1.
[217] Hinck, *supra* note 7.
[218] *See* SUNAK, *supra* note 10, at 18.
[219] 47 U.S.C. § 21.

deterrence of commercial actors, those actors are still the most likely to cause a break. So, the increase is likely to be a meaningful policy intervention.

This base level fine should be increased and tiered based on several factors. For one, large corporate actors guilty of breaking a cable should face a higher fine than commercial fishermen; this differentiation would help mitigate any political pushback from the organizations representing the latter group. Additionally, the fine should increase based on the level of culpability; for instance, a safe harbor could be created for commercial entities that install specific equipment to assist with location monitoring of ships. Finally, those entities that have repeatedly broken cables should face continually greater fines as their number of violations increase. And, as mentioned above, the culpable party should have to directly compensate the cable owner for the repair costs, so long as the cable owner is a part of the information sharing regime.

VIII. Conclusion

Those nations that are part of UNCLOS should form a coalition to amend Article 113 to remedy the provision's current practical effect. More specifically, as currently written, "when a submarine cable beneath high seas or EEZ is broken or damaged by intentional or reckless conduct, in many cases no crime has been committed under any State's laws" because Article 113 requires States to have incorporated the article into their national laws and most states have not done so based on research by Beckman.[220] This same coalition should also establish universal jurisdiction over persons who intentionally destroy or damage submarine cables; doing so would reflect the reliance of so many States on this system, as well as the increased threat of terrorist acts against the cables.[221]

Other ideas worthy of consideration by the international community include laying more "dark cables," creating a new international treaty penalizing international interference with undersea cables, and mandating minimum levels of CLS security in that same international treaty. Sunak recommended each of these strategies, as well as several others, in his report.[222] Dark cables refer to cables that do not appear on publicly available maps. By staying out of public knowledge, the cables are made more secure against intentional sabotage or

[220] *See* BECKMAN, *supra* note 102, at 13–14.
[221] *Id.*; *see also* SUNAK, *supra* note 10, at 17 (stating "There is a strong argument that international damage is a crime that attracts universal jurisdiction and all states should have jurisdiction over the offender, something that Article 113 does not provide for.").
[222] *See* SUNAK, *supra* note 10, at 34–36.

espionage efforts. Sunak envisions using tax incentives to encourage cable owners to create these clandestine cables.[223]

Sunak also calls for the creation of an entirely new international treaty specifically tailored to meeting the needs of the undersea cable system.[224] Though the prospects of getting the international community to agree on much of anything these days seem dim, this narrowly tailored treaty could bring a sufficient number of major stakeholders together to build momentum toward a new treaty. If legislation incorporating Article 113 into domestic law is any indication of a willingness to take proactive steps to protect the undersea cable system, then even China may be supportive of such a treaty. Of course, private stakeholders would likely sign on as well if the treaty helped them more expeditiously repair their cables. This treaty should also include efforts to inventory and coordinate the use of cable repair resources. Given that there are around 59 cable ships in the world and only half stand ready to conduct emergency repairs, it is essential that these resources are used deliberately by the international community.[225] This would be a marked improvement on the current approach to sharing repair resources: private contracts developed around geographic regions.[226] An international agreement could also incentivize the creation of more such ships, especially if treaty signatories could provide extra funds to ships that reach breaks in the most timely fashion.

Though CLS protection was not the focus of this paper, Sunak makes a convincing case for making CLS a focus of international collaboration. Right now, CLS tend to be concentrated in a few areas in coastal states.[227] Oftentimes, these CLS have little to no security, making them easy targets for attackers. An international agreement could help create standards for keeping these sites safe from threats, ranging from climate change to terrorists. Notably, the FCC could also institute such standards through its licensing authority.

No single policy is capable of mitigating all of the threats facing the undersea cable system. Still, some policies seem more likely than others to deter the actions most commonly associated with breaks in undersea cables. These policies ought to be pursued first, though efforts to form a broader, more

---

[223] *See id*. at 35.
[224] *See id*. at 35–36.
[225] *See* BURNETT & CARTER, *supra* note 97, at 45.
[226] *Id*.
[227] *See, e.g.*, SUNAK, *supra* note 10, at 6 ("UK cables are highly concentrated in a small number of landing sites.").

comprehensive international treaty related to undersea cables should also get underway.

The United States, given the transition to a new presidential administration, is well suited to lead on efforts to reform domestic laws related to undersea cables and respond to attackers and commercial actors. The Biden Administration must recognize the centrality of the undersea cable system to America's national security and economy; foreign actors have already come to that realization and are ready to exploit the nation's vulnerabilities.