Catholic University Journal of Law and Technology

Volume 24 | Issue 1 Article 4

December 2015

Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis

Tara Davenport
Yale Law School

SUBMARINE CABLES, CYBERSECURITY AND INTERNATIONAL LAW: AN INTERSECTIONAL ANALYSIS

Tara Davenport*

The international community's ever-increasing reliance on the Internet and web-based information and communications technologies ("ICT") has meant that cybersecurity is becoming one of the most pressing concerns in the 21st century. The International Telecommunications Union ("ITU")[1] has defined cybersecurity to mean "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."[2] The Distributed Denial of Service attacks against Estonia and Georgia in 2007 and 2008 respectively where coordinated botnets overwhelmed servers and shut down the Internet;[3] the disruption of the operation of centrifuges at an Iran nuclear facility by the Stuxnet worm in 2010;[4] the sustained State-sponsored cyber-hacking program in China;[5] and the discovery that national security agencies in the West have been carrying out mass surveillance of virtual communications for years have

* LLB, London School of Economics, 2002; LLM (Maritime Law), National University of Singapore, 2010; LLM, Yale Law School, 2014; Lecturer, National University of Singapore; Research Fellow, Centre of International Law, National University of Singapore; J.S.D. Candidate, Yale Law School, 2017.

1 The International Telecommunications Union ("ITU") is the leading U.N. agency that establishes international standards for information and communication technology. *See About ITU,* INT'L TELECOMM. UNION, http://www.itu.int/en/about (last visited Oct. 5, 2015).

2 INT'L TELECOMM. UNION, REC. ITU-T X.1205, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY 2 (2008), https://ccdcoe.org/sites/default/files/documents/ITU-080418-RecomOverviewOfCS.pdf.

3 Oona A. Hathaway et al., *The Law of Cyber-Attack,* 100 CALIF. L. REV. 817, 837-38 (2012).

4 Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon,* WIRED (Nov. 3, 2015, 6:30 AM), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

5 David Barboza & Kevin Drew, *Security Firm Sees Global Cyberspying,* N.Y. TIMES, Aug. 3, 2011 at A11.

elevated cybersecurity to the forefront of global attention.[6]

The discussions on cybersecurity in international policy and academic circles have focused primarily on how to protect the information that exists in cyberspace.[7] A glaring omission from this discussion is the security of the physical infrastructure that underpins the virtual cloud of cyberspace, namely the security of the submarine fiber optic network. These submarine communication cables—which are hidden from plain view—form a vast network on the seabed, are often no bigger than a garden hose, and transmit massive amounts of data across oceans.[8] They provide over 95% of international telecommunications—not via satellites as is commonly assumed.[9] The global submarine network is the "backbone" of the Internet, and enables the ubiquitous use of e-mail, social media, phone and banking services;[10] goods and services we now take for granted. As technology develops, uses for submarine fiber optic cables continue to evolve, and their utility goes beyond the mere transmission of data—these cables are now extensively relied upon by the military, the oil and gas industry, as well as the scientific community.

Notwithstanding their status as critical communications infrastructure, submarine cable systems remain vulnerable to a variety of emerging cybersecurity challenges. First, since September 11th, there has been a growing concern about submarine cable systems as targets—specifically, the possibility of what will be broadly described as *intentional interference* with submarine cable systems by State and/or non-State actors.[11] This includes intentional damage to subma-

---

6 Ewen MacAskill et al., *NSA Files: Decoded – What the Revelations Mean for You,* THE GUARDIAN, (Nov. 1, 2013) [hereinafter MacAskill et al., *NSA Files*], http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

7 *See generally* Press Release, The White House, Off. of the Press Sec'y, Securing Cyberspace: President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015) (on file with author); Cheryl Pellerin, *Defense, Intel Leaders: Cybersecurity Priorities Are Defense, Deterrence*, U.S. DEP'T OF DEF. (Sept. 29, 2015), http://www.defense.gov/News-Article-View/Article/621018/defense-intel-leaders-cybersecurity-priorities-are-defense-deterrence.

8 Christopher Intagliata & Marlisse Silver Sweeney, *What Links the Global Internet? Wires Inside Tubes No Bigger Than a Garden Hose*, PRI (Apr. 20, 2015. 8:00 AM), http://www.pri.org/stories/2015-04-20/what-links-global-internet-wires-inside-tubes-no-bigger-garden-hose; Victoria Woollaston, *Messages From the Deep: Interactive Map Plots the Sprawling Growth of the Submarine Cable Network Since 1989*, DAILY MAIL (July 24, 2014, 2:37 AM), http://www.dailymail.co.uk/sciencetech/article-2692774/Messages-deep-Interactive-map-plots-sprawling-growth-submarine-cable-network-1989.html.

9 LIONEL CARTER ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD 8 (2009), http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf.

10 Tara Davenport, *Submarine Communications Cables and Science: A New Frontier in Ocean Governance?, in* SCIENCE, TECHNOLOGY, AND NEW CHALLENGES TO OCEAN LAW 209, 209 (Harry N. Schreiber et al. eds., 2015) [hereinafter Davenport, *A New Frontier*].

11 Robert Beckman, *Protecting Submarine Cables From Intentional Damage–The Secu-*

rine cables laid on the seabed, cable landing stations, as well as attacks against the virtual or cyber aspect of submarine cable systems when perpetrators hack into the network management systems used to operate cable systems.[12]

Second, submarine cables can also be used as *tools* in cyber-espionage and intelligence gathering.[13] The recent startling disclosure by Edward Snowden that, for instance, the United States and the United Kingdom have engaged in the "the largest programme [sic] of suspicionless surveillance in human history"[14] by "tapping directly into the Internet backbone,"[15] namely the fiber optic cables, has catapulted this issue to the forefront of global discourse.

As such, this Article will examine the relationship between submarine cables and cybersecurity in the context of these two challenges. Specifically, it will examine the applicable international law that could potentially address these two challenges and whether the current legal regimes are adequate in ensuring the security of the vast network of cables that cross the ocean floor, and thus the security of the world's telecommunications systems.

Part I will provide background on the development of submarine communications cables, its importance, and how the industry works. Part II will discuss the prevailing regime governing submarine cables as set out in the 1982 United Nations (U.N.) Convention on the Law of the Sea. Part III will examine the first threat to cybersecurity, namely intentional interference with submarine cable systems while Part IV will explore how submarine cables have been used as tools in cyber-espionage. Part V will set out some recommendations on what can be done to enhance the security of the submarine cable network.

---

rity Gap, in SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 281, 281 (Douglas R. Burnett, et al., eds. 2014) [hereinafter Beckman, *Protecting Submarine Cables*]; *see generally* David E. Sanger & Eric Schmitt, *Russian Ships Near Data Cables Are Too Close*, N.Y TIMES (Oct. 25, 2015), http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=1 ("Russian submarines and spy ships are aggressively operating near the vital undersea cables that carry almost all global Internet communications, raising concerns among some American military and intelligence officials that the Russians might be planning to attack those lines in times of tension or conflict.").

12 Beckman, *Protecting Submarine Cables, supra* note 11, at 283.

13 Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, THE ATLANTIC (July 16, 2013), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

14 Ewen MacAskill et al., *GCHQ Taps Fibre-optic Cables For Secret Access to World's Communications*, THE GUARDIAN (June 21, 2013, 12:23 PM) [hereinafter MacAskill et al., *GHCQ*], http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

15 Jon Street, *Wikimedia Among Nine Groups Suing the NSA for 'Tapping Directly Into the Internet Backbone'*, THE BLAZE (Mar. 10, 2015, 10:55 PM), http://www.theblaze.com/stories/2015/03/10/wikimedia-among-nine-groups-suing-the-nsa-for-tapping-directly-into-the-internet-backbone/.

I. SUBMARINE COMMUNICATIONS CABLES: A PRIMER

A. Development

There are two main types of submarine cables: submarine communications cables used to transmit data communications[16] and submarine power cables used to transmit electrical power from one location to another.[17] Both are designed for underwater use and are typically laid on or buried within the seabed.[18] These submarine communications cables are the basis of this Article and its discussion.

The genesis of submarine cables can be traced to the early part of the 19th century and the development of the electric cable that used electricity to transmit and receive information over significant distances.[19] In 1850, the first submarine telegraph cable, consisting of copper wires and *gutta percha*—a type of naturally produced latex—was laid across the English Channel from Dover, England to Calais, France.[20] While this cable did not last more than a few messages, its creation marked the beginning of the submarine cable industry.[21] Advances in laying technique, design, and material meant that submarine telegraph cables were becoming increasingly durable and "[b]y the early 20th century, much of the world was connected by a network that enabled rapid communication and dissemination of information for government, commerce and the public."[22] However, submarine telegraph cables soon faced growing competition from radio telegraph technology, which had greatly improved during World War I.[23] Facing the global depression of the 1930s, the submarine telegraph cable industry steadily declined.[24]

The end of the submarine telegraph era, however, saw the emergence of a new submarine communications cable, namely the submarine telephone cable. During the 1930s, a polyethylene-encased cable with a copper coaxial core was

---

16 *See, e.g., Submarine Network Solutions: Crossing Oceans to Connect the Planet*, ALCATEL-LUCENT, https://www.alcatel-lucent.com/solutions/submarine-networks (last visited Oct. 5, 2015).

17 *See* Patrick J. Kiger, *New Energy Projects Boost the Use of Undersea Power Cables*, NAT'L GEO. (Aug. 18, 2014, 11:03 AM), http://news.nationalgeographic.com/news/energy/2014/08/140819-submarine-power-cables-offshore-wind/.

18 Intagliata & Silver Sweeney, *supra* note 8.

19 Stewart Ash, *The Development of Submarine Cables, in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 19, 20 (Douglas R. Burnett, et al., eds., 2014).

20 CARTER ET AL., *supra* note 9, at 12.

21 *Id.*

22 *Id.* at 13.

23 Ash, *supra* note 19, at 27-28.

24 *Id.*

developed which allowed multiple voice channels to be realized.[25] In 1955 and 1956, two cables were laid between Scotland and Newfoundland called TAT-1 and thus began the age of submarine coaxial telephone communications.[26] During the 1960s, there were a slew of technological developments in design and laying techniques that enabled longer cables to be laid deeper in the ocean.[27] However, as with submarine telegraph cables, submarine telephone cables soon faced competition from satellite communications due to the former's lower capacity and relatively high cost.[28] During the 1970s and 1980s, satellites emerged as the primary means of telecommunications.[29] The last submarine telephone cable was laid between India and the United Arab Emirates in 1986 bringing the submarine telephone cable era to an end.[30]

That was not, however, the end of the submarine cable story. In 1966, two scientists made a discovery that would revolutionize telecommunications.[31] Dr. Charles Kao and Dr. George Hockham found "a fibre [sic] of glassy material constructed in a cladded structure" had "important potential as a new form of communication medium . . . compared with existing coaxial and radio systems" due to its "large information capacity and possible advantages in basic material cost."[32] This milestone discovery facilitated the development of terrestrial fiber optic systems in the late 1970s and in 1980, the first sea trial of a submarine fiber optic system occurred.[33] In 1986, a series of fiber optic submarine cables were installed, and thus began the fiber-optics era.[34] In 1988, the first trans-oceanic fiber optic cable linking the United States, United Kingdom, and France was installed and from this year onwards, submarine cables "started to outperform satellites in terms of the volume, speed and economics of data and voice communications."[35] This coincided with the release of the commercial Internet in the mid-1990s.[36] Essentially, these two technologies taken together revolutionized telecommunications:

---

25 CARTER ET AL., *supra* note 9, at 14.

26 *Id.* (noting that the submarine telephone cables carried 707 calls between London and North America on the first day of operation).

27 *Id.* at 14-15.

28 Ash, *supra* note 19, at 32.

29 CARTER ET AL., *supra* note 9, at 15.

30 Ash, *supra* note 19, at 32.

31 G.A. Hockham & K.C. Kao, *Dialectric-fibre Surface Waveguides for Optical Frequencies*, 113 PROCEEDINGS OF THE INST. OF. ELEC. ENG'RS, no.7, July 1966, at 1151, 1158.

32 G.A. Hockham & K.C. Kao, *Dialectric-fibre Surface Waveguides for Optical Frequencies*, 113 PROCEEDINGS OF THE INST. OF. ELEC. ENG'RS, no.3, July 1986, at 198.

33 *See* Ash, *supra* note 19, at 33-34.

34 *See id.* at 34.

35 CARTER ET AL., *supra* note 9, at 16.

36 *See* Barry M. Leiner et. al., *Brief History of the Internet,* INTERNET SOC., http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Nov. 15, 2015).

> [C]ables carried large volumes of voice and data traffic with speed and security; the internet made that data and information accessible and usable for a multitude of purposes. As a result, communications, business, commerce, education and entertainment underwent radical change.[37]

Today's modern submarine communications cables consist of a set of six to 24 glass fibers, an electrical conductor, an internal steel strength member, and a protective sheath of marine grade polypropylene, which are constructed to withstand harsh environmental conditions for up to 25 years.[38] Depending on where it is laid, a cable may have a protective armor (used on the continental shelf) composed of steel wires.[39] Cables without protective armor are usually laid in the deep ocean and are typically 17-20 millimeter (mm) diameter, whereas armored fiber-optic cables may reach 50 mm diameter.[40] "Cable sections and amplifiers, which boost the light signals carried by the glass fibers, are assembled into a nearly complete system, coiled in tanks in a factory and then loaded onto special cable-laying ships for installation."[41]

B. Critical Communications Infrastructure

The United Nations, in 2010, described submarine communications cables as "critical communications infrastructure" and "vitally important to the global economy and the national security of all States."[42] This is not an understatement. Today, submarine fiber optic cables provide the vast majority of international telecommunications—some 95% overall.[43] The global cable network is composed of an estimated 213 independent cable systems amounting to approximately 877,122 kilometers of fiber optic cables.[44] The majority of coun-

---

37 CARTER ET AL., *supra* note 9, at 16.

38 Ronald J. Rapp, Director, Cable Eng'g & Tech., Tyco Elec. Subsea Commc'n LLC, Submarine Cables: Critical Infrastructure Supplier Perspective, Address Before the 34th Annual Center for Oceans Law and Policy Conference 5 (May 21, 2010) [hereinafter Rapp, Submarine Cables], http://www.virginia.edu/colp/pdf/Rapp-Presentation.pdf.

39 Ronald J. Rapp, Director, Indus. & Mar. Liason, TE SubCom, Cable Laying and Repair – Cable Ship Operations, Address Before the Submarine Cables in the Sargasso Sea Workshop 6 (Oct. 23, 2014) [hereinafter Rapp, Cable Laying & Repair], http://www.virginia.edu/colp/pdf/Rapp-Presentation.pdf.

40 *Id.* at 7.

41 DOUGLAS BURNETT ET AL., SUBMARINE CABLES IN THE SARGASSO SEA: LEGAL AND ENVIRONMENTAL ISSUES IN AREAS BEYOND NATIONAL JURISDICTION 10 (2015) [hereinafter BURNETT ET AL., WORKSHOP REPORT], http://cil.nus.edu.sg/cil-news-highlights/submarine-cables-in-the-sargasso-sea-final-workshop-report-published/

42 G.A. Res. 65/37, ¶ 121 (Dec. 7, 2010).

43 CARTER ET AL., *supra* note 9, at 8.

44 Douglas Burnett et al., *Introduction: Why Submarine Cables?* to SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 1, 2 (Douglas R. Burnett et al. eds., 2014).

tries now rely on submarine cables for their communications needs and as of mid-2012, only 21 nations and territories remain unconnected to the fiber network with several of them having projects underway.[45] The global submarine network forms the backbone of the Internet, and consequently e-mail, social media, phone and banking services; goods and services we now take for granted.

With regard to financial services, it has been estimated that submarine cables "carry an excess of 10 trillion [U.S. dollars] a day in transactions."[46] Similarly, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) relies on cables to transmit financial data to "more than 8,300 member financial institutions in 195 countries."[47] "The U.S. Clearing House Interbank Payment System processes over 1 trillion [dollars] a day to more than 22 countries."[48]

From a global and national security perspective, submarine communications cables also play an essential role. For example, "a major portion of the [U.S. Department of Defense] data traveling on undersea cables is unmanned aerial vehicle (UAV) video, essential for war preparation."[49] As one scholar observed, "without ensured cable connectivity, the future of modern warfare is in jeopardy."[50] A further example of the importance of cables to the military is the development of the Global Information Grid (GiG) by the U.S. Department of Defense.[51] The GiG is the "globally, interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel."[52] The Grid utilizes portions of the international telecommunications systems and has been described as a "global network that can be used to control a global battlespace."[53]

Another recently developed use for submarine fiber optic cables is providing

---

45 *Id.*

46 Michael Sechrist, *New Threats, Old Technology: Vulnerabilities In Undersea Communications Cable Network Management Systems* 9 (Harv. Kennedy Sch., Belfer Ctr. for Sci. & Int'l Affs., Discussion Paper No. 2012-03, 2012) [hereinafter Sechrist, *New Threats*], https://citizenlab.org/cybernorms2012/sechrist.pdf.

47 *Id.* at 10.

48 *Id.*

49 MICHAEL SECHRIST, CYBERSPACE IN DEEP WATER: PROTECTING UNDERSEA COMMUNICATION CABLES BY CREATING AN INTERNATIONAL PUBLIC-PRIVATE PARTNERSHIP 6 (2010) [hereinafter SECHRIST, DEEP WATER], http://belfercenter.ksg.harvard.edu/files/PAE_final_draft_-_043010.pdf.

50 *Id.* at 5.

51 *Id.*; *see generally Global Information Grid*, NAT'L SEC. AGENCY, https://www.nsa.gov/ia/programs/global_information_grid/ (last visited Oct. 3, 2015).

52 *Global Information Grid, supra* note 51.

53 Robert Fonow, *Cybersecurity Demands Physical Security*, SIGNAL MAG., Feb. 2006, at 43, 44, http://www.afcea.org/content/?q=cybersecurity-demands-physical-security.

connectivity for offshore oil and gas installations.[54] "Communications between onshore facilities and offshore oil and gas facilities have historically been a challenge for the oil and gas industry" due to distance to land and space constraints on the installation itself.[55] Submarine fiber optic cables are now being increasingly utilized to link onshore oil and gas facilities to a variety of assets based in the sea, including conventional fixed platforms, floating platforms, and storage.[56] This facilitates real-time monitoring with sensors, collaboration, video surveillance, and work management systems as well as other applications that require continuous connectivity.[57]

Additionally, submarine communications cables are proving invaluable for scientific development.[58] In recent years, developments in technology have allowed submarine communications cables to be used for the collection of oceanographic data from the marine environment.[59] In this facet, "scientists have utilized submarine communications cables to transport data in real time from ocean observatories that collect oceanographic data."[60] Additionally, "there has been interest in using submarine communications cables not to just transport data but also to *collect* data by placing scientific sensors on these cables."[61] Scientists believe that the placement of sensors on these cables will allow for the collection of data on ocean temperature, salinity, and water pressure which could lead to disaster risk reduction and real-time monitoring of the oceans and climate.[62]

The many uses for communications cables are boundless and in many ways, submarine cables have emerged as one of the most important uses of the oceans. There is no doubt these "unseen and unsung cables are the true skeleton and nerve of our world, linking our countries together in a fiber optic web."[63]

---

54 *See generally* Wayne F. Nielsen & Tara Davenport, *Submarine Cables and Offshore Energy*, *in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 351, 351-54 (Douglas R. Burnett et al. eds., 2014).

55 *Id.* at 351.

56 *Id.* at 353.

57 *Id.*; s*ee GoM Fiber Optic Network*, BP GLOBAL, http://www.gomfiber.com/ (last visited Oct. 3, 2015).

58 *See generally* Lionel Carter & Alfred H.A Soons, *Marine Scientific Research Cables, in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 323, 325-28 (Douglas R. Burnett et al. eds., 2014); *see also* Davenport, *A New Frontier, supra* note 10, at 210-13.

59 Davenport, *A New Frontier*, *supra* note 10, at 210.

60 *Id.*

61 *Id.*

62 *Id.*; *see also* RHETT BUTLER, USING SUBMARINE CABLES FOR CLIMATE MONITORING AND DISASTER WARNING 3 (2012), https://www.itu.int/dms_pub/itu-t/oth/4B/04/T4B040000150001PDFE.pdf.

63 U.N. GAOR, 65th Sess., 59th plen. mtg. at 4, U.N. Doc. A/65/PV.59 (Dec. 7, 2010).

C. The Submarine Cable Industry

Two brothers, Jacob and John Brett, formed a British company called the English Channel Submarine Telegraph Company and developed the first submarine cable that was laid between Dover and Calais in 1850.[64] Telegraphs were perceived as benefitting trade and commerce, and thus it was inevitable that the industry would be driven by private investment.[65] This private commercial model employed by the Brett Brothers shaped the way in which the industry would develop and this structure remains prevalent today.[66] In the early stages, "British companies, with the assistance of the Empire, owned and controlled the vast majority of the submarine [telegraph] cable network."[67] However, other powers like France, Germany and Russia "were jarred to reality by the way in which Britain had put its control over large portions of the global telegraph cable infrastructure to great strategic and military advantage during the war," and thus they began their own cable laying program to shatter the British monopoly.[68] Indeed, in order to break their dependence on British cables, other countries started to investigate other technologies, such as the wireless telegraph, which in part caused the demise of the telegraph.[69]

Today, there are many private cable enterprises from various jurisdictions. There are two main types of cable companies involved in the industry.[70] The first category is the cable system owner that owns and/or operates the system.[71] They can consist of national telecommunications carriers, private companies and/or investment banks.[72] A trans-oceanic cable can cost up to 500 million U.S. dollars, and therefore, more often than not, these companies form consortiums of about 20-30 telecommunications companies to fund the design, construction, and maintenance of a new cable in return for a proportionate share of capacity.[73]

---

64 GRAEME MARETT, A HISTORY OF THE TELEGRAPH IN JERSEY: 1858 – 1940, at 2-3 (2009), http://www.marett.org/telecom/telegraph.pdf.

65 Jonathon W. Penney, *The Cycles of Global Telecommunication Censorship and Surveillance*, 26 U. PA. J. INT'L L. 693, 704 (2015).

66 *Id.* at 703.

67 *Id.*

68 *Id.* at 716.

69 *Id.* at 721.

70 Mick Green, *The Submarine Cable Industry: How Does it Work?, in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 41, 42 (Douglas R. Burnett et al. eds., 2014).

71 *Id.*

72 *Id.* at 43.

73 *Id.* at 46. For example, the Southern Cross Cable, which is located in Australian waters provides international bandwidth to Australia, New Zealand, Hawaii, and the continental United States. It cost $1.5 billion dollars to build and is jointly owned by Telecom New Zealand, SingTel Optus and Verizon Business. *See Our Company: About Southern Cross*, S. CROSS CABLES NETWORK, http://www.southerncrosscables.com/home/company (last visited Oct. 13, 2015).

The second category of cable companies comprises the cable suppliers who are responsible for the construction, operation, and maintenance of submarine cables.[74] These include the system suppliers who design, plan, and manufacture the cable system; the marine service suppliers who provide specialist vessels for cable installation operations; and the cable joint suppliers who supply joints and associated equipment required to replace damaged cables with new cables.[75]

The International Cable Protection Committee ("ICPC"), established in 1958, is an industry-based organization whose members include owners, operators, and suppliers of over 97 percent of the world's international submarine cable systems.[76] In 2010, membership was opened to governments, and several governments are now represented.[77] The ICPC issues Recommendations on various issues concerning submarine cables and has been instrumental in working with governments, international organizations, and other seabed users to preserve the integrity of the submarine cable network.[78]

At this juncture, it is pertinent to note that cables, unlike vessels, are not registered to any nationality.[79] The consortia or private companies that own and operate them are from various countries, as are the cable suppliers that construct them. One cable can span many different jurisdictions and for this reason, submarine cables are the very essence of transnational infrastructure.

II. THE INTERNATIONAL LEGAL REGIME GOVERNING SUBMARINE CABLES

Submarine cables were recognized early on as a public good that ought to be protected and regulated.[80] From 1863 to 1913, the protection of submarine cables appeared on the agenda of seven international conferences.[81] Between 1884 and 1982, the international community adopted four legal instruments that addressed the rights and obligations of States vis-à-vis submarine cables. These are: (1) the 1884 Convention for the Protection of Submarine Telegraph

---

74 Green, *supra* note 70, at 42.

75 *Id.* at 42-44.

76 *See About the ICPC,* INT'L CABLE PROT. COMM. (Jul. 24, 2015), https://www.iscpc.org/about-the-icpc/.

77 *Id.*

78 *See e.g.*, *ICPC Recommendations,* INT'L CABLE PROT. COMM. (Dec. 22, 2014), https://www.iscpc.org/publications/recommendations/.

79 Convention on the High Seas, art. 2, Apr. 29, 1958, 450 U.N.T.S. 82, 83-84 [hereinafter High Seas Convention].

80 *United Nations Documents on the Development and Codification of International Law,* 41 AM. J. INT'L L. SUPP. 29, 33-34 (1947).

81 *Id.*

Cables ("1884 Cable Convention");[82] (2) the 1958 Geneva Convention on the High Seas;[83] (3) the 1958 Convention on Continental Shelf;[84] and (4) the 1982 United Nations Convention on the Law of the Sea ("UNCLOS").[85]

The 1884 Cable Convention is a stand-alone convention dealing solely with the *protection* of submarine telegraph cables.[86] The convention's primary goal was to require State adoption of legislation that protected cables laying outside of territorial waters;[87] and presently has 40 State Parties.[88]

The 1958 Geneva Conventions on the High Seas and the Continental Shelf ("the 1958 Geneva Conventions") and UNCLOS are broad, comprehensive treaties that address various aspects of law of the sea. For purposes of this Article, UNCLOS is assumed to be the applicable legal regime governing submarine cables.[89]

The adoption of UNCLOS in 1982 was a milestone in international law and relations.[90] The 320 articles and 9 annexes, often described as a "constitution for the oceans"[91] took nine years to negotiate and involved more than 140 States, six non-independent States, eight national liberation movements, 12 specialized agencies, 19 intergovernmental organizations, and a number of quasi-autonomous units of the U.N.[92] One hundred and nineteen States signed

---

82 Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989, T.S. No 380 [hereinafter 1884 Cable Convention].

83 High Seas Convention, *supra* note 79, at 82.

84 Convention on the Continental Shelf, Apr. 29, 1958, 499 U.N.T.S. 311 [hereinafter Continental Shelf Convention].

85 United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].

86 *See generally* 1884 Cable Convention, *supra* note 82, art. 1.

87 Douglas R. Burnett et al., *Overview of the International Legal Regime Governing Submarine Cables, in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 63, 66 (Douglas R. Burnett et al. eds., 2014) [hereinafter Burnett et al., *Overview*].

88 *Id.* at 64.

89 UNCLOS has received widespread acceptance and presently has 167 Parties. *See Status of U.N. Convention on the Law of the Sea,* UNITED NATIONS TREATY COLL., https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&lang=en (last visited Oct. 2, 2015). For parties to both the 1958 Geneva Conventions and UNCLOS, the latter supersedes the former. *See* UNCLOS, *supra* note 85, art. 311, ¶ 1. Further, most of the UNCLOS provisions on submarine cables are based on the provisions found in the 1958 High Seas Convention which codified existing customary international law. *See* Burnett, *Overview, supra* note 87, at 65. These provisions are consequently binding on non-parties. *Id.*

90 *See generally The United Nations Convention on the Law of the Sea (a historical perspective)*, U.N. DIV. FOR OCEAN AFF. & THE LAW OF THE SEA, http://www.un.org/Depts/los/convention_agreements/convention_historical_perspective.htm (last visited Oct. 2, 2015).

91 *See* Tommy T.B. Koh, Former Singapore Ambassador to the United Nations, Remarks Before the Third United Nations Conference on the Law of the Sea (Dec. 11, 1982), http://www.un.org/Depts/los/convention_agreements/texts/koh_english.pdf.

92 For an overview of the negotiating history of the Third Conference on the Law of the

the Convention and it presently has 167 States Parties.[93] UNCLOS purports to establish a "legal order for the seas and oceans"[94] by demarcating zones of juridical competence and assigning different rights and obligations to coastal States and other users of the sea.[95] These maritime zones can be generally categorized as (1) areas under territorial sovereignty (the territorial sea, archipelagic waters, straits used for international navigation); (2) areas outside sovereignty but within national jurisdiction (the Exclusive Economic Zone and Continental Shelf) and (3) areas beyond national jurisdiction (high seas and the deep seabed).[96]

UNCLOS addresses the rights and obligations of States for both the *protection of submarine cables* and *the freedom to lay, repair and maintain such cables* (the installation of cables), the scope and extent of which are determined by where these cable activities are taking place.[97]

A. The Installation of Submarine Cables

Cable installation on the seabed involves three distinct phases. First, the optimal cable route must be determined.[98] This initially involves a Desktop Survey, which takes into account landing sites, seabed bathymetry and geology, fishing and anchoring uses, cable and pipeline crossings, permitting requirements of coastal States and other constraints, such as boundaries.[99] The Desktop Survey is followed by a cable route survey by a survey vessel in order to "fully characterize that route and to avoid hazards and/or environmentally sig-

---

Sea, *see* Tommy T.B. Koh & Shanmugam Jayakumar, *The Negotiating Process of the Third United Nations Conference on the Law of the Sea, in* 1 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY 29-68 (Myron Nordquist et al. eds., 1985) [hereinafter 1 UNCLOS COMMENTARY].

93 *See Chronological Lists of Ratifications of, Accessions and Successions to the Convention and the Related Agreements as at 3 October 2014*, U.N. DIV. FOR OCEAN AFF. & THE LAW OF THE SEA, http://www.un.org/Depts/los/reference_files/chronological_lists_of_ratifications.htm (last visited Oct. 2, 2015).

94 UNCLOS, *supra* note 85, pmbl.

95 *Id.*

96 *Id.* arts. 2, 46, 55, 76, 86.

97 *Id.* arts. 79, 112, 113.

98 *Subsea Cables – Installation Procedures and Methods*, KINGFISHER INFO. SERV.-OFFSHORE RENEWABLE & CABLES AWARENESS, http://www.kis-orca.eu/subsea-cables/installation-procedures-and-methods#.Vg8GoxNViko (last visited Oct. 2, 2015).

99 *See generally* Graham Evans & Monique Page, *The Planning and Surveying of Submarine Cable Routes, in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 93, 94-95 (Douglas R. Burnett et al. eds., 2014).

nificant zones that may not have been identified from existing information."[100] "The selection of the final route is determined by a cost-benefit analysis of the cost of laying a cable along a particular route versus the need to protect the cable."[101] Thus, the final selection will be the route that best "avoid[s] hazards and obstacles such as fishing areas, anchorages, military operation areas, munitions or other dumping areas and environmentally sensitive areas."[102]

The second stage is the laying of the cable on the seabed.[103] A cable is deployed along the previously designated route by trained crew on specialized cable-laying vessels, which spool the cable out of huge holding tanks.[104] Depending on the route, the cable will either be buried beneath the seabed or laid on the seabed surface. Typically, cables will be surface laid in water depths deeper than 1500 meters—a depth beyond the reach of risky human activities such as anchoring and fishing.[105] Once laid on the seabed close to land, cables cross a beach and enter a "beach manhole", running a land route until it reaches the cable landing station, a shore terminal building.[106] In short, the beginning and ending points of undersea cable systems are the landing stations which provide a gateway to landline communication networks.[107]

The third stage is cable repair and maintenance.[108] Typically, a cable's lifespan is 15 – 20 years, during which time, it may need to be retrieved from the seabed for repairs or maintenance.[109] Repairs entail finding the location of the cable, identifying the faulted section and replacing that section with a new cable.[110]

1. The High Seas

Since the laying of the first submarine cable in 1850, the freedom to lay submarine cables in the high seas has been unchallenged[111] and subsequently

---

100 CARTER ET AL., *supra* note 9 at 21.

101 BURNETT ET AL., WORKSHOP REPORT, *supra* note 41, at 10.

102 *Id.*

103 *Id*. at 11.

104 *See* Keith Ford-Ramsden & Tara Davenport, *The Manufacture and Laying of Submarine Cables*, *in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 123, 127-28 (Douglas R. Burnett et al. eds., 2014).

105 BURNETT ET AL., WORKSHOP REPORT, *supra* note 41, at 10-11.

106 Tara Davenport, *Submarine Communications Cables and Law of the Sea: Problems in Law and Practice*, *in* 43 OCEAN DEV. & INT'L L. 201, 204 (2012) [hereinafter Davenport, *Submarine Cables*].

107 Michael Matis, The Protection of Undersea Cables: A Global Security Threat 7 (July 3, 2012) (unpublished M.S.S. dissertation, U.S. Army War College) (on file with author).

108 Davenport, *Submarine Cables, supra* note 106, at 204.

109 *Id.*

110 CARTER ET AL., *supra* note 9, at 24.

111 *See* MYRES S. MCDOUGAL & WILLIAM T. BURKE, THE PUBLIC ORDER OF THE OCEANS:

affirmed in the 1958 Convention on the High Seas[112] and UNCLOS.[113] Article 87 of UNCLOS states that the freedom of the high seas includes the freedom to lay submarine cables and pipelines, subject to Part VI, on the continental shelf.[114] Article 112 (1) of UNCLOS reinforces this by stipulating that "all States are entitled to lay submarine cables and pipelines on the bed of the high seas beyond the continental shelf."[115] While not explicitly mentioned, there is no doubt that survey, repair and maintenance activities that are an essential component of cable operations are included in the freedom to lay cables in the high seas.[116]

However, the freedom is not completely unlimited. First, Article 112 (2) requires States to have due regard to cables already in position and not to prejudice the possibility of repairing existing cables or pipelines.[117] Second, the freedom to lay submarine cables must be exercised with due regard for the interests of other States in their exercise of high seas freedoms (such as fishing and navigation) in addition to the due regard for the rights under UNCLOS

A CONTEMPORARY INTERNATIONAL LAW OF THE SEA 781 (1962). The 1884 Cable Convention dealt only with the protection of submarine cables and not the freedom to lay cables because "[i]t was evident that freedom of use was conceded by all and that the real concern was to adopt measures for protecting cables from other, sometimes physically incompatible uses of the ocean." *Id.*

112 See Report of the International Law Commission to the General Assembly, ¶ 192, 5 U.N. GAOR Supp. No. 12, at 21, U.N. Doc. A/1316 (1950), *reprinted in* [1950] 2 Y.B. Int'l L. Comm'n 364, U.N. Doc. A/CN.4/SER.A/1950/Add.1. In 1950, the International Law Commission (ILC) first recognized the principle that all States were entitled to lay submarine cables on the high seas. *See Summary Records of the 65th Meeting,* [1950] 1 Y.B. Int'l L. Comm'n 199, U.N. Doc A/CN.4/SER.A/1950. Indeed, at the second session of the ILC, it was observed that there was no need to explicitly mention the freedom to lay cables in any convention on the topic as this freedom had never been questioned. *Id.* However, it was ultimately agreed that that it was important to include it in any convention on the law of the sea. *See* High Seas Convention, *supra* note 79, arts. 2, 26 ¶ 1. Accordingly, Article 27 of the ILC Draft Articles states that freedom of the high seas comprises, amongst other things, the freedom to lay submarine cables and pipelines and article 61 recognizes that "all States shall be entitled to lay telegraph, telephone or high-voltage power cables and pipelines on the bed of the high seas." 1 SIR ARTHUR WATTS, THE INTERNATIONAL LAW COMMISSION 1949-1998: THE TREATIES 58, 92 (1999).

113 *See* UNCLOS, *supra* note 85, art. 112.

114 *Id.* art. 87, ¶ 1. This is in recognition of the fact that for cables which are laid on the extended continental shelf beyond 200 nm, the continental shelf regime on submarine cables and not the high seas regime will apply.

115 *Id.* art. 112, ¶ 1.

116 *Id*. art. 79, ¶ 5. Article 112 (2) of UNCLOS states that Article 79 (5) (found in Part VI on the continental shelf) applies to cables laid in the high seas. *Id.* art. 112, ¶ 2. Article 79 (5) states that "possibilities of repairing existing cables or pipelines shall not be prejudiced." This reinforces the position that the freedom to lay also includes the freedom to repair. *Id.* art. 79, ¶ 5.

117 *Id.*

with respect to activities in the area where deep seabed mining takes place and that which is under the purview of the International Seabed Authority.[118]

At this juncture, it warrants noting that UNCLOS affords the freedom to lay cables to "all States."[119] In reality, as previously mentioned, it is private companies that own and operate cables, and it is private companies that lay and repair cables. The Virginia Commentary noted that the term "all States" should not be read restrictively as "[i]n practice, many submarine cables and pipelines are privately owned and are laid by corporations or other private entities. The term therefore refers to the right of States or their nationals to lay cables or pipelines."[120]

2. The Exclusive Economic Zone / Continental Shelf

During the negotiations of UNCLOS, the long-recognized freedom to lay submarine cables on the high seas had to be adapted to take into account the interests of the coastal State and other States in the newly established maritime zones of the continental shelf and the Exclusive Economic Zone ("EEZ").[121] Both these maritime zones are areas in which the coastal State did not have sovereignty but instead had *sovereign rights* to resources that could impact the freedom to lay cables and vice versa.

Under the continental shelf regime in Part VI of UNCLOS, a coastal state has sovereign rights for the purpose of exploring the continental shelf and exploiting its natural resources,[122] which include "mineral and other non-living resources of the seabed and subsoil."[123] The continental shelf is defined as:

> the seabed and subsoil of the submarine areas that extend beyond its territorial sea throughout the natural prolongation of its land territory to the outer edge of the continental margin, or to a distance of 200 nautical miles from the baselines from which the breadth of the territorial sea is measured where the outer edge of the continental margin does not extend up to that distance.[124]

The EEZ regime in Part V of UNCLOS, recognized the rights of the coastal State to claim a 200 nautical mile (nm) EEZ that gives coastal States *sovereign rights* to the exploration and exploitation of both living and non-living re-

---

[118] *Id.* art. 87, ¶ 2.

[119] *Id.*

[120] 3 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY 264 (Myron Nordquist et al. eds., 1995) [hereinafter 3 UNCLOS COMMENTARY].

[121] UNCLOS, *supra* note 85, arts. 56, 79. While the existence of the continental shelf pre-dated UNCLOS and was recognized in the 1958 Continental Shelf Convention, the definition of the continental shelf changed significantly during the negotiations of UNCLOS. *See generally* 2 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY 841-84 (Myron Nordquist et al. eds., 1993) [hereinafter 2 UNCLOS COMMENTARY].

[122] UNCLOS, *supra* note 85, art. 77, ¶ 1.

[123] *Id.* art. 77, ¶ 4.

[124] *Id.* art. 76.

sources of "the waters superjacent to the seabed and of the seabed and subsoil."[125] A coastal State also has jurisdiction, as provided in UNCLOS, over artificial islands, installations, and structures; marine scientific research; and the protection and preservation of the marine environment in its EEZ.[126]

Both the EEZ and the continental shelf regime give the coastal State two distinct legal bases for rights over the seabed within 200 nm. However, the negotiators of UNCLOS recognized the need to harmonize the content of the legal interest within two separate regimes that geographically overlapped.[127] Accordingly, Article 56 (3) of UNCLOS provides that the rights set out in the EEZ regarding the seabed and subsoil are to be *"exercised in accordance with Part VI on the continental shelf* [emphasis added]."[128] The provisions on submarine cables in Part V and Part VI, while not drafted in identical terms, essentially result in the same rights and obligations with respect to submarine cables, in areas within 200 nm of the coast. In situations where a coastal state has an entitlement to a continental shelf beyond 200 nm (i.e. an outer continental shelf), the continental shelf regime solely applies.[129]

UNCLOS affirms that all States have the freedom to lay submarine cables in the EEZ and continental shelf. In the EEZ, Article 58 provides:

> In the exclusive economic zone, all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in article 87 of navigation and overflight and of the *laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines,* and compatible with the other provisions of this Convention (emphasis added).[130]

As mentioned above, Article 87 provides that freedoms of the high seas include the "freedom to lay submarine cables and pipelines, subject to Part VI [on the continental shelf]."[131] Similarly, Part VI reinforces this right on the continental shelf by stipulating in Article 79 (1) that "all States are entitled to lay

---

[125] *Id.* art. 56.

[126] *Id.*

[127] MALCOLM EVANS, RELEVANT CIRCUMSTANCES AND MARITIME DELIMITATION 36 (1989).

[128] UNCLOS, *supra* note 85, art. 56, ¶ 3.

[129] The waters above the outer continental shelf are high seas, but Article 87(1)(c) recognizes that the freedom
to lay cables in the high seas is subject to Part VI on the continental shelf. *Id.* art. 87, ¶ 1.

[130] *Id.* art. 58.

[131] *Id.* art. 87. The Virginia Commentary on UNCLOS notes that the high sea freedoms exercised in the EEZ by other States are the same as those incorporated from Article 87, provided that they are compatible with the other provisions of UNCLOS. The difference is that these freedoms are subject to measures related to the sovereign rights of the coastal state in the EEZ and they are not subject to such measures or those rights beyond that zone. 2 UNCLOS COMMENTARY, *supra* note 121, at 564-65.

submarine cables and pipelines on the continental shelf in accordance with the provisions of this article."[132]

Laying of submarine cables also includes the right to repair and maintain them as these activities would be considered "other internationally lawful uses of the sea related to these freedoms . . . such as those associated with the operation of . . . submarine cables" in the EEZ.[133] With regard to the continental shelf, Article 79 (1) does not explicitly refer to repair or maintenance, however, the rest of Article 79 assumes that the right to lay submarine cables includes the right to maintain and repair them.[134] Similarly, cable route surveys should also be considered an "internationally lawful use of the sea related . . . to the operation of . . . submarine cables" as they are essential to the laying of cables.[135]

However, the right to lay submarine cables and associated rights is not unlimited. First, States or companies conducting cable operations in the EEZ/continental shelf must have due regard to the cables or pipelines already in position and must not prejudice the possibilities of repairing existing cables or pipelines.[136]

Second, such states or companies must have due regard to the rights and duties of the coastal state in the EEZ[137] and in the continental shelf, to the extent the latter overlaps with the EEZ. The rights and duties of the coastal State refers to the rights and duties enumerated in Article 56 and elaborated on in other UNCLOS provisions, namely, rights over the exploration and exploitation of: living resources; nonliving resources; other economic resources such as the production of energy from the water, currents, and winds; jurisdiction over artificial islands, installations, and structures; jurisdiction over marine scientific research; and jurisdiction over the protection and preservation of the marine environment, and the consequent duties that accompany such jurisdiction.[138]

Third, states conducting cable operations "shall comply with the laws and regulations adopted by the coastal State in accordance with the provisions of this Convention and other rules of international law in so far as they are not incompatible with this Part."[139] The question is to what extent a coastal State can regulate cable operations in the EEZ/continental shelf.

---

132 UNCLOS, *supra* note 85, art. 79, ¶ 1.

133 *Id.* art. 58.

134 *See id.* art.79, ¶ 2 (referring to the "laying or maintenance" of submarine cables); *Id.* art. 79 ¶ 5 (referring to "repairing" existing cables).

135 *Id.* art. 58.

136 *Id.* art. 79, ¶ 5.

137 *Id.* art. 58.

138 UNCLOS, *supra* note 85, art. 56.

139 *Id.* art. 58.

In this regard, "UNCLOS has substantive provisions on the type of regulations coastal States may adopt, as well as procedural obligations that must be complied with if such regulations are adopted."[140] First, Article 79 (2) of UNCLOS states:

> Subject to its right to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources and the prevention, reduction and control of pollution from pipelines, the coastal State may not impede the laying or maintenance of such cables or pipelines.[141]

Article 79 (2) appears to distinguish between submarine cables and pipelines. Specifically, with respect to pipelines, a coastal State is permitted to impose reasonable measures for (1) the exploration of the continental shelf; (2) the exploitation of its natural resources and (3) the prevention, reduction, and control of pollution from pipelines.[142] For submarine cables, a coastal State can only subject it to reasonable measures for the (1) exploration of the continental shelf and (2) the exploitation of its natural resources. This appears to be in recognition of the belief that submarine cables do not cause pollution.[143]

Second, Article 79 (3) states that the "delineation of the course for the laying of such pipelines on the continental shelf is subject to the consent of the coastal State."[144] The clear implication is that the delineation of the course for submarine cables is *not* subject to the consent of the coastal State. This is supported by the legislative history of the provision.[145] However, it has been argued that the coastal State can still impose conditions for the delineation of the cable route pursuant to the right to impose "reasonable measures" for the exploration of the continental shelf and the exploitation of its natural resources as set out in Article 79 (3).[146] For example, the coastal State could require that the route avoid areas in which offshore exploration/exploitation is taking place or areas that are intensively fished.

Third, Article 79 (4) provides that nothing in Part VI "affects the right of the coastal State to establish conditions for cables or pipelines entering its territory

---

140 Davenport, *Submarine Cables, supra* note 106, at 210.

141 UNCLOS, *supra* note 85, art. 79, ¶ 2.

142 The provision for prevention, reduction and control of pollution from pipelines did not exist in the equivalent article (Article 4) of the 1958 Continental Shelf Convention, and was added during the negotiations of UNCLOS III. *See* 2 UNCLOS COMMENTARY, *supra* note 121, at 912.

143 *See* Lionel Carter, Douglas Burnett, & Tara Davenport, *The Relationship Between Submarine Cables and the Marine Environment, in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 179, 183 (Douglas R. Burnett et al. eds., 2014).

144 UNCLOS, *supra* note 85, art. 79, ¶ 3.

145 2 UNCLOS COMMENTARY, *supra* note 121, at 915.

146 *See* Rainer Lagoni, Legal Aspects of Submarine High Voltage Direct Current (HVDC) Cables 20 (1998); *see also* UNCLOS, *supra* note 85, art. 79, ¶ 3.

or territorial sea . . . ."[147] This reflects the fact that in its territorial sea and land territory, coastal States have sovereignty over submarine cables and can impose conditions for their operation within these areas. The purpose of this provision is to ensure:

> [T]he restrictions in article 79 on the right of a coastal State to regulate cables on the continental shelf [where it has sovereign rights but not sovereignty] does not affect the more extensive rights of the coastal State to impose additional conditions on cables which enter its territory or territorial sea [where it has sovereignty].[148]

Apart from the above substantive rights that coastal States have in relation to the regulation of submarine cables, UNCLOS also imposes certain procedural obligations on coastal States when exercising their rights to regulate submarine cables. First, these measures must be "reasonable" as required in Article 79 (2).[149] The term "reasonable" is admittedly vague but "no more definite criterion than that of reasonableness could be established for the measures which coastal states may take, for the reason that it was impossible to foresee all situations that might arise in the application of [this article]."[150] The second procedural obligation is that in the EEZ (and in the continental shelf to the extent it overlaps with the EEZ), a coastal state must have due regard to the rights and duties of other States and shall act in a manner compatible with the provisions of UNCLOS.[151] Third, on the continental shelf (and in the EEZ to the extent it overlaps with the continental shelf), a coastal state must not exercise its rights in a manner that will infringe or result in "any unjustifiable interference" with navigation and other rights and freedoms of other states as provided for in UNCLOS.[152]

3. Submarine Cables Under the Jurisdiction of the Coastal State

UNCLOS provides for an exception to the freedom to lay submarine cables in the EEZ/continental shelf.[153] Under Article 79 (4), submarine cables "used in connection with the exploration of its continental shelf or exploitation of its resources or the operations of artificial islands, installations and structures un-

---

147 UNCLOS, *supra* note 85, art. 79, ¶ 4.

148 Robert Beckman, Director, Ctr. for Int'l Law Nat'l Univ. of Sing., Submarine Cables—A Critically Important but Neglected Area of the Law of the Sea, Presented Before the 7th International Conference on Legal Regimes of Sea, Air, Space and Antarctica 7 (Jan. 17, 2010) [hereinafter Beckman, Critically Important], cil.nus.edu.sg/wp/wp-content/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables- rev-8-Jan-10.pdf.

149 UNCLOS, *supra* note 85, art. 79, ¶ 2.

150 Marjorie Whiteman, *Conference on the Law of the Sea: Convention on the Continental Shelf*, 52 AM. J. INT'L L. 629, 642 (1958).

151 UNCLOS, *supra* note 85, art. 56.

152 *Id.* art. 78.

153 *Id.* art. 79.

der its jurisdiction" are under the jurisdiction of the coastal State.[154]

The coastal State's jurisdiction over submarine cables under Article 79 (4) is a direct consequence of its sovereign rights over the resources of the continental shelf/EEZ as well as over other activities for the economic exploitation and exploration of the zone (such as the production of energy from water, currents and winds),[155] and its jurisdiction over the establishment and use of artificial islands, installations, and structures.[156] This provision would appear to apply to submarine communications and power cables used to provide communications for oil and gas platforms and wind farms.

4. Territorial Seas

Under UNCLOS, a coastal State has sovereignty over 12 nautical miles of sea known as the territorial sea.[157] Pursuant to their sovereignty over the territorial sea,[158] coastal States clearly have extensive authority to regulate ships engaged in cable operations (i.e. the surveying of cable routes and the laying, repair, and maintenance of cables in these maritime zones). Coastal States will usually require the whole gamut of permits, licenses, and environmental conditions to be met before permission is given to deploy a power cable in these maritime zones.[159]

B. The Protection of Submarine Cables

The protection of submarine cables has always been a concern of the international community as early as the 1880s when the 1884 Cable Convention was adopted.[160] Within the territorial sea, coastal States[161] have an express right to adopt laws and regulations "relating to innocent passage through their territorial sea" in order to protect submarine cables.[162] They also have a general competence to enact laws to protect submarine cables within such territorial waters.[163] However, under UNCLOS there is no *obligation* on coastal States to adopt laws and regulations to protect submarine cables within territorial wa-

---

154 *Id.* art. 79, ¶ 4.
155 *Id.* arts. 56, 77.
156 *Id.* arts. 56, 80.
157 *Id.* art. 3.
158 *Id.* art. 2.
159 *See generally* Ford-Ramsden & Davenport, *supra* note 104, at 140-46 (relating to the regulations imposed on communications cables in territorial waters).
160 *See* 1884 Cable Convention, *supra* note 82.
161 UNCLOS, *supra* note 85, art. 21.
162 *Id.*
163 *Id.*

ters.[164]

Outside territorial waters, namely the EEZ, continental shelf and high seas, there are express provisions in UNCLOS on the protection of cables that apply. Articles 113 to 115 of UNCLOS address the protection of submarine cables on the *high seas* and are based on three articles in the 1884 Cable Convention.[165] They are also applicable to submarine cables laid in the EEZ under Article 58(2) as well as to cables laid on the continental shelf. [166]

Article 113 of UNCLOS requires States to adopt laws and regulations to provide that the breaking or injuring by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done willfully or through culpable negligence, is a punishable offense.[167] Such laws and regulations must also apply to conduct calculated or likely to result in such breaking or injuring. However, it shall not apply to any break or injury caused by persons whom acted to save lives or their ships, after having taken all necessary precautions to avoid such an occurrence.[168] Article 113 essentially extends a State's criminal jurisdiction (usually limited to territory) over acts of breaking or injury to submarine cables done "willfully or through culpable negligence."[169] This extension of jurisdiction only applies to ships flying the State's flag on the high seas or EEZ, or to its nationals whom commit such acts, consistent with general principles of international law on the prescription of extra-territorial jurisdiction.[170]

Article 114 of UNCLOS, which is based on Article IV of the 1884 Cable Convention, requires every State to adopt laws and regulations concerning the liability of owners of cables for the cost of repairs to existing cables which are damaged in the course of laying or repair operations.[171]

Article 115, which is based on Article VII of the 1884 Cable Convention, provides that every State should adopt laws and regulations to provide for an indemnity to be paid by cable owners to ship owners whose master sacrifices an anchor, a net or any other fishing gear in order to avoid injuring a submarine cable, provided that the ship owner has taken all reasonable precautionary measures beforehand.[172]

III. INTENTIONAL INTERFERENCE WITH SUBMARINE CABLE

---

164 *Id.*
165 *Id.* arts. 113-115.
166 UNCLOS, *supra* note 85, art. 58, ¶ 2.
167 *Id.* art. 113.
168 *Id.*
169 *Id.*
170 Davenport, *Submarine Cables, supra* note 106, at 218.
171 UNCLOS, *supra* note 85, art. 114.
172 *Id.* art. 115.

SYSTEMS

Submarine cables are laid on the seabed and are vulnerable to a host of threats including fishing and shipping activity as well as natural hazards such as earthquakes. Eighty per cent of cable faults are estimated to be attributable to human activity, with fishing being responsible for more than 60 percent of all human activity faults.[173] Cable faults can take several forms, including damage to the outer insulation that results in seawater seeping in and damaging the power conductor as well as the optical fibers so that they can no longer transmit light or a complete break in the cable.[174] Cable owners and operators utilize Network Operations Centers (NOCs) to monitor data traffic "through their networks on a 24/7 basis and are able to immediately identify any interruption to the traffic or a change in the normal operating conditions of the marine portion of the network."[175]

If an interruption does take place, the NOC operators will attempt to restore traffic as soon as possible by using other cable systems pursuant to a mutual restoration agreement.[176] If there are multiple simultaneous failures, there may be significant delays in restoration.[177] Quickly identifying the fault and deploying a cable repair ship to fix it as soon as possible is imperative.[178] Given the predominant dependence that today's world has on communications cables, an interruption in traffic could have serious consequences. For example, in a 2012 report on the Economic Impact of Submarine Cable Disruptions, it was estimated that the indirect economic costs of a fault in all the landing points in Australia would amount to 3.169 million U.S. dollars, mostly due to the loss of international internet traffic.[179]

Since the September 11th attacks, there has been a growing concern about the possibility of what will be broadly described as intentional interference with submarine cable systems by State and/or non-State actors.[180] In this re-

---

[173] Robert Wargo & Tara Davenport, *Protecting Submarine Cables From Competing Uses*, *in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 255, 256 (Douglas R. Burnett et al. eds., 2014).

[174] *Id.*

[175] Keith Ford-Ramsden & Douglas Burnett, *Submarine Cable Repair and Maintenance*, *in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 155, 158 (Douglas R. Burnett et al. eds., 2014).

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] ASIA PAC. ECON. COOP. POL'Y SUPPORT UNIT, ECONOMIC IMPACT OF SUBMARINE CABLE DISRUPTIONS 42 (2012), http://www.suboptic.org/uploads/Economic%20Impact%20of%20Submarine%20Cable%20Disruptions.pdf.

[180] Paul Saffo, *Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability,* ATL.

gard, intentional interference can take two potential forms. First is intentional damage to the physical infrastructure of submarine cable systems, namely, submarine cables laid on the seabed and cable landing stations.[181] The second type is an attack involving the virtual or cyber aspect of submarine cable systems, and the exploit would entail hacking into the cable network management systems used to operate cable systems and disrupting communications.[182] Both will be dealt with in greater detail below.

A. Intentional Damage to Submarine Cables and Cable Landing Stations

The U.S. Department of Defense listed the world's cable landing sites as among the most critical of infrastructures for the United States.[183] Cable landing sites are concentrated in a few geographic areas due to high expense and economies of scale.[184] According to one report, there are at least ten major cable chokepoints that exist globally.[185] As observed by one commentator:

> The most dangerous vulnerability is the aggregation of high-capacity bandwidth circuits into a small number of unprotected carrier hotels in which several hundred network operators interconnect their circuits in one non-secure building. These buildings often feed directly into the international undersea cable system. Security is often farcical. This lack of protection exists in several carrier hotels on transit points along the axis of the international telecommunications system that includes Dubai, Zurich, Frankfurt, London, New York, San Francisco, Los Angeles, Tokyo, Hong Kong and Singapore.[186]

Apart from cable landing sites, another vulnerability is the vast network of submarine cables on the seabed itself. Telecommunications companies "concentrate a large percentage of overall bandwidth in just a few major cable systems because new cable designs also incorporate tremendous capacity."[187] Cables also tend to be bundled together, "offering a potentially lucrative, consolidated target for sabotage."[188] If a bundle of cables are severed all at once, it could result in responders having little to no chance of restoring the connection by rerouting the traffic to mitigate the effects of the cut.[189] Due to the unpre-

---

COUNCIL (Apr. 4, 2013), http://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability.

181 Sechrist, *New Threats, supra* note 46, at 15.

182 *Id*.

183 *See* Mark Clayton, *WikiLeaks List of 'Critical' Sites: Is it a Menu for Terrorists?,* CHRISTIAN SCI. MONITOR (Dec. 6, 2010), http://www.csmonitor.com/USA/Foreign-Policy/2010/1206/WikiLeaks-list-of-critical-sites-Is-it-a-menu-for-terrorists.

184 Sechrist, *New Threats, supra* note 46, at 9.

185 *Id*.

186 Fonow, *supra* note 53, at 43-44.

187 Laurence Reza Wrathall, *The Vulnerability of Subsea Structure to Underwater Attack: Shortcomings and the Way Forward*, 12 SAN DIEGO INT'L L.J 223, 231 (2010).

188 *Id.* at 232.

189 *Id.* at 232, n.40.

dictable ocean environment, there are obvious challenges in actually carrying out an attack, however, a disruption could occur as a result of something as simple as dropping an anchor on a cable or sending a scuba diver down to physically cut them (all cable routes are publicly available).[190] Further, one scholar has pointed out the possibility of nefarious elements using an Unmanned Undersea Vehicle (UUV) to attack cables.[191]

The possibility of intentional damage to submarine cables is not as farfetched as it first appears. Indeed, from the Crimean War in the 1850s, the British were well aware of "the strategic importance of the telegraph network and its vulnerability to cable-cutting and other disruptions by hostile States."[192] Indeed, the first act of the British in World War I was to cut Germany's undersea telegraph cable that left Germany with just one cable, which was in any event under British control.[193] Germany retaliated by attempting to destroy Allied telegraph cables in the Pacific and Indian Oceans and attacking telegraph stations and cables at Fanning Island and the Cocos Island in 1914, starting the notorious cables wars.[194] Today, submarine cables are still legitimate targets during wartime (the 1884 Cable Protection Convention explicitly provides that obligations of protection contained in the Convention "do not in any way restrict the freedom of action of belligerents),[195] however, submarine cables between neutral countries, even during wartime, are inviolable and can not be seized or destroyed except in the case of absolute necessity.[196]

While there have been no large-scale attacks against cables since then, there have been isolated incidents of deliberate cable damage. For example, in March 2007, the Vietnamese military reported that a considerable amount of cable had been discovered on Vietnamese soil, that some vessels had been found with special cable cutting equipment and that cable coordinates were being sold illegally.[197] This was followed by the discovery that 500 kilometers

---

190 Beckman, *Protecting Submarine Cables, supra* note 11, at 283.

191 Wrathall, *supra* note 187, at 237-38.

192 Penney, *supra* note 65, at 704.

193 Elizabeth Bruton, *From Australia to Zimmermann: A Brief History of Cable Telegraphy During World War I*, at 1 (Sept. 20, 2013) (unpublished manuscript) (on file with author), http://blogs.mhs.ox.ac.uk/innovatingincombat/files/2013/03/Innovating-in-Combat-educational-resources-telegraph-cable-draft-1.pdf.

194 *Id.*

195 *See* 1884 Cable Convention, *supra* note 82, art. 15; John MacDonnell, *Recent Changes in the Rights and Duties of Belligerents & Neutrals According to International Law*, 17 J. ROYAL UNITED SERV. INST., July-Dec. 1898, at 915, 916 ("Her Majesty's Government takes Article 15 to mean that in time of war, a belligerent who is a a signatory to the Convention, will be free to act with respect to submarine cables, as if the Convention did not exist.").

196 Convention (IV) Respecting the Laws and Customs of War on Land, art. 54, Oct. 18, 1907, 36 Stat. 2277, 2308, T.S. No. 539.

197 Wrathall, *supra* note 187, at 244.

of cable, including an 11 kilometer segment of the SEA-ME-WE 3 cable system had been stolen.[198] Local authorities had apparently permitted fishermen to remove old undersea cables to sell its copper, but they had helped themselves to the newer cables.[199] This incident reportedly resulted in 82 percent of voice/data traffic lost, Internet delays for up to three months after thefts, and cost 5.8 million U.S. dollars to restore normal service.[200]

In November 2007, there was a report of the intentional sabotage of a cable in Bangladesh, which resulted in a total loss of communications for at least one week causing a loss of 1.05 million U.S. dollars in revenue by the Bangladesh Telegraph and Telephone Board.[201] In addition, there have also been reports of cable theft in Jamaica in 2008 where Cable and Wireless Jamaica lost 1.5 million dollars,[202] and a 2010 attack by separatists against the beach manhole connection of a submarine cable system linking the Philippines with Japan.[203] In March 2013, it was reported that 16 tons of submarine cables laid on the seabed between Bangka Island and the Riau Islands in Indonesia were stolen.[204] Perhaps more disturbingly is an incident that occurred in April 2013, when there were interruptions on multiple undersea communications cables that link Europe to the Middle East and Asia including I-ME-WE, TE North, EIG and SEA-ME-WE 3.[205] While initially chalked up to dragging ship anchors, the Egyptian coast guard caught three divers trying to cut the SEA-ME-WE-4 near Alexandria, although the motives of such an act remain unknown.[206]

As grimly observed by one commentator, if attacks on cable landing sites or cables themselves occur:

> …these cascading failures could immobilize much of the international telecommunications systems and internet for several weeks. The effect on international finance, military logistics, medicine, commerce and agriculture in a global economy would be profound. A degraded system of military logistics would leave troops in the field with less support. The international flow of oil and food supplies would be impeded. Chaos in the shipping and airline industries would result. The system that supports e-mail, Word and Excel file transfers would be gone. Electronic funds transfers, credit card

---

198 *See* Mick Green & Douglas R. Burnett, *Security of International Submarine Cable Infrastructure: Time to Rethink?, in* LEGAL CHALLENGES IN MARITIME SECURITY 557, 559-61 (Myron H. Nordquist et al. eds., 2008).

199 *Id.* at 562.

200 SECHRIST, DEEP WATER, *supra* note 49, at 40.

201 *Id.* at 38.

202 *Id.* at 40.

203 Douglas R. Burnett, *Cable Vision,* PROCEEDINGS, Aug. 2011, at 66, 69.

204 Fadli & Raras Cahyafitri, *Indosat Spends Rp 10 Billion Replacing Stolen Underwater Cable,* JAKARTA POST (June 29, 2013, 12:45 PM), http://www.thejakartapost.com/news/2013/06/29/indosat-spends-rp-10-billion-replacing-stolen-underwater-cable.html.

205 Saffo, *supra* note 180.

206 *Id.*

transactions and international bank reconciliations would slow to a crawl.[207]

B. Interference with Network Management Systems

In order to drive down costs by reducing personnel and management expenses, the cable industry has employed Network Management Systems (NMS) to remotely connect cable systems, landing stations, spare depots and other cable system components.[208] As one scholar observed, while "[c]onnecting cable sites with software creates more efficiency and provides operators greater operational awareness…it creates potential new risk, particularly to cyber attacks."[209] The worse case scenario is if hackers hack into a NMS, gain control of multiple cable management systems, and "attain unprecedented top-level views of multiple cable networks and data flows, discover physical cable vulnerabilities, and disrupt and divert data traffic."[210] An incident akin to this occurred in 2010, when the Stuxnet worm, a cyber weapon reportedly developed to target Iran nuclear facilities, disrupted the operation of specific plant processes that were controlled by Siemens-manufactured industrial control systems.[211]

C. Gaps in the Existing Law Governing the Protection of Submarine Cables

The next question is: what role can international law play in addressing the above-mentioned threats to submarine communications cables? There are several instruments in international law that could potentially be utilized, but the existing legal framework is fragmented and is not capable of ensuring the security of this vital communications infrastructure.

1. The Law of the Sea

The natural starting point is the law of the sea, as reflected in UNCLOS. As previously discussed, in territorial waters, i.e. waters under the sovereignty of the coastal State, coastal States have the power to adopt laws to protect submarine cables, even going as far as to regulate the innocent passage of foreign vessels through territorial waters.[212] Further, UNCLOS recognizes the follow-

---

207 Fonow, *supra* note 53, at 44.
208 *See* Sechrist, *New Threats, supra* note 46, at 12.
209 *Id.* at 8.
210 *Id.* at 13.
211 Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem,* 42 GEO. J. INT'L L. 971, 972-73 (2010).
212 UNCLOS, *supra* note 85, art. 21, ¶ 1(c).

ing activities are "prejudicial to the peace, good order or security of the State" and are thus prohibited in territorial waters:[213]

> Any act aimed at collecting information to the prejudice of the defense or security of the coastal State;
>
> Any act of propaganda aimed at affecting the defense or security of the coastal State;
>
> Any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State.[214]

In the event that a vessel is found to be engaging in the above activities, passage is rendered non-innocent, and coastal States can take the necessary steps to prevent this passage.[215] Prima facie, these provisions give coastal States the basis to take measures to protect submarine cables from intentional damage. However, these provisions do not oblige States to take such measures, and many States do not have sufficient laws and regulations to protect cables from intentional damage within territorial waters, including the most basic measure of ensuring that damage to submarine cables is criminalized.[216]

In areas outside of territorial waters, namely the EEZ and the high seas, Article 113 applies. To recapitulate, Article 113 of UNCLOS requires States to adopt laws and regulations to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done willfully or through culpable negligence is a punishable offense.[217] While Article 113 could in principle cover intentional damage to the cable network, it has several limitations that render it ineffective at addressing these threats. First, many States Parties to UNCLOS have not implemented their obligation under Article 113 to extend criminal jurisdiction over acts committed on the high seas or EEZ.[218] The States that have implemented Article 113 are usually implementing their obligations under the 1884 Cable Convention; meaning their legislation has not been updated and the penalties are

---

213 *Id.* art. 19, ¶ 2(c)-(d).

214 *Id*.

215 *Id.* art. 25, ¶ 1.

216 For example, the U.S. had at one time only imposed a maximum penalty of only $5000 for willful injury to submarine cables. *See* Scott Coffen-Smout & Glen J. Herbert, *Submarine Cables: A Challenge for Ocean Management,* 24 MARINE POL'Y 441, 444 (2000). "This insignificant maximum criminal penalty provides little incentive for enforcement authorities to assign full time legal and investigative personnel to prosecute vessel owners caught damaging a submarine cable," and would not even begin to cover the costs of repairs. *Id*.

217 UNCLOS, *supra* note 85, art. 113.

218 Tara Davenport, Research Fellow, Ctr. for Intl. Law, The Criminalization of Damage to Submarine Cables: Problems and Prospects 5 (2010) (unpublished presentation) (on file with the National University of Singapore Centre for International Law), http://cil.nus.edu.sg/wp/wp-content/uploads/2012/04/TaraDavenport-Criminalization-of-Damage-to-Submarine-Cables.pdf.

consequently woefully inadequate.[219] The most common penalty in national legislation for intentional damage to cables is a monetary penalty,[220] which is arguably not commensurate with the damage resulting from intentional interference with cable systems.

Second, jurisdiction under Article 113 is limited to perpetrators who are nationals of that State, or if they use a vessel flying the flag of that State.[221] Given the critical nature of submarine communications cables there is a strong argument that intentional damage is a crime that attracts universal jurisdiction and that all States should have jurisdiction over the offender. At the very least, the State(s) whose communications have been disrupted should have jurisdiction to prosecute as well as the State on whose continental shelf the damaged cable is located.[222]

Third, Article 113 only obliges States to adopt laws criminalizing intentional damage, and neither gives warships the right to board, nor arrest a vessel suspected of intentionally breaking a cable.[223] Generally speaking, due to concerns about unnecessary interference with the freedom of navigation, the right to board vessels in areas outside the territorial sea (i.e. EEZ/high seas) is highly regulated under UNCLOS and is only allowed in certain instances.[224] States have opposed a right to board without the consent of the flag states even for the suppression of the most serious crimes.[225] However, there is some merit in the argument that warships of all States should have the right to board vessels suspected of intentionally breaking a cable. For example, Article X of the 1884 Cable Convention allows warships to require the master of a vessel suspected of having broken a cable to provide documentation to show the ship's nationality and thereafter to make a report to the flag state.[226] This provides an effective

---

[219] For example, the penalty in the United States is $5000 for willfully breaking a submarine cable. 47 U.S.C. § 21 (2012). In Australia, the fine is set at $2000 for intentional breaking. *Submarine Cables and Pipelines Protection Act 1963* (Cth) s 7 (Austl.). In New Zealand, the fine was set at substantially higher at $250,000. Submarine Cables and Pipelines Protection Act 1996, s 11 (N.Z.).

[220] COMMC'NS SEC, RELIABILITY, & INTEROPERABILITY COUNCIL, PROTECTION OF SUBMARINE CABLES THROUGH SPATIAL SEPARATION 53 (2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf.

[221] UNCLOS, *supra* note 85, art. 113; Davenport, *Submarine Cables, supra* note 106, at 218.

[222] UNCLOS, *supra* note 85, art. 113; Davenport, *Submarine Cables, supra* note 106, at 220.

[223] UNCLOS, *supra* note 85, art. 113.

[224] Article 110 of UNCLOS provides that the right to board exists when there are reasonable grounds for believing that the ship engaged in piracy, the slave trade, engaged in unauthorized broadcasting, or that it is without nationality or flying the same flag as the boarding war ship. *See id*. art. 110, ¶ 1.

[225] *Id.* art. 110, ¶ 2.

[226] 1884 Cable Convention, *supra* note 82, art. 10.

deterrent to prospective attacks.

Some scholars have argued that intentional damage to cables could fall within the definition of piracy under UNCLOS.[227] Article 101 defines piracy as, "any illegal acts of violence or detention or any act of depredation, committed for private ends by the crew or the passengers of a private ship, or a private aircraft, and directed . . . on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft . . . against a ship, aircraft, persons or property in a place outside the jurisdiction of any State."[228] The advantage of deeming intentional damage to cables as a piratical act is that it would be subject to universal jurisdiction and gives all warships the right to board and arrest a suspected vessel.[229] However, it would certainly be a strained interpretation due to the requirement under the definition of piracy that two vessels be involved, and that it be done for private ends/commercial purposes.[230]

Fourth, UNCLOS only applies to the portion of cable that is laid on the seabed and does not apply to attacks against cable landing sites.[231]

2. The Law of Cyberattack

There is no accepted definition of what constitutes a "cyberattack," and indeed this term has been used interchangeably with cyber-warfare and cybercrime.[232] The U.S. Department of Defense's Dictionary of Military Terms defines "computer network attack" ("CNA") as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[233] The North Atlantic Treaty Organization ("NATO") also adopts this

---

[227] Beckman, Critically Important, *supra* note 148, at 15; *see generally* Travers Twiss, The International Protection of Submarine Telegraph Cables, Address Before the Association for the Reform & Codification of the Law of Nations (Aug. 24, 1880), *in* REPORT OF THE EIGHTH ANNUAL CONFERENCE HELD AT BERNE, AUGUST 24TH – 27TH, 1880, at 98, 99 (1880) ("The [U.S. Government] took the initiative by making a proposal upon this question in the year 1869, when it expressed a desire that a diplomatic conference should meet at Washington to consider a draft international convention; but the Franco-German war supervened and put an end to the project.").

[228] UNCLOS, *supra* note 85, art. 101.

[229] *Id.* art. 105.

[230] Wrathall, *supra* note 187, at 247-48.

[231] *See* UNCLOS, *supra* note 85, arts. 2-16.

[232] *See* Hathaway et al., *supra* note 3, at 823; *but see* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 106 (Michael N. Schmitt ed. 2013) ("A cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.").

[233] CHAIRMAN OF THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.1, ELECTRONIC WARFARE, at GL-6 (2007), http://fas.org/irp/doddir/dod/jp3-13-1.pdf.

definition but adds that "a computer network attack is a type of cyber attack."[234] The Joint Chiefs of Staff have defined network warfare as:

> [T]he employment of Computer Network Operations (CNO) with the intent of denying adversaries the effective use of their computers, information systems, and networks, while ensuring the effective use of our own computers, information systems, and networks. These operations include Computer Network Attack (CNA), Computer Network Exploration (CNE) and Computer Network Defense (CND).[235]

The U.S. National Research Council defines cyber-attacks as "deliberate actions to alter, disrupt, deceive, degrade or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[236] Some suggest an objective-based definition of cyberattack: "[a] cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose."[237]

Under any of the above definitions, an intentional attack on submarine cables laid on the seabed, on cable landing sites, and on the network management systems that operate cable systems, would constitute a cyber-attack.[238] The next question is whether international law applies to cyber-attacks and if it does, does it provide an effective framework that protects the security of submarine cables.

There has been much debate on whether and to what extent international law applies to cyber- attacks. After all, unlike traditional battle domains:

> [C]yberspace is the only domain which is entirely man-made. It is created, maintained, owned and operated collectively by public and private stakeholders across the globe and changes constantly in response to technological innovation. Cyberspace not being subject to geopolitical or natural boundaries, information and electronic payloads are deployed instantaneously between any point of origin and any destination connected through the electromagnetic spectrum . . . While cyberspace is readily accessible to governments, non-state organizations, private enterprises and individuals alike, IP spoofing and the use of botnets, for example, make it easy to disguise the origin of an operation, thus rendering the reliable identification and attribution of cyber activities particularly difficult.[239]

This highlights one of the central difficulties in developing an adequate legal

---

234 N. ATL. TREATY ORG., AAP-6, NATO GLOSSARY OF TERMS AND DEFINITIONS, at 2-C-12 (2008), http://fas.org/irp/doddir/other/nato2008.pdf.

235 JEFFREY CARR, INSIDE CYBER WARFARE 176 (Mike Loukides ed., 1st ed. 2009) (citing CHAIRMAN OF THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS (2006)).

236 NAT'L RES. COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009).

237 Hathaway et al., *supra* note 3, at 826.

238 *Id.* at 827 ("Using a regular explosive to sever the undersea network cables that carry information packets between continents . . . is a cyber-attack.").

239 NILS MELZER, U.N. INST. FOR DISARMAMENT RES., CYBERWARFARE & INTERNATIONAL LAW 5 (2011), http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

framework to govern a cyber-attack that has challenged international law, namely the fact "the speed and anonymity of cyberattacks makes proving State responsibility and 'distinguishing among the actions of terrorists, criminals and nation states difficult.'"[240]

Experts and scholars alike have struggled with what international law applies to cyberattacks. For example, from its inception in 2004, the United Nations' Governmental Group of Experts ("GGE") on Developments in the Field of Information and Telecommunications in the Context of International Security debated over whether international law applied to the use of information and communication technologies by States.[241] In particular, there was disagreement on whether the laws of war, namely *jus ad bellum* (when it is appropriate to go to war) and *jus in bello* (principles governing the way in which war is conducted) applied to cyberattacks.[242] That said, in September 2012, the U.S. Department of State Legal Advisor, Harold Koh, confidently asserted that established principles of the international laws of war apply to cyberspace.[243] In June 2013, the GGE stated, "[i]nternational law, and in particular the Charter of the United Nations, is applicable, and is essential in maintaining peace and stability and promoting an open, secure and peaceful and accessible ICT environment."[244] While there is no doubt that certain bodies of international law can be used to deal with cyber-attacks, it is piecemeal and fragmented, and by no means comprehensively addresses the security challenges posed by cyber-attacks.[245]

In the context of intentional damage to submarine cables, cable landing sites and interference with network management systems, which involve both physical infrastructure and virtual space, the laws of war can fill some of the gaps. *Jus ad bellum* determines when the use of force is justified.[246] As a starting point, Article 2 ¶ 4 of the U.N. Charter provides that Member States "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other man-

---

[240] Shackelford & Andres, *supra* note 211, at 974 (quoting DAVID HELD, MODELS OF DEMOCRACY 293-97 (2006)).

[241] G.A. Res. 58/62, ¶ 4 (Dec. 18, 2003).

[242] *See* U.N. Secretary-General, *Developments In the Field of Information and Telecommunications In the Context of International Security,* U.N. Doc. A/66/152, at 35-37 (July 11, 2011).

[243] Harold Hongju Koh, U.S. Dep't of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.

[244] Rept. of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 8, para. 19, U.N. Doc. A/68/98 (June 24, 2013).

[245] Hathaway et al., *supra* note 3, at 821.

[246] INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW: ANSWERS TO YOUR QUESTIONS 8 (2015), https://www.icrc.org/eng/assets/files/other/icrc-002-0703.pdf.

ner inconsistent with the [p]urposes of the United Nations."[247] This is reinforced by the customary international law principle of non-intervention in the internal affairs of States.[248] There are two exceptions to the prohibition on the use of force. Article 39 of the Charter allows the Security Council to authorize collective security operations in response to threats to the peace, breach of peace or an act of aggression.[249] Article 51 provides that States have the inherent right of individual or collective self-defense if an armed attack occurs.[250] Thus, in the event that intentional interference with submarine cable systems amount to a "threat to international peace and security or an act of aggression,"[251] (as determined by the Security Council), the Security Council can authorize a use of force against that State. Similarly, if intentional interference with submarine cable systems amounts to an "armed attack,"[252] a State or States have the right of self-defense.

While this is of course important, these principles do not effectively address the protection of this critical communications infrastructure. First, such attacks would have to amount to a "threat to international peace and security" or an "armed attack" before the Security Council and/or States can take action.[253] This may prove to be particularly difficult for intentional infiltration against the network management systems of submarine cables, in which there may be no physical manifestation. Second, it assumes that the perpetrators of such attacks are easily identifiable, and does not address intentional damage to cable systems committed by non-State actors. Third, a State's use of force in response to an armed attack in the form of intentional interference with cable systems must also comply with *jus ad bellum* principles of necessity and proportionality under customary international law.[254] Necessity requires that force must only be used as a last resort when diplomatic means fail and proportionality requires that responses cannot be excessive. This circumscribes the response that States can take. "[C]yber-attacks rising to the level of armed attacks may require decision-makers to devise ways of measuring harm to computer networks and its indirect effects against more conventional kinds of harm

---

247 U.N. Charter art. 2, para. 4.

248 *See* G.A. Res. 25/2625 (XXV), at 123 (Oct. 24, 1970); *see also* G.A. Res. 37/10, Manila Declaration on the Public Settlement of International Disputes (Nov. 15, 1982).

249 U.N. Charter art. 39.

250 *Id.* arts. 40-42, 51.

251 *Id.* art. 39, para. 1.

252 *Id.* art. 51, para. 1.

253 Hathaway et al., *supra* note 3, at 843-48 (comprehensively discussing the difficulties of establishing that an act is a threat to peace and security or armed attack thus warranting the use of collective action and the right of self-defense).

254 *Id.* at 849.

in order to determine what would constitute a lawful response."[255]

Apart from the laws of war, international telecommunications law may also address cyberattacks, including intentional damage to cable systems. The ITU is the leading U.N. agency that establishes international standards for information and communication technology.[256] The organization is primarily concerned with allocating global radio spectrum and satellite orbits, and developing technical standards to ensure that networks and technologies seamlessly interconnect.[257] The ITU has issued some regulations and standards that could apply to cyber-attacks which make use of electromagnetic spectrum or international telecommunications networks, but none of these directly implicate the protection of cables systems from intentional damage.[258]

3. Terrorism Conventions

There are existing counter-terrorism conventions that could apply to intentional attacking cable systems. For example, the International Convention for the Suppression of Terrorist Bombings adopted in 1997 provides that it is an offense to unlawfully and intentionally use an explosive or lethal device against an infrastructure facility with the intent to cause extensive destruction of such facility or where such destruction results in or likely to result in major economic loss.[259] An "infrastructure facility" is defined as "any publicly or privately owned facility providing or distributing services for the benefit of the public such as water, sewage, energy, fuel or communications."[260] However, this is restricted in its effectiveness as it would only apply to cable landing sites destroyed as a result of bombing and not necessarily to actual cables destroyed by another method. It would also not apply to attacks on the NMS of cable facilities.

D. The Way Forward: An International Treaty

The above discussion amply illustrates that presently that while there is a patchwork of international laws that could theoretically address certain aspects of the security of cable systems, there are significant gaps. Given the potential severe ramifications of intentional damage to global economy and security, as well as the complexity of regulating something that inherently transnational in

---

255 *Id*.
256 *See About ITU, supra* note 1.
257 *Id.*
258 Hathaway et al., *supra* note 3, at 866-67.
259 International Convention for the Suppression of Terrorist Bombings art. 2, ¶ 1, Dec. 15, 1997, 2149 UNTS 256 (entered into force May 23, 2001).
260 *Id.* art. 1, ¶ 2.

nature, international cooperation between States in the form of an international multilateral treaty on the protection of submarine cable systems appears to be the best way forward.

This would no doubt be a complex endeavor in view of the fact that protecting a submarine cable system involves the virtual, land, and sea domains, and consequently, a cross-section of international and national agencies as well as a variety of experts from different fields. However, as will be illustrated below, a useful starting point is to use the structure of the terrorism conventions.[261]

First, the international treaty should define a range of offenses which would include intentional damage to cable landing sites, land cables and submarine cables provided that they are part a submarine cable system. Moreover, it should also include the offense of using malware to take control of network management systems for the purpose of disrupting communications.

Second, the treaty should oblige State Parties to ensure that these offenses are reflected in national legislation punishable with commensurate penalties.

Third, States Parties should also be required to establish jurisdiction over the offenses defined in the convention when they have a link or connection to the offense because the act took place within their territory, or was committed by their national, or from a ship flying their flag.[262]

Fourth, State Parties should also be required to establish jurisdiction over the offense when the alleged offender is "present in their territory" and the State chooses not to extradite them. This requires States to enact legislation which give their courts jurisdiction to try the offender, even though the offense was committed by a foreign national outside their territory, so long as the offender is physically present in their territory.[263]

Fifth, if the alleged offender is present in their territory, State parties should have a legal obligation to take them into custody and to ensure their presence in their territory. The State then has only two choices: it must either extradite the alleged offender or prosecute them. The State can extradite the alleged offender to another State party that has jurisdiction, such as the State of nationality of the offender, the State in whose territory the offense was committed, or the State on whose ship the offense was committed. If they elect not to extradite the alleged offender, the State's only option is to prosecute the offender in their courts.[264]

Sixth, the convention should include provisions that make it possible to extradite alleged offenders to other State parties, even in the absence of an extra-

---

261 Beckman, Critically Important, *supra* note 148, at 14.
262 *Id.*
263 *Id.*
264 *Id.*

dition treaty between the two countries.[265]

Seventh, the convention should contain provisions that require State parties to provide mutual legal assistance to assist the State where the alleged offenders are prosecuted. The legal assistance would include matters such as providing evidence or witnesses.[266]

The first question is whether States have the necessary political will to negotiate such a convention. Indeed, it is surprising that such a treaty has not been negotiated as yet given the critical importance of submarine cables and how other conventions have been adopted for airport and maritime infrastructure.[267] There are several possible reasons for this. First, there is a lack of awareness about the importance of cables to the international telecommunications system. Evidence about the lack of awareness is highlighted by the common misconception that the Internet and other web-based technologies are provided by satellite.

Second, unlike other public infrastructure that has received protection under international treaties, the cable industry has been driven by private investment and companies.[268] Governments have very little involvement in the construction and management of cables, and have thus always perceived cable systems as a problem for the private sector.[269]

Third, there is also no international intergovernmental organization responsible for submarine cables and thus nobody is advocating for its protection on the international level.[270] The ITU, as mentioned above, would seem the most relevant agency but is unaware about the marine portion of submarine cables. The ICPC is an industry based organization representing the industry although it recently began to admit States as members.[271]

In this regard, the best forum to raise the protection of submarine cables would appear to be the United Nations efforts to address cyber security con-

---

265 *Id.*

266 *Id.*

267 *See, e.g.*, The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, 1589 UNTS 474 (entered into force Aug. 6, 1989).

268 Douglas R. Burnett, International Law Advisor, Int'l Cable Prot. Comm., Economic, social, and environmental aspects of submarine cables, Presentation Before the 16th Meeting of the United Nations Open-ended Informal Consultative Process on Oceans and the Laws of the Sea 6 (Apr. 7, 2015), http://www.un.org/depts/los/consultative_process/icp16_presentations/Burnett.pdf.

269 *Id*.

270 DOUGLAS R. BURNETT ET AL., INT'L SEABED AUTH., ISA TECH. STUDY NO. 14, SUBMARINE CABLES AND DEEP SEABED MINING: ADVANCING COMMON INTERESTS AND ADDRESSING UNCLOS "DUE REGARD" OBLIGATIONS 17 (2015), http://www.squirepattonboggs.com/~/media/files/insights/publications/2015/08/submarine-cables-and-deep-seabed-mining/techstudy14_final_web.pdf.

271 CARTER ET AL., *supra* note 9, at 25.

cerns. There have been two GGEs that have examined the existing and potential threats from the cyber-sphere, first in 2004 and second in 2009.[272] The Report of the 2009/2010 recommended, amongst other things, dialogue on norms for State use of information and communications technologies to reduce risk and protect critical infrastructure.[273] Indeed, in its most recent Report issued in 2015, it has been reported that the GGE has adopted several norms that include understandings that nations should not intentionally damage each other's critical infrastructure with cyber attacks; should not target each other's cyber emergency responders; and should assist other nations investigating cyberattacks and cybercrimes launched from their territories.[274] While it is not clear whether the protection of submarine cable systems has come up during discussions, it certainly provides an appropriate platform to discuss such issues.

IV. SUBMARINE CABLES: A TOOL FOR INTELLIGENCE-GATHERING?

Frequently described as the second oldest profession,[275] espionage has existed since time immemorial, leading Hugo Grotius to write in the 17th Century that "there is no doubt, but the law of nations allows anyone to send spies, as Moses did to the land of promise, of whom Joshua was one."[276] The concept of peacetime espionage or intelligence gathering "encompasses a wide range of clandestine government activities"[277] with the objective of ensuring that "as much as possible is known in advance of any particular course of action being taken."[278] Arguably, intelligence gathering is one of the lesser-known uses of the submarine cable network.[279] While the practice remains unsurprisingly

---

[272] *See* U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* ¶ 5, U.N. Doc. A/60/202 (Aug. 5, 2005); *see also* Rep. of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶¶ 4-11, U.N. Doc. A/65/201, (July 30, 2010) [hereinafter 2009 GGE Rep.].

[273] 2009 GGE Rep., *supra* note 272, ¶ 18.

[274] *See* Rep. of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶¶ 13(d), 13(f), 13(k) , U.N. Doc. A/70/174 (July 22, 2015).

[275] For example, *see* Paul Reynolds, *The World's Second Oldest Profession,* BBC NEWS (Feb. 26, 2004, 5:01 PM) http://news.bbc.co.uk/2/hi/americas/3490120.stm.

[276] HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE, INCLUDING THE LAW OF NATURE AND NATIONS 331 (1901).

[277] Ashley Deeks, *An International Legal Framework for Surveillance,* 55 VA. J. INT'L L. 291, 298 (2015).

[278] NATALIE KLEIN, MARITIME SECURITY AND THE LAW OF THE SEA 214 (2011)

[279] Khazan, *supra* note 13.

shrouded in mystery, there appear to be two ways in which submarine cables have been used for intelligence gathering purposes, first by placing a recording device on undersea cables (hereinafter referred to as "underwater surveillance") and the tapping of undersea cables for purposes of collecting the data that passes through them.[280] Each will be dealt with in detail below.

A. Underwater Surveillance

A vital component of maritime security is ensuring that States have all the available information at their disposal to take preventative or responsive action.[281] As observed by Klein:

> [I]ntelligence gathering at sea has predominantly concerned the pursuit of information that may prove useful for a state's national security. In other words, what does a state need to know about the maritime areas of another state, or what may otherwise be learned about a state (including its defensive or aggressive capacity) from the water surrounding it? This intelligence enables states to make decisions about their own national defence.[282]

The United States has described intelligence gathering in ocean spaces as Maritime Domain Awareness ("MDA"), which is "the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy or environment of the United States,"[283] in order to "facilitate timely, accurate decision-making so as to enable actions that neutralize threats to US national security interests."[284] Maritime intelligence collection really began to gain traction in World War II where maritime signal intelligence gathering ("SIGINT") and maritime electronic intelligence gathering ("ELINT") were developed and employed.[285] Ships were increasingly seen as "modern intelligence-gathering platforms" tasked with gathering communications and electronic intelligence.[286] There now exist a plethora of technologies that are utilized for maritime intelligence gathering, including "radar, sonar and laser technologies; electro-optical, oceanographic, hydrographic, acoustic, geophysical and geospatial sensing; satellite spot-beam and microwave relay

---

280 *Id.*

281 KLEIN, *supra* note 278, at 212, 214.

282 *Id.* at 214-15.

283 WHITE HOUSE, NATIONAL PLAN TO ACHIEVE MARITIME DOMAIN AWARENESS FOR THE NATIONAL STRATEGY FOR MARITIME SECURITY 2 (2013), https://www.whitehouse.gov/sites/default/files/docs/national_maritime_domain_awareness_plan.pdf.

284 *Id.* at 10.

285 Asaf Lubin, The Dragon-Kings Restraint: Proposing a *Jus Ad Bellum* Model for the EEZ Surveillance Conundrum 2 (unpublished manuscript) (on file with author).

286 Judson Knight, *Ships Designed for Intelligence Collection*, ENCYC. OF ESPIONAGE, INTELLIGENCE, & SEC., http://www.faqs.org/espionage/Se-Sp/Ships-Designed-for-Intelligence-Collection.html (last visited Nov. 15, 2015).

traffic interception systems; airborne and ship-based maritime communication surveillance, and electronic warfare ("EW") capabilities; and more recently, long-endurance reconnaissance Unmanned Aerial Vehicles ("UAVs")."[287]

Submarine coaxial cables, now just submarine cables, also provided an opportunity for maritime intelligence gathering. In the late 1950s, the Office of Naval Research funded the American Telephone and Telegraph Company ("AT&T") to develop an undersea surveillance system designed to detect and track Soviet submarines.[288] By "setting up multiple listening posts – arrays of hydrophones strung along lengths of cabling – at strategic choke points like the GIUK gap, the U.S. Navy would be able to triangulate and track the locations of otherwise deep-diving Soviet subs."[289] This system was known as Sound Surveillance System ("SOSUS") and was viewed as "a key, long-range early warning asset for protecting the United States against the threat of Soviet ballistic missile submarines…and also provided vital cueing information for tactical, deep-ocean anti-submarine warfare.[290] The hydrophones were connected by cables to processing centers located on shore known as Naval Facilities.[291] At the height of the Cold War in the 1970s, the U.S. Government launched Operation Ivy Bells, which involved deploying submarines and combat divers to place waterproof hydrophones on the undersea cable that ran parallel to the Kuril Islands off Russia.[292] SOSUS was eventually supplemented by surface-based listening posts and subsequently integrated into the larger Integrated Undersea Surveillance System ("IUSS").[293] The Russians discovered the project in 1981 when NSA employee Ronald Pelton sold information about the program to the KGB for $35,000.[294] They then began to develop quieter submarines and by the end of the Cold War, the ability of IUSS to detect and track Soviet nuclear submarines had considerably diminished,[295] and the end of the

---

287 Lubin, *supra* note 285, at 2.

288 Edward C. Whitman, *SOSUS, The "Secret Weapon" of Undersea Surveillance,* 7 UNDERSEA WARFARE, no. 2, Winter 2005, http://www.public.navy.mil/subfor/underseawarfaremagazine/Issues/Archives/issue_25/sosus.htm.

289 Andrew Tarantola, SOSUS: The US Navy's Long-Range Undersea Ears for Spotting Soviet Subs, GIZMODO (June 12, 2014, 11:40 AM), http://gizmodo.com/sosus-the-us-navys-long-range-undersea-ears-for-spotti-1588077646. "GIUK" is the channels between Greenland, Iceland and the UK. Whitman, *supra* note 288.

290 J. Ashley Roach, Military Cables, *in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 338, 340 (Douglas R. Burnett, et al. eds., 2014).

291 Whitman, *supra* note 288.

292 Khazan, *supra* note 13.

293 *Id*.

294 *Id.*

295 Whitman, *supra* note 288.

Cold War reduced the necessity for such a system.[296] That said, it has been reported that "growing concerns of China's rising naval power and Russia's renewed aggression have the Navy's Space and Naval Warfare Systems Command (SPAWAR) propositioning to commercial ventures and defense contractors alike for a new generation of deep water listening stations."[297] While the initial SOSUS used submarine cables specifically constructed for intelligence gathering, it is not clear whether a new generation of underwater listening stations would use the existing submarine fiber optic network. The latter possibility appears to be more unlikely, given the industry's concern with preserving the integrity of global telecommunications.[298] Moreover, the military would likely own and operate an underwater listening system using its own submarine cable network, rather than commercially owned ones.

SOSUS provided the foundation for cables to be used by scientists for marine data collection. During the Cold War, the U.S. Navy permitted a small number of oceanographers to make use of the SOSUS system for research.[299] The Navy's action fueled further research into how submarine cables could be used for scientific purposes, and as mentioned above, submarine cables are now used for deep-ocean monitoring.[300] This involves equipping submarine communications with scientific sensors for climate monitoring and disaster reduction.[301] These scientific sensors would collect key measurements relevant to climate change and disaster detection such as temperature, pressure, salinity/conductivity, seismic, hydroacoustic, and cable voltage.[302] The scientific sensors are placed within the repeaters found on submarine cables every 60 to 100 kilometers.[303] There are three ways in which submarine cables can be integrated into real-time global climate and disaster monitoring systems. First, by

---

296 *Id.*

297 Tarantola, *supra* note 289.

298 For example, the cable industry has expressed concern at scientific sensors being placed on existing submarine fiber optic networks may undermine the reliability of the communication network which always remains its first priority. *See* BURNETT, WORKSHOP REPORT, *supra* note 41, at 24-26.

299 *The Cold War: History of the SOund SUrveillance System (SOSUS),* DISCOVERY OF SOUND IN THE SEA, http://www.dosits.org/people/history/SOSUShistory/ (last visited Oct. 15, 2015).

300 *See generally* Davenport, *A New Frontier, supra* note 10, at 243-45.

301 *See generally* STEPHEN LENTZ & PETER PHIBBS, INT'L TELECOMM. UNION, USING SUBMARINE CABLES FOR CLIMATE MONITORING AND DISASTER WARNING: ENGINEERING FEASIBILITY STUDY 2-3 (2012), http://www.itu.int/dms_pub/itu-t/oth/4B/04/T4B040000170001PDFE.pdf.

302 BUTLER, *supra* note 62, at 3.

303 BURNETT ET AL., WORKSHOP REPORT, *supra* note 41, at 24. Repeaters are used to amplify the optical signals over long distance. YUZHU YOU, INT'L TELECOMM. UNION, USING SUBMARINE COMMUNICATIONS NETWORKS TO MONITOR THE CLIMATE 4 (2010), http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000110003PDFE.pdf

re-using out of service cables.[304] Second, another suggestion has been to attach sensors and related components to in-service communications cables.[305] The third option is the development of a new generation of multi-purpose cables.[306] This would entail redesigning the repeaters that are integrated with built-in sensors that would enable climate monitoring and disaster detection.[307]

B. UNCLOS

Before addressing the applicable provisions in UNCLOS in detail, a few salient points should be mentioned. First, except for one provision in Part II on the territorial sea,[308] intelligence gathering is not explicitly mentioned in UNCLOS. It only occasionally came up in during the negotiations of UNCLOS as part of a larger debate on the permissibility of military activities[309] in the oceans and was never the object of formal negotiations[310] due to the belief of many States, that this would rapidly derail any efforts to come to an agreement on a convention.[311] However, the issue of military activities including intelligence gathering was always hovering in the background and shaped the way in which many of the provisions were drafted, particularly in the EEZ.[312] After all, the maritime powers wanted to preserve their ability to move freely around the

---

304 Cables usually have a life span of 20 – 25 years, and a large quantity of first-generation fiber optic cables were retired before the end of its lifespan due to such cables becoming outdated in the face of new cable technology. YOU, *supra* note 303, at 2.

305 Yuzhu You, *Multipurpose Submarine Cable Repeaters: Required to Monitor Climate Change*, 54 SUBTEL FORUM, Nov. 2010, at 7, 8-9, http://www.subtelforum.com/issues/STF_54.pdf. "Slight modification of these repeaters – plugging in only one pressure sensor into their housing, for example – could turn the single purpose telecommunication network into multi-purpose, real-time global tsunami and sea-level rise monitoring network." *Id.*

306 BUTLER, *supra* note 62, at 18.

307 YOU, *supra* note 305, at 10.

308 UNCLOS, *supra* note 85, art. 19, ¶ 2(c) (stating that "any act aimed at collecting information to the prejudice of the defense or security of the coastal State" is deemed prejudicial to the peace, good order or security of the coastal State and renders passage non-innocent).

309 *See* KLEIN, *supra* note 278, at 43. Military activities cover a range of activities, "from intelligence gathering, to training of forces, testing and use of vessels and equipment and installations, to weapons tests and military engagements either short of or amounting to armed conflict." *Id.*

310 FRANCISCO ORREGO VICUNA, THE EXCLUSIVE ECONOMIC ZONE: REGIME AND LEGAL NATURE UNDER INTERNATIONAL LAW 108 (1989).

311 *See* Capt. George V. Galdorisi & Comm. Alan G. Kaufman, *Military Activities in the Exclusive Economic Zone: Preventing Uncertainty and Defusing Conflict*, 32 CAL. W. INT'L L. J. 253, 272 (2002).

312 VICUNA, *supra* note 310, at 108-09.

oceans and to defend national security interests.[313] Coastal States, on the other hand, were naturally wary of the navies of third States operating in areas near their coasts and perceived such activities as prejudicial to their national security.[314] Ultimately, the Convention is largely silent on this issue, and as will be demonstrated below, this has resulted in a considerable amount of uncertainty and ambiguity on whether intelligence gathering is permitted under UNCLOS.

The next three sections will discuss the UNCLOS regime on intelligence gathering in three major maritime zones, the territorial sea, the EEZ and the high seas, and how it relates to the construction of an underwater listening station either by laying new cables on the seabed specifically for this purpose or by placing recording devices on an existing cable telecommunications network.

1. Territorial Seas

Within the territorial sea, the coastal state controls and authorizes the laying of cables and any activity associated with it.[315] Further, it is very clear that any intelligence gathering by third States is prohibited. As noted in Part II, the territorial sea is a zone in which the coastal State has sovereignty, and this is only constrained by the coastal State's obligation to allow foreign flagged vessels innocent passage.[316] Passage is innocent provided it is not prejudicial to the peace, good order, or security of the coastal State.[317] Research and survey activities "are any act aimed at collecting information to the prejudice of the defense or security of the coastal State," and "any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State," and "any activity not having a direct bearing on passage" will render passage non-innocent.[318] Clearly, the establishment of underwater listening stations using cables would fall foul of the above prohibitions.[319]

2. Exclusive Economic Zone

As mentioned above, the EEZ is neither under the sovereignty of the coastal

---

313 James Kraska, *The Law of the Sea Convention: A National Security Success—Global Strategic Mobility Through The Rule of Law*, 39 GEO. WASH. INT'L L. REV. 543, 547 (2007).

314 *Id.* at 554-55.

315 UNCLOS, *supra* note 85, art. 2.

316 *Id.* art. 17.

317 *Id.* art. 19, ¶ 1.

318 *See id*. art. 19, ¶¶ 2(c), 2(k), 2(l).

319 Although one could argue that the placement of such devices is not an interference with any systems of communications or any other facilities or installations of the coastal State.

State nor part of the high seas, but is a special *sui generis* regime[320] where the coastal State has rights and jurisdiction over resources and certain other activities[321] to be balanced with the traditional high seas freedoms afforded to other States.[322]

There are several arguments both for and against the legality of using submarine cables for intelligence gathering, many of which are part of the larger debate between States such as the United States and China on the legality of military activities generally.[323] The academic discourse on the legality of military activities generally, which can be somewhat polemic, is vast and not possible to comprehensively canvas in this Article. The discussion that follows will attempt to synthesize some of this literature and apply it to the specific example of using cables for intelligence gathering.

The first issue that arises is whether submarine cables used for underwater surveillance falls within one of the rights of all States recognized in the EEZ under Article 58 (1):

> In the exclusive economic zone, all States, whether coastal or land-locked, enjoy, subject to the relevant provisions of this Convention, the freedoms referred to in article 87 of navigation and overflight and of the laying of submarine cables and pipelines, and other internationally lawful uses of the sea related to these freedoms, such as those associated with the operation of ships, aircraft and submarine cables and pipelines, and compatible with the other provisions of this Convention.[324]

All States have the right to lay cables in the EEZ.[325] In the majority of the relevant provisions in UNCLOS, the generic phrase "submarine cable" is used and the term is not defined anywhere in UNCLOS. It has been argued that "the objective, purpose and interpretation of this term—"submarine cables"—and subsequent agreements strongly suggest that the term refers to cables used to transport voice, data and internet traffic between system end points."[326] Thus, it

---

320 *See* UNCLOS, *supra* note 85, art 19, ¶ 2.

321 *Id.* art. 56, ¶ 1; *see also* discussion *supra* Part II(1).

322 *Id.* art. 58, ¶ 1.

323 *See*, *e.g.,* MARK J. VALENCIA, E.-W. CTR., MILITARY AND INTELLIGENCE GATHERING ACTIVITIES IN EXCLUSIVE ECONOMIC ZONES: CONSENSUS AND DISAGREEMENT—A SUMMARY REPORT OF THE BALI DIALOGUE 4-10 (2002), www.eastwestcenter.org/sites/default/files/private/BaliDialogue.pdf; Stuart Kaye, *Freedom of Navigation, Surveillance and Security: Legal Issues Surrounding the Collection of Intelligence from beyond the littoral*, 24 AUSTR. YB. INT'L L. 93, 102-04 (2005); Raul Pedrozo, *Preserving Navigational Rights and Freedoms: The Right to Conduct Military Activities in China's Exclusive Economic Zone*, 9 CHIN. J. INT'L L. 9, 12-20 (2010); Zhang Haiwen, *Is it Safeguarding the Freedom of Navigation or Maritime Hegemony of the United States?—Comments on Raul (Pete) Pedrozo's Article on Military Activities in the EEZ*, 9 CHIN. J. INT'L L. 31 (2010).

324 UNCLOS, *supra* note 85, art. 58, ¶ 1.

325 *Id.*

326 KENT BRESSIE, USING SUBMARINE CABLES FOR CLIMATE MONITORING AND DISASTER

has been contended that the laying of hydrophone arrays in the EEZ using cables can be subsumed under the freedom to lay cables since their "key functions of transmitting electronic impulses and information to terminals or other receivers have common elements."[327] Roach has also argued that military cables, which are submarine cables used for military purposes or are military owned and/or leased, are subject to the same regime under international law that governs submarine cables.[328]

It could also be argued cables used for underwater surveillance cannot be subsumed under the freedom to lay cables because the objectives of such cables is not the transmission of data or telecommunications but rather covert intelligence gathering.[329] Accordingly, the next question is whether it can be considered part of "other internationally lawful use of the sea related to these freedoms, such as those associated with the operation of… submarine cables." [330] The answer to this hinges on whether intelligence gathering is permitted in the EEZ, an issue which is mired in controversy.[331] According to the United States, this phrase was an implicit reference to traditional high seas freedoms such as the freedom to conduct a large range of military activities, including intelligence gathering activities and consequently using cables for underwater surveillance.[332] Preserving traditional high seas freedoms of military activities in the EEZ was a high priority for the US[333] and thus U.S. Ambassador Elliot Richardson proposed the language of "internationally lawful uses of the sea" to preserve such freedoms.[334] According to the United States, the treaty negotiations support this interpretation.[335] The maritime powers were willing to concede to the coastal States economic rights over a vast portion of the oceans provided that traditional high seas freedoms such as military activi-

---

WARNING: OPPORTUNITIES AND LEGAL CHALLENGES 21 (2012), https://www.itu.int/dms_pub/itu-t/oth/4B/04/T4B040000160001PDFE.pdf.

327 Moritaka Hayashi, *Military and Intelligence Gathering Activities in the EEZ: Definition of Key Terms*, 29 MARINE POL'Y 123, 129 (2005); *see* Elmar Rauch, *Military Uses of the Oceans*, 28 GER. Y.B. INT'L L. 229, 256-57 (1985); *see also* ROBIN R. CHURCHILL & A.VAUGHAN LOWE, THE LAW OF THE SEA 427 (3rd ed., 1999).

328 Roach, *supra* note 290, at 339.

329 VALENCIA, *supra* note 322, at 4-10.

330 UNCLOS, *supra* note 85, art. 58.

331 VALENCIA, *supra* note 322, at 4-10.

332 Galdorisi & Kaufman, *supra* note 311, at 272.

333 For example, during the negotiations of UNCLOS, the US and other maritime powers had objected to the suggestion that the phrase "other internationally lawful uses of the sea related to navigation and communications" because they felt it was too restrictive. *See* Jorge Casteñeda, *Negotiations on the Exclusive Economic Zone at the Third United Nations Conference on the Law of the Sea, in* ESSAYS ON INTERNATIONAL LAW IN HONOUR OF JUDGE MANFRED LACHS 621, 622 (1984).

334 Galdorisi & Kaufman, *supra* note 311, at 272.

335 *Id.* at 280.

ties were preserved in this zone.[336] As the nomenclature suggests, the "concept of an [EEZ] was not intended to reserve any rights for coastal States other than the economic rights of the coastal State in those waters, as well as a narrow slice of associated jurisdiction for specific purposes."[337] Attempts during negotiations to recognize the security interests of the coastal State in the EEZ were explicitly rejected.[338] Thus, any aerial, surface, and subsurface surveillance activities in the EEZ is an "internationally lawful use of the sea" that has been borne out by State practice.[339] Relative to this interpretation, the laying of cables with recording devices and the placement of recording devices on existing cable networks are lawful intelligence gathering activities; however, there are several counter-arguments to this, some of which raise legitimate legal arguments.

First, the plain reading of "internationally lawful uses of the sea" only recognize that all vessels, including military vessels, enjoy freedom of navigation within the EEZ.[340] The language does not give States unrestricted rights to conduct military activities in the EEZ.[341] Further, in contrast to the position put forth by the United States, there was not a clear and unanimous understanding that military activities would not be prohibited in the EEZ.[342] Several States rejected such an interpretation, even at the time of adoption of the Convention. For example, Brazil stated on the signing of the Convention that the "provisions of the Convention do not authorize other States to carry out military exercises or maneuvers, within the exclusive economic zone, particularly when these activities involve the use of weapons or explosives.[343] Indeed, it is true that the issue was not formally raised in negotiations and therefore, it can be said that there was no agreement on the issue. Further, it is also argued that

---

336 *Id.* at 264.

337 Jonathan G. Odom, *The True "Lies" of the Impeccable Incident: What Really Happened, Who Disregarded International Law, and Why Every Nation (Outside of China) Should be Concerned*, 18 MICH. ST. J. INT'L L. 411, 438 (2010).

338 *Id.*

339 Raul Pedrozo, *Coastal State Jurisdiction over Marine Data Collection in the Exclusive Economic Zone*, *in* MILITARY ACTIVITIES IN THE EEZ: A U.S.-CHINA DIALOGUE ON SECURITY AND INTERNATIONAL LAW IN THE MARITIME COMMONS 23, 30 (Peter Dutton ed., 2010).

340 Haiwen, *supra* note 323, at 33.

341 Galdorisi & Kaufman, *supra* note 311, at 279 (citing UNCLOS, *supra* note 85, art. 59 which requires that the maritime States conduct their operations in the EEZ with "due regard to the rights and duties of the coastal States").

342 *Id.* at 280.

343 *See* 2 U.N. OFF. OF LEGAL AFF., MULTILATERAL TREATIES DEPOSITED WITH THE SECRETARY-GENERAL, at 212, U.N. Doc. ST/LEG/SER.E/19, U.N. Sales No. E.01.V.5 (2001). The declarations of Cape Verde, India, Malaysia, Pakistan and Uruguay voiced similar statements. *See id.* at 213, 220, 222, 225, 231. This was in turn protested by France, Italy, the Netherlands and the United Kingdom. *See id*. at 218, 221, 230-31.

there is no consistent State practice on this issue, and indeed, several States have adopted EEZ legislation that recognize security-related interests in the EEZ.[344] While such legislation may be prima facie a violation of UNCLOS, it certainly demonstrates a lack of consensus on the permissibility of intelligence gathering in the EEZ.[345]

Second, it has also been suggested by some Chinese academics that intelligence gathering activities are contrary to the obligation of reserving the EEZ for peaceful purposes[346] and the overarching obligation in Article 301 of UNCLOS requiring all States to refrain from any threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the principle of international law embodied in the UN Charter.[347] Not all military activities/intelligence gathering activities are contrary to the peaceful purposes obligation, only those that threaten or use force against the territorial integrity or political independence of a state inconsistent with the UN Charter.[348] The question then becomes what constitutes a threat or use of force inconsistent with the Charter. Some intelligence gathering technologies used in the EEZ are becoming "increasingly more intensive and intrusive,"[349] this includes:

> *[A]ctive* signals intelligence (SIGINT) activities conducted from aircraft and ships, some of which are deliberately provocative and intended to generate programmed responses. Other SIGINT activities intercept naval radar and emitters, thus enabling the location, identification and tracking of surface ships as well as the planning and preparation of electronic missiles against them. These activities appear to involve far greater interference with the communication and defense systems of the targeted coastal State than any traditional passive intelligence gathering activities conducted from outside national territory.[350]

Notwithstanding the above, the threshold for an intelligence gathering activity reaching the threshold of a use of force or threat of use of force is high, and underwater surveillance by cables does not meet this threshold.[351]

Fourth, it has also been argued that a user State's obligation to have due regard for the rights and duties of the coastal State, and to comply with the laws and regulations adopted by the coastal State under Article 58 (3) of UNCLOS is a restraint on military activities in the EEZ.[352] China, for example, has suggested that the due regard obligation requires States to refrain from any activi-

---

344 JAMES KRASKA, MARITIME POWER AND THE LAW OF THE SEA: EXPEDITIONARY OPERATIONS IN WORLD POLITICS 276-77 (2011).

345 KLEIN, *supra* note 278, at 47.

346 UNCLOS, *supra* note 85, art. 58, ¶ 2.

347 Haiwen, *supra* note 323, at 44-45.

348 Hayashi, *supra* note 327, at 125.

349 *Id.* at 126.

350 *Id.*

351 *Id.*

352 *Id.*

ties "which endanger the sovereignty, security and national interests of the coastal countries."[353] Due regard has not been defined by the Convention; however, it is considered a procedural obligation which involves a balancing of the rights, jurisdiction and duties of the coastal State and user States in the EEZ.[354] It is said to consist of two elements, an awareness of and consideration for other State's interests and a weighing of those interests or sources of authority.[355] In the present case, the due regard obligation does not prohibit military activities, as it merely mandates that it does not interfere with the coastal State's economic rights over resources, and its jurisdiction over the environment, marine scientific research and installations. Moreover, from a practical perspective, it is difficult to see how the due regard obligation would be implemented for military reconnaissance activities. For example, as has been argued elsewhere, for military activities like weapons exercises, the due regard obligation can be implemented through a system of notification. Intelligence gathering is inherently covert and thus a system of notifications would not work. Thus, the due regard obligation provides a weak, if any, limit on intelligence gathering activities.

Fifth, instead of being an "internationally lawful use of the sea associated with the operation of ships, aircraft, and submarine cables,"[356] it has been argued that cables used for underwater surveillance fall within "artificial islands, installations and structures"[357] under the jurisdiction of the coastal State pursuant to Article 60 of UNCLOS. Article 60 stipulates that the coastal State has the "exclusive right to construct and to authorize and regulate the construction, operation and use of (a) artificial islands; (b) installations and structures for the purposes provided for in article 56 and other economic purposes; (c) installations and structures which may interfere with the exercise of the rights of the coastal State in the zone."[358] There are several problems with this argument. A submarine cable is not easily classified as an installation or structure.[359] Further, Article 60 also clearly sets out with some specificity the artificial islands, installations, and structures which the coastal State has jurisdiction over those which are used for economic purposes, marine scientific research or environmental purposes, as set out in Article 56, and those which interfere with the rights of the coastal State in the EEZ as recognized under UNCLOS. Proposals to give the coastal State the exclusive right to construct and regulate *all* artifi-

---

353 VALENCIA, *supra* note 323, at 36-37.
354 KRASKA, *supra* note 344, at 267.
355 2 UNCLOS COMMENTARY, *supra* note 121, at 543.
356 UNCLOS, *supra* note 85, art. 58, ¶ 1.
357 Hayashi, *supra* note 327, at 132.
358 *Id.* at 131.
359 *Id.* at 129.

cial islands, installations and structures for any purpose, including military installation and devices were rejected, which suggests that the coastal State right was intended to be circumscribed, and thus does not apply to military installations.

3. High Seas

Customary international law has always recognized military activities including intelligence gathering has a lawful use of the high seas associated with the operation of warships exercising the freedom of navigation.[360] The list of high seas freedoms set forth in Article 87 of UNCLOS was not intended to be an exhaustive list,[361] and although not explicitly mentioned in Article 87 of UNCLOS, it is generally agreed that intelligence gathering is a high seas freedom.[362]

As mentioned above, the laying of cables is also a high seas freedom,[363] and thus, prima facie, a country's military forces would be free to lay cables with underwater listening stations used specifically for military purposes pursuant to this right.

C. Tapping of Undersea Fiber Cables

Historically, the U.S. National Security Agency conducted its covert intelligence gathering activities using satellite and microwave towers but this was considerably hindered with the increasing use of submarine cables for the transmission of communications.[364] The pinnacle of these tapping endeavors is certainly the discovery in 2013 that both the United States and United Kingdom national security agencies have been "tapping directly into the Internet's backbone,"[365] namely the fiber optic cables. According to newspapers reports, the existence of these programs was disclosed by the NSA whistleblower Edward Snowden as part of his efforts to expose "the largest programme of suspicionless surveillance in human history."[366] The UK's fiber tapping program known as Tempora was able to collect around 21 million gigabytes per day, including "recordings of phone calls, the content of e-mail messages, entries on

---

360 Galdorisi & Kaufman, *supra* note 311, at 272.

361 KLEIN, *supra* note 278, at 45. Article 87 uses the terminology *inter alia*. UNCLOS, *supra* note 85, art. 87.

362 Hayashi, *supra* note 327, at 130.

363 UNCLOS, *supra* note 85, art. 87, ¶ 1(c).

364 *US Spy Agency Labors to Preserve Hearing in Tech Age,* 9 SUBMARINE FIBER OPTIC COMMC'NS SYS. NEWSL., No. 8, Aug. 2001, at 6-7 [hereinafter SFOCS Newsletter].

365 Khazan, *supra* note 13.

366 MacAskill et al., *GCHQ, supra* note 14.

Facebook and the history of any internet user's access to websites- all of which is deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets."[367] Hundreds of analysts from both the GCHQ and NSA sifted through the data that was obtained from more than 200 fiber optic cables.[368] This has been described as "upstream collection," which involves the accessing of communications of fiber cables and infrastructure as data flows past.[369] The data "provides a powerful tool in the hands of the security agencies enabling them to sift for evidence of serious crime…it has allowed them to discover new techniques used by terrorists to avoid security checks[,]…identify terrorists planning atrocities[, and]…used against child exploitation networks and in the field of cyberdefence."[370]

At least seven telecommunications companies have been allegedly complicit in this project.[371] Indeed, it has been alleged that some companies have been paid for the cost of their cooperation and/or were obliged to co-operate as a condition of their licensing.[372] How these agencies might tap an underwater cable is not entirely clear as the process is extremely secretive. One report has stated that intercept probes are attached to transatlantic fiber-optic cables where they land at cable landing stations located on British shores.[373]

Other reports speculate that it is done by directly tapping undersea cables that are laid on the seabed. In the mid-1990s, it was reported that the NSA installed a tap onto an undersea cable by using a special submarine to splice into the cable, although details are vague.[374] Similarly, in 2005, it was reported that the submarine USS Jimmy Carter was equipped with the ability to tap undersea cables and eavesdrop on the communications passing through them.[375] Such an operation involves the submarine lifting the cable from the seabed and onto the submarine into a special chamber where crew would extract data either by bending the fiber or by splicing a second fiber to each of the fibers. [376] According to one article "the easiest place to get into the cables is at the regeneration

---

367 *Id*.

368 *Id*.

369 Craig Timberg, *NSA Slide Shows Surveillance of Cables*, WASH. POST (July 10, 2013), http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html.

370 MacAskill et al., *GCHQ, supra* note 14.

371 Pratap Chatterjee, *Glimmerglass Intercepts Undersea Cable Traffic for Spy Agencies*, CORPWATCH (Aug. 22, 2013), http://www.corpwatch.org/article.php?id=15862.

372 MacAskill et al., *GCHQ, supra* note 14.

373 Khazan, *supra* note 13.

374 SFOCS Newsletter, *supra* note 364, at 7.

375 *New Nuclear Sub is Said to Have Special Eavesdropping Ability,* N. Y. TIMES (Feb. 20, 2005) [hereinafter *Nuclear Sub*], http://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html?_r=1.

376 SFOCS Newsletter, *supra* note 364, at 9.

points—spots where their signals are amplified and pushed forward on their long circuitous journeys."[377] Such physical tapping is necessary when cable-landing stations are on foreign soil and are otherwise inaccessible.[378] However, in 2001 cable experts expressed doubt that physical tapping could occur, considering that splicing a fiber could result in an interruption in communications which could be detected by the cable operator.[379]

At this point, it is appropriate to highlight the distinction in objectives between cables used for the Sound Surveillance System described above, and the tapping of cables. The former is done in order to enhance awareness about the environment in which navies operate, including gathering information on the military capabilities of the Soviet Union.[380] The latter is a form of mass surveillance or bulk electronic surveillance that has been described as the "clandestine surveillance by one state during peacetime of the communications of another's state's officials or citizens when those communications take place partly or entirely outside the surveilling state's territory."[381]

Whether UNCLOS can be used to address the mass surveillance carried out through the tapping of undersea cables is not entirely clear. To the extent that UNCLOS governs intelligence gathering activities, it could be argued that it only applies to intelligence gathering activities that take place within the maritime domain, and will not govern the use of intercepts at cable landing stations. Further, if indeed mass surveillance can be done by physically tapping undersea cables by splicing the cable or otherwise, it is also not certain that UNCLOS is the applicable regime to govern such acts. Such surveillance does not fall within conventional perceptions of military activities/intelligence gathering at sea, which as mentioned above, is targeted, and aims at enhancing knowledge of the marine environment and/or the military capabilities of other State's navies. That said, UNCLOS is of course a living instrument and subject to evolutionary interpretation, and for present purposes, this Article will assume that UNCLOS applies to the mass surveillance carried out by tapping undersea cables to the extent it involves physically tapping cables as they lay on the seabed.

Within the territorial sea, as was the case for cables used for underwater surveillance discussed above, the physical tapping of submarine cables will certainly be deemed as an "act aimed at collecting information to the prejudice of

---

377 Khazan, *supra* note 13.

378 *Nuclear Sub*, *supra* note 375.

379 SFOCS Newsletter, *supra* note 364, at 9.

380 B. Kaushik, Don Nance, & K. K. Ahuja, *A Review of the Role of Acoustic Sensors in the Modern Battlefield* 2 (Am. Inst. of Aeronautics & Astronautics, AIAA 2005-2997, 2005).

381 Deeks, *supra* note 277, at 299.

the defence or security of the coastal State,"[382] or an "act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State,"[383] and will thus render passage non-innocent.[384]

Within the EEZ, the discussion above on the controversy surrounding the legality of intelligence gathering activities would also apply—the bottom line is that there is no clear prohibition against the physical tapping of fiber optic cables in the EEZ to be found in UNCLOS. However, if the physical tapping of fiber optic cables results in the interruption or obstruction of telecommunications, then Article 113 may come into play. Article 113 obliges State Parties to ensure that there is adequate national legislation penalizing the willful or negligent breakage or injury to a submarine cable that results in obstruction or interruption of telecommunications. In particular, if physical tapping involves splicing a cable which does cause a disruption of communications, this would be a breach of Article 113.[385] That said, Article 113 may not be particularly useful, considering that many States have not implemented their obligation under Article 113 to adopt national legislation. Further, physical taps may also be hard to detect although they reportedly can cause a slow-down in communications. In the high seas, intelligence gathering is a freedom of the high seas; however, if physical tapping results in breakage/injury to the cable so as to disrupt telecommunications, Article 113 applies.

D. The Way Forward

The legal regime established in UNCLOS has significant gaps in relation to intelligence gathering in maritime areas. This is arguably unsurprising given that "traditional international law is remarkably oblivious to the peacetime practice of espionage."[386] As observed by Chesterman:

> Despite its relative importance in the conduct of international affairs, there are few treaties that deal with it directly. Academic literature typically omits the subject entirely, or includes a paragraph or two defining espionage and describing the unhappy fate of captured spies. For the most part, only special regimes such as the laws of war

---

382 UNCLOS, *supra* note 85, art. 19, ¶ 1(c).

383 *Id.* art. 19, ¶ 1(k).

384 *See id.* art. 19, ¶ 2.

385 This may not be particularly useful, considering that most States have not implemented their obligation under Article 113 to adopt national legislation. *See* discussion *supra* Part III; *see also* UNCLOS, *supra* note 85, art. 113.

386 Christopher S. Yoo, Cyber Espionage or Cyber War? International Law, Domestic Law and Self-Protective Measures 23-24 (Jan. 26, 2015) (unpublished manuscript) (on file with the University of Pennsylvania Legal Scholarship Repository), www.scholarship.law.upenn.edu/faculty_scholarship/1540 (citing Richard A. Falk, *Foreword* to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v (Roland J. Stanger ed., 1962)).

> address intelligence explicitly. Beyond this, it looms large but almost silently in the legal regimes dealing with diplomatic protection and arms control.[387]

Deeks postulates that there are three approaches to international law's regulation of intelligence gathering.[388] The first approach contends that because there is nothing in international law that prohibits espionage, it is permitted under international law.[389] The second approach argues that "international law should be read affirmatively to permit spying" as it is inherent in a State's right to act in self-defense and/or it has been affirmed by widespread state practice.[390] The third approach proposes that international law does regulate intelligence gathering, drawing from three sources of law, namely the law on sovereignty and territorial integrity, human rights law such as the International Convention on Civil and Political Rights and the Vienna Convention on Diplomatic Relations, although "those sources lack crisp content or have not been consistently read by states to inhibit foreign surveillance."[391] The lack of clarity on when and the extent to which international law applies to espionage has meant that domestic law governs much espionage activity.[392]

It is beyond the scope of this Article to put forth comprehensive solutions to the legal issues related to intelligence gathering in the oceans.[393] Nonetheless, a few salient points are worth mentioning. While it is possible that States will negotiate a treaty to regulate intelligence gathering in general, it is arguably a far-off possibility given the wide divergence of opinions on its legality.[394] Other scholars have put forth suggestions on what an international legal framework could look like and these provide extremely useful foundations for a dialogue on this issue. Regardless of whether international law can provide a solution, a wider question needs to be asked—should submarine cables be used for intelligence gathering activities at all? The mass surveillance done by physically tapping cables underwater (to the extent that it is done) would appear to run the risk of damaging the cable and thus putting the submarine cable network in jeopardy. While there is less of a chance of cables being damaged when they are used for acoustic surveillance underwater, such uses of submarine cables

---

387 Simon Chesterman, *The Spy Who Came In From the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1072 (2006).

388 *See* Deeks, *supra* note 277, at 301-13.

389 Duncan B. Hollis, *Is Law Losing Cyberspace?*, OPINIO JURIS (June 4, 2015, 10:48 PM), http://opiniojuris.org/2015/06/04/is-law-losing-cyberspace.

390 Deeks, *supra* note 277, at 302.

391 *Id.* at 304.

392 Yoo, *supra* note 386, at 24.

393 Lubin, for example, suggests that the *jus ad bellum* principles of just cause, necessity, immediacy and proportionality should be applied to intelligence gathering activities. *See* Lubin, *supra* note 285, at 56-62. Deeks suggests that domestic law is a profitable source of ideas for international law on surveillance. *See* Deeks, *supra* note 277, at 343-61.

394 Deeks, *supra* note 277, at 342.

increases the suspicion and mistrust on the part of States to cable laying activity. Coastal States are increasingly imposing regulations on cable laying and repair in the EEZ undermining its status as one of the freedoms recognized there.[395] While this is unsurprising given that coastal States view the EEZ in quasi-territorial terms and wish to control all activities which take place there, the perception cables can be used for such military purposes arguably increases the chances of *all* cable activities being unduly restricted. This, in turn, could impact the connectivity that we so depend on today. Thus, governments and the cable industry must carry out a careful cost/benefit ratio when making decisions on whether to use submarine cables for intelligence gathering. After all, submarine cables are the backbone of the Internet and using them for this purpose implicates the security of global telecommunications.

V. CONCLUSION

The international community's reliance on submarine fiber optic cables cannot be underestimated. From the Internet to phone and bank services to science and military uses, it is not an exaggeration to say that the submarine fiber optic cable has become the foundation of our modern digital society, and one of the most important drivers in globalization. The focus of this Article has been on the importance of submarine cables to security in general and to cybersecurity in particular. Despite this criticality, the emphasis in discussions about cyber security has been hitherto directed at the protection of information, and not about the protection of the submarine cables that transmit this information. As discussed above, submarine cables are vulnerable to two distinct challenges—intentional interference with submarine cable systems by State and/or non-State actors, as well as tools for intelligence gathering. The legal regime for the protection of cables from both these threats consists of a patchwork of international conventions and customary international law and significant gaps remain. While intentional interference and intelligence gathering are qualitatively different requiring different responses, it is undeniable that the international community must begin to, at the very least, start a dialogue about these issues.

With regard to the protection of cable systems from intentional interference by State and/or non-State actors, this Article demonstrated that the present legal regime is deficient in ensuring the security of cables. UNCLOS, the laws of war and terrorism conventions are capable of addressing certain aspects of the protection of cables, but surely critical communications infrastructure such as cables deserves a more comprehensive and holistic legal regime. To this end,

---

[395] For a more comprehensive discussion on the regulation of cable laying in the EEZ by coastal States, see Ford-Ramsden & Davenport, *supra* note 104, 140-52.

the Article proposed the adoption of an international treaty that protects submarine cables, making intentional interference (be it a physical or cyberattack) with submarine cable systems an international crime, and including provisions for mutual cooperation on enforcement against such crimes. While there is always a certain amount of inertia when negotiating an international instrument, the cable industry and the ICPC should work together with national governments to include this issue in current discussions at the UN about cybersecurity. Framing it as a cybersecurity issue is likely to get the most traction.

With regard to using submarine fiber optic cables for intelligence gathering, this raises a whole set of different issues. Using cables for intelligence gathering does not necessarily result in damage to the cables—although in some cases it might. Further, the practice is shrouded in mystery, particularly using cables to conduct mass or bulk surveillance. As with the protection of submarine cables from intentional interference, the legal regime is patchy and piecemeal, perhaps because intelligence gathering general subsists in the shadows of the law. In the context of ensuring the security of submarine communications, the question must be asked whether submarine cables should even be used for intelligence gathering purposes given how vital they have become to the world. While this issue is unlikely to ever be a subject of an international treaty, it is imperative that governments and the cable industry alike must carry out a careful cost/benefit ratio when making decisions on whether to use submarine cables for intelligence gathering. In the author's view, the risk to the submarine cable system may outweigh the benefits of using them for intelligence gathering.