CUTTING SUBMARINE CABLES: THE LEGALITY OF THE USE OF FORCE IN SELF-DEFENSE

Blair Shepherd*

* Blair Shepherd is a New Zealand lawyer currently practicing international arbitration as an Intern in the Paris office of Three Crowns LLP. He graduated *magna cum laude* from Duke University School of Law (2020) with a Master of Laws (LL.M.), and from the University of Otago (2017) with a Bachelor of Laws (LL.B.) and a Bachelor of Arts (B.A. (Philosophy, Politics and Economics)). The author would like to thank Maj. Gen. Charles J. Dunlap, Jr., USAF (Ret.)—Professor of the Practice of Law and Executive Director of the Center on Law, Ethics and National Security at Duke University School of Law—for his feedback and assistance; along with the helpful editors of the Journal. The author can be contacted at blair.shep@gmail.com.

I. INTRODUCTION

States, people, organizations, and economies are becoming increasingly dependent on the Internet to conduct their everyday affairs. Despite this ever-increasing cyber dependence, a small number of privately-owned submarine cables—that are remarkably vulnerable to damage—are responsible for the transmission of almost all internet communications.[1] The criticality of these cables, along with advances in submarine military technology, give rise to the possibility that a state may attack the cables providing telecommunications access to another state in order to deny that state, businesses, and people access to the Internet. In the event that a state does conduct such an attack on submarine cables, the victim state and international community at large will need to urgently consider whether such an attack constitutes an armed attack, which would justify the use of force in self-defense, and, if so, what use of force in defense is legal.

Part II of this paper summarizes the criticality of the Internet to modern society, while Part III describes the international submarine cable network and its vulnerability. Part IV sets out the modern legal framework for analyzing uses of force under international law. Part V analyzes whether an attack on submarine cables would constitute an armed attack justifying the use of force in self-defense, considering both attribution and the severity of the consequences of the attack.[2] Part VI discusses what uses of force in self-defense would be appropriate then follows, with regard to necessity, proportionality and the legitimacy of targets.

Part VII concludes that some attacks by states on submarine cables could foreseeably amount to an armed attack that would justify the use of force in self-defense. Such an attack will meet this threshold if it causes a severe reduction in a state's access to the Internet and other telecommunications for a substantial period of time, which is highly-fact specific. In addition, states exercising their right to self-defense must be cautious of a range of factors that could render their use of force illegal. In particular, they must be able to satisfy requirements of necessity, proportionality and legitimacy of targets.

1. This paper focuses only on submarine *communications* cables and not submarine *power* cables.

2. This paper does not address the separate (and similarly pressing) issue of the legality of wiretapping submarine cables. For a discussion of this (possibly already-realized) threat, *see* Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 CATH. U. J. L. & TECH. 57 (2015).

II. THE CRITICALITY OF THE INTERNET AND SUBMARINE CABLES

Since the invention of the World Wide Web in 1989,[3] and particularly since the mid-to-late 2000s, the Internet has revolutionized modern life. An estimated 4.1 billion people now use the Internet, with the number of users having grown by an average of ten percent each year since 2005.[4] In developed countries, 86.6% of people use the Internet, while 47.0% of people in developing countries use the Internet.[5] Demand for bandwidth is predicted to increase almost twofold biennially for the foreseeable future.[6]

Despite the Internet's crucial role in modern life, little attention is paid to how communications are actually transmitted through the Internet[7]—that is, not how internet service providers connect computers and smartphones to the Internet through Wi-Fi and phone data plans, but rather how information is thereafter communicated around the world.[8] In fact, submarine cables—not satellites—carry ninety-nine percent of the world's international telecommunications.[9] The preeminence of cables is due to the fact that they can transmit much more data at a much lower cost than satellites.[10]

Not only individuals rely on the Internet—businesses and states' economies do, too. Globalization has caused the integration of states' economies and their subsequent interdependence, with businesses using email and international phone calls to communicate with overseas parties. In international finance, the Society for Worldwide Interbank Financial Telecommunication uses the global submarine cable network for data transmissions between financial institutions in over 200 countries and territories.[11] Those transmissions averaged 34.18 million per day in

3. *History of the Web*, WORLD WIDE WEB FOUND., https://webfoundation.org/about/vision/history-of-the-web (last visited Dec. 12, 2019).

4. INT'L TELECOMM. UNION, MEASURING DIGITAL DEVELOPMENT: FACTS AND FIGURES 2019 1 (2019).

5. *Id.* at 2.

6. SUBMARINE TELECOMM. FORUM, INC., SUBMARINE TELECOMS INDUSTRY REPORT 19/20 15 (Stephen Nielsen ed.) (2019).

7. *See* Adam Satariano, *How the Internet Travels Across Oceans*, N.Y. TIMES (Mar. 11, 2019), https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html ("People think that data is in the cloud, but it's not,' said Jayne Stowell, who oversees construction of Google's undersea cable projects. 'It's in the ocean.'").

8. *Id.*

9. SUBMARINE TELECOMM. FORUM, INC., *supra* note 6, at 14. For a primer on the development of the global submarine communications cable network, *see* Davenport, *supra* note 2, at 60–62.

10. *See Submarine Cable Frequently Asked Questions*, TELEGEOGRAPHY, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions#Cable-101 (last visited Nov. 26, 2019) [hereinafter *Frequently Asked Questions*].

11. *About Us*, SWIFT, https://www.swift.com/about-us (last visited Dec. 12, 2019).

September 2019 (bringing year-to-date growth to 7.5%).[12] As Chief Executive Eric Handa of APTelecom recently summarized, "[s]ubmarine [c]able capacity for reasons of diversity in avoiding points of failure and 'enabling always on' networks is critical for banking and finance, aviation, and various other industries that utilize cloud computing, artificial intelligence, and are poised to seize on the upcoming 4th Industrial Revolution of automation."[13]

States also rely on submarine cables for their international communications, including for national security, as the radiofrequency circuits that satellites use have insufficient bandwidth for the operational orders necessary for global military operations.[14] Accordingly, states use the cable network for military operations, diplomatic missions, and intelligence-gathering.[15] Although the United States has laid submarine cables solely for national security purposes,[16] this appears to be a novel concept.[17] For example, the lack of exclusively national security related submarine cables between Egypt and Italy caused U.S. Air Force disruptions in 2008.[18] Three of the world's largest submarine cables (between Egypt and Italy) were damaged, causing a reduction in connectivity between Europe and the Middle East of eighty percent.[19] This disruption meant that the U.S. Air Force could only launch tens of drone flights per day from Balad Air Base in Iraq, instead of the usual hundreds.[20]

For the reasons stated in this section, the submarine cable network is increasingly being labelled as "critical infrastructure"[21]—a classification that reflects its profound significance to modern life.

---

12. *SWIFT IN FIGURES Sept. 2019 YTD*, SWIFT, https://www.swift.com/sites/default/files/documents/sif_201909.pdf (last visited Dec. 8, 2019).

13. SUBMARINE TELECOMM. FORUM, INC., *supra* note 6, at 12.

14. Bryan Clark, *Undersea Cables and the Future of Submarine Competition*, 72 BULL. ATOMIC SCIENTISTS 234, 235 (2016).

15. *Id.*

16. *See* Garrett Hinck, *Evaluating the Russian Threat to Undersea Cables*, LAWFARE (Mar. 5, 2018, 7:00 AM), https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables (referring to the Pentagon's admission that it had laid a cable connecting Miami, Florida with Guantanamo Bay, Cuba, and was planning a second cable connecting Guantanamo Bay to Puerto Rico).

17. Rishi Sunak, UNDERSEA CABLES: INDISPENSABLE, INSECURE 8 (2017).

18. *Id.* at 21–22.

19. *Id.*

20. *Id.*

21. *See generally, e.g.*, Doug Brake, SUBMARINE CABLES: CRITICAL INFRASTRUCTURE FOR GLOBAL COMMUNICATIONS (2019) (highlighting increased demand and use of submarine cables).

III. THE VULNERABILITY OF SUBMARINE CABLES

Given the criticality of the submarine cable network, it is reasonable to expect that submarine cables could be targeted for malicious purposes. Despite their significance, however, they are highly vulnerable due to the characteristics of the cable network and the cables themselves.[22]

Submarine cables generally have a girth similar to that of a garden hose and are simply laid along the seabed (although they are typically buried beneath the seabed close to shore).[23] Their locations are easily accessible on the Internet[24] and they may be easily signposted close to land to caution nearby vessels.[25] Moreover, they are generally owned by consortia or private companies,[26] with the effect that states do not have the same direct responsibility or ability to protect them than if they were publicly-owned.[27]

The fact that there is an average of 100 cable faults each year (i.e., more than one quarter of all submarine cables)[28] demonstrates submarine cables' vulnerability to physical harm. Dragged anchors caused approximately two-thirds of faults, with environmental events such as earthquakes also causing damage.[29] On rarer occasions, aquatic animals have caused damage, such as by way of shark bites.[30] Due to this vulnerability, then U.S. Secretary of State Hillary Clinton listed dozens of cable landing sites around the world as "critical foreign dependencies" in a confidential cable to all U.S. diplomatic posts in 2009.[31]

Fixing cable faults is usually a lengthy and complicated process.[32] The owner of the damaged cable must first determine the location of the break

---

22. For an in-depth technical explanation of the vulnerability of the international submarine cable network, *see generally* DNI, THREATS TO UNDERSEA CABLE COMMUNICATIONS (2017).

23. *Frequently Asked Questions*, *supra* note 10.

24. *See, e.g.*, *Submarine Cable Map*, TELEGEOGRAPHY, https://www.submarinecablemap.com (last visited Dec. 9, 2019).

25. This is the case in New Zealand, for example, where the Submarine Cables and Pipelines Protection Act 1996, s 12 (N.Z.), has resulted in Orders in Council establishing signposted protected areas surrounding coastal cable landing zones. The author has travelled to one such protected area off the Cook Strait coast of Marlborough, New Zealand, himself.

26. *See Frequently Asked Questions*, *supra* note 10. For a primer on the submarine cable industry, *see* Davenport, *supra* note 2, at 65–66.

27. *See, e.g.*, U.N. Convention on the Law of the Sea art. 114, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS] (mandating that states should impose liability for damage to cables during the laying or repairing of other cables on the owners of those other cables). Brake, *supra* note 21, at 2.

28. Brake, *supra* note 21, at 2.

29. *Frequently Asked Questions*, *supra* note 10.

30. *Id.*

31. *Request for Information: Critical Foreign Dependencies (Critical Infrastructure and Key Resources Located Abroad)*, WIKILEAKS: PUBLIC LIBRARY OF US DIPLOMACY, https://wikileaks.org/plusd/cables/09STATE15113_a.html (last visited Dec. 8, 2019).

32. Clark, *supra* note 14.

using a built-in monitoring system.[33] The owner must then contract cable repair ships to attend the site of the damage.[34] This can take a considerable amount of time for long and remote cables—for example, the damage could occur in the middle of the Pacific Ocean, thousands of miles away from the nearest repair ship.[35] For this reason, although cable faults in the populous 'Transatlantic' region are typically repaired within days or hours, the worldwide average repair timeframe was approximately 27 days in 2019, while the average for the much more expansive 'Transpacific' region was longer than all other regions' averages combined.[36]

The evolution of undersea warfare technology compounds the threat to the submarine cable network. It is expected that unmanned underwater vehicles (UUVs) will replace submarines for offensive missions in the 2020s and early 2030s, given that they are smaller and more difficult to detect.[37] The fact that use of a UUV does not directly threaten the life of an officer of the offensive state will remove the direct risk to human life inherent to offensive missions, along with the decrease in political capital that results from the loss of patriotic life.[38] Further, developments in undersea communication methods are likely to allow submarines, UUVs and onshore commanders to communicate without any above-the-surface vehicles or facilities.[39]

In this context of improving autonomous access to cables, reporters documented a significant increase in the activity of Russian submarines and spy ships along submarine cable routes as early as October 2015.[40] In November 2019, *Yantar*—a Russian intelligence ship that has previously been observed "loitering" around cables—was operating near North America in the Atlantic Ocean in a manner that was invisible to open-source tracking systems.[41]

---

33. *Id.*

34. *Id.*

35. *See* SUBMARINE TELECOMM. FORUM, INC., *supra* note 6, at 51.

36. *Id.* at 49–51.

37. Clark, *supra* note 14, at 236.

38. *See* Teresa A. Myers & Andrew F. Hayes, *Reframing the Casualties Hypothesis: (Mis)Perceptions of Troop Loss and Public Opinion About War*, 22 INT'L J. PUB. OP. RES. 256, 257–58 (2010) ("Wartime casualties reduce the legitimacy and political capital of state leaders across the world . . . This lack of legitimacy can then lead to an inability for those leaders to maintain power.").

39. *See id.*

40. David E. Sanger & Eric Schmitt, *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*, N.Y. TIMES (Oct. 25, 2015), https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

41. H. I. Sutton, *Russia's Suspected Internet Cable Spy Ship Vanishes Off the Americas*, FORBES (Dec. 1, 2019, 7:50 AM), https://www.forbes.com/sites/hisutton/2019/11/19/russias-suspected-internet-cable-spy-ship-vanishes-off-the-americas/#54da4e8f62c1; *see also* Hinck, *supra* note 16.

IV. INTERNATIONAL LAW FRAMEWORK

This section introduces the sources of international law and their hierarchy, before identifying treaty provisions and rules of international customary law that set the framework for determining the legality of responses to cable attacks.

A. Sources of International Law

The sources of international law and their order of primacy are codified in Article 38 of the Statute of the International Court of Justice of 1945.[42] Those sources, in order, are: international conventions; international custom; "the general principles of law recognized by civilized nations;" and "judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of the rules of law."[43] Although there is no principle of *stare decisis* in international law (International Court of Justice (I.C.J.) judgments are not binding on subsequent judgments or non-parties),[44] the I.C.J. frequently references its previous judgments to promote the consistency of its jurisprudence.[45]

B. Relevant Provisions of International Conventions

No international convention contains any direct provisions regarding an attack against a submarine internet cable. Despite cable-related provisions in the Convention for the Protection of Submarine Telegraph Cables[46] and United Nations Convention on the Law of Sea,[47] neither convention provides for the issue of the use of force in self-defense in response to a cable attack by another state.[48] The core relevant treaty is therefore the Charter of the United Nations of 1945 (the U.N. Charter),[49] which revised the law on the use of force in response to World War II.[50] To that end, Article 2(4) prohibits the threat or use of force:

---

42. STAT. INT'L CT. OF JUST. art. 38, June 26, 1945, 59 Stat. 1031; 33 U.N.T.S. 993, available at https://www.icj-cij.org/en/statute [hereinafter I.C.J. Statute].

43. *Id.*

44. *Id.* at art. 59.

45. Gilbert Guillaume, *The Use of Precedent by International Judges and Arbitrators*, 2 J. INT'L DISP. SETTLEMENT 5, 9 (2011).

46. Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989.

47. *See* UNCLOS, *supra* note 27, arts. 51, 79, & 112–15.

48. Convention for the Protection of Submarine Telegraph Cables, *supra* note 46, at art. 2; *see* NATO COOP. CYBER DEF. CTR. OF EXCELLENCE STRATEGY AND LAW BRANCH RESEARCHERS, *Strategic Importance Of, And Dependence On, Undersea Cables* 5 (2019); *see also* U.N. Convention on the Law of the Sea, *supra* note 27, art. 114.

49. U.N. Charter.

50. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 9–10 (4th ed. 2018).

> All Members 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 manner inconsistent with the Purposes of the United Nations.[51]

Under Article 39, the U.N. Security Council has the sole right to determine "the existence of any threat to the peace, breach of the peace, or act of aggression."[52] The same provision gives the Security Council—whose members include five permanent members holding veto power (the United States, United Kingdom, People's Republic of China, Russian Federation, and France)—the power to decide what measures should be taken in response to such threats, breaches or acts.[53] However, because of the veto power of the five permanent members, Article 39 often does not provide states with satisfactory recourse.[54] With the Russian Federation's aforementioned scoping of cables, it is foreseeable that a permanent member would invoke their veto power in the event of determination of resolutions following an attack on submarine cables. As such, Article 51 is relevant. Despite the prohibition on the threat or use of force and the U.N. Security Council's sole authority to authorize responses, Article 51 allows a state to use self-defense without prior approval in the event of an "armed attack":

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[55]

Unfortunately, the drafters of the U.N. Charter did not define an "armed attack."[56] The remainder of the U.N. Charter also provides no contextual assistance, as there is no use of the phrase "armed attack" in any other provision.[57] One must therefore revert to the other sources of international law, in accordance with Article 38 of the I.C.J. Statute.[58] It is important to note that although Article 38 of the I.C.J. Statute ranks international custom

---

51. U.N. Charter art. 2, ¶ 4.

52. U.N. Charter art. 39.

53. *Id.*

54. GRAY, *supra* note 50, at 20 (noting how the U.N. General Assembly—which is more representative than the U.N. Security Council—has had to step in to condemn acts of aggression where the U.N. Security Council has failed to pass a resolution because of the use, or threat of use, of a veto).

55. U.N. Charter art. 51 (emphasis added).

56. *See id.*

57. *See generally* U.N. Charter (lacking the phrase "armed attack" in all but one provision).

58. I.C.J. Statute, *supra* note 42.

and general legal principles higher than I.C.J. judgments and scholarship, it is necessary nonetheless to consult the latter two sources to determine international custom and general legal principles.

C. Relevant International Custom and General Legal Principles

The I.C.J. first considered the invocation of Article 51 of the U.N. Charter in *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*.[59] That case centered on allegations that the United States executed an armed attack against Nicaragua by supporting the right-wing Contras in their armed rebellion against the Government of Nicaragua.[60] The I.C.J. noted that the U.N. Charter "by no means covers the whole area of the regulation of the use of force in international relations."[61] As Article 51 of the U.N. Charter refers to the "inherent right of self-defense" and states that it does not impede that right, the I.C.J. recognized that the right must be customary in nature.[62] Accordingly, the I.C.J. confirmed that Article 51 neither "subsumes" nor "supervenes" relevant international customary law rules, such as those that self-defense only warrants measures that "are proportional to the armed attack and necessary to respond to it"[63]

The I.C.J. next considered the use of force in *Oil Platforms (Iran v. U.S.)*.[64] The I.C.J. applied its judgment in *Nicaragua*, essentially determining that the United States needed to prove four elements to justify the legality of its retaliatory attacks: firstly, that it had been subject to attacks that Iran was responsible for; secondly, that those attacks were of the gravest forms constituting an armed attack; thirdly, that its response was necessary and proportional; and finally, that the subjects of its response were legitimate military targets.[65] These elements can be referred to in short as attribution, gravity, necessity and proportionality, and legitimacy. Attribution and gravity are necessary to establish the right to use self-defense. In addition to the right to use self-defense, necessity and proportionality and legitimacy are required to establish the legality of self-defense as a response.

Having deduced the above four-element test for a legal use of force in self-defense, it is necessary to consider the law in respect to each of those

59. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 24 (June 27); s*ee also* GRAY, *supra* note 50, at 125.

60. Nicar. v. U.S., 1986 I.C.J. at 18, 20.

61. *Id.* at 94.

62. *Id.* (quoting U.N. Charter art. 51).

63. *Id.*

64. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶¶ 38–78 (Nov. 6).

65. *Id.* at 186–87.

four elements and how it would apply in the context of a malicious attack on submarine cables.

V. "ARMED ATTACK"?

If a state suffers suspicious damage to its submarine cable network, will be to determine whether it has been subjected to an "armed attack" for the purposes of Article 51. This inquiry encompasses the first two elements above: attribution and gravity. If both elements are met, then the state can turn to considerations of what use of force in response is justifiable.

A. Attribution

Attribution is the first hurdle in proving legal use of force in self-defense,[66] and states have often fallen on it. Essentially, a state wishing to use force against another state in self-defense must be able to prove that the alleged perpetrator did actually attack the cables.[67] In the context of a cable attack, a victim state would need to be able to prove two elements: firstly, that the cable damage was a deliberate attack, and secondly, that the state it wishes to retaliate against was responsible.

1. Deliberate Attack

The first element is significant because of the aforementioned prolificacy of unintentional cable damage. Most orthodox uses of force, such as a missile strike or armed invasion, are obviously deliberate. However, while a state with several cables may be prone to assuming that a significant outage is the result of a deliberate attack to its cable network, damage to cables may have another cause, such as a dragged anchor or earthquake.[68] Consequently, a victim state must be very cautious not to use force in self-defense as a 'knee-jerk' reaction—particularly if it is one of the many well-connected states whose cables converge at "chokepoints."[69] There are at least ten such "chokepoints" worldwide;[70] for example, all cables connecting

66. *See id.*

67. *See id.* at 189 ("The Court does not have to attribute responsibility for firing the missile that struck the *Sea Isle City*, on the basis of a balance of evidence, either to Iran or to Iraq; if at the end of the day the evidence available is insufficient to establish that the missile was fired by Iran, then the necessary burden of proof has not been discharged by the United States.").

68. *See Frequently Asked Questions*, *supra* note 10.

69. *See* Doug Tsuruoka, *How World War III Could Start: Cut the 'Cable"*, NAT'L INT.: THE BUZZ (Jan. 7, 2018), https://nationalinterest.org/blog/the-buzz/how-world-war-iii-could-start-cut-the-cable-23974 ("Chokepoints where cables converge because of underwater terrain or other factors are especially vulnerable.").

70. 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), https://citizenlab.org/cybernorms2012/sechrist.pdf.

Hong Kong, Taiwan, South Korea and Japan converge in the Luzon Strait.[71] Those countries suffered disrupted internet access when an earthquake caused six cables to sever at once in 2006.[72] Accordingly, a state that suffers damage to its submarine cable connections must first establish that it actually was the victim of an *attack*, rather than mere accidental cable damage from other causes.

2. Establishing Responsibility

If a state is convinced that it is the victim of a cable attack, it must also be able to attribute the attack to a particular state before it uses force in self-defense. The I.C.J. considered responsibility in *Oil Platforms* and *Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)*.[73]

Oil Platforms centered on events in the Persian Gulf in 1987 and 1988.[74] In 1987, a missile struck a U.S.-flagged oil tanker (*Sea Isle City*) near Kuwait Harbor.[75] The United States attributed the attack to Iran.[76] Three days later, U.S. naval forces destroyed two Iranian offshore oil platforms, asserting self-defense.[77] The next year, the U.S. warship USS *Samuel B. Roberts* struck a mine in international waters off the coast of Bahrain.[78] Again, the United States attributed the attack to Iran.[79] Four days later, the United States destroyed two Iranian offshore oil platforms, again asserting self-defense.[80] The United States alleged that those two attacks were part of an Iranian campaign responsible for over 200 attacks on neutral shipping in the Persian Gulf.[81] Iran asserted that Iraq was actually responsible.[82]

The I.C.J. held that the United States provided insufficient evidence to discharge its burden of proof for attribution,[83] failing to prove that Iran was

71. Tsuruoka, *supra* note 69.

72. *Id.*; *see also Asia Communications in Chaos After Earthquake Off Taiwan - Asia - Pacific - International Herald Tribune*, N.Y. TIMES (Dec. 27, 2006), https://www.nytimes.com/2006/12/27/world/asia/27iht-quake.4032404.html (reporting the Asian telecommunication chaos caused by an earthquake in Taiwan which damaged undersea cables).

73. *See* Iran v. U.S., 2003 I.C.J. at 191–92; *see also* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 316 (Dec. 19).

74. Iran v. U.S., 2003 I.C.J. at 175–76.

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

79. *See id.*

80. *Id.*

81. *Id.* at 176.

82. *Id.*

83. *See id.* at 191–92.

responsible for either the missile attack[84] or the laying of the mine.[85] Accordingly, the United States' attacks on Iranian oil platforms were held to be illegal.[86]

The I.C.J. considered attribution again two years later in *Armed Activities*.[87] The dispute in that case was Uganda was justified in using armed force in the Democratic Republic of the Congo (D.R.C.) during the Second Congo War. Uganda claimed that it had acted in self-defense against cross-border attacks by the Allied Democratic Forces (A.D.F.), a Congolese Islamist rebel group.[88] The I.C.J. found that there was insufficient evidence of D.R.C. support for the A.D.F. to hold the D.R.C. responsible for the cross-border attacks.[89] Moreover, the D.R.C.'s inaction (or ineffective action) to prevent the A.D.F.'s attacks could not amount to an "armed attack" by the D.R.C.[90]

In light of these cases, it is crucial for a victim state to establish responsibility for an attack to a particular state in order to justify using force against that state in self-defense. This may well be difficult as the development of UUVs and other covert seabed warfare technology progresses. States would be wise to develop their detection capabilities in order to mitigate the risk that the perpetrator of an attack would be unidentifiable.

B. Gravity

Even if a victim state has sufficient evidence to attribute a malicious attack to another state, that alone is insufficient for it to use force in self-defense. After establishing attribution, a state must then prove that the attack reaches the threshold of an "armed attack" under Article 51 of the U.N. Charter.

1. Previous Cases

In *Nicaragua*, the I.C.J. set an ambiguous test for subsequent determinations of armed attacks, which established that not all uses of force meet the threshold of an armed attack: "it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack)

84. *Id.* at 189.
85. *Id.* at 195–96.
86. *Id.* at 199.
87. Dem. Rep. Congo v. Uganda, 2005 I.C.J. at 242. *See* Gray, *supra* note 50, at 140.
88. *See* GRAY, *supra* note 50, at 140.
89. *See id.*
90. *See id.*

from other less grave forms."[91] In *Armed Activities*, the I.C.J. dismissed Uganda's argument that this ambiguous threshold of "armed attack" in *Nicaragua* was too narrow.[92] However, gravity did not play a controversial role in either case.

In *Oil Platforms*, the I.C.J. considered whether all of the alleged uses of force on U.S.-flagged or U.S.-owned vessels and aircraft in the Persian Gulf would have amounted to an armed attack (had they had been attributable to Iran).[93] Regarding the missile strike on *Sea Isle City*, the I.C.J. determined that, even cumulatively, there was insufficient severity to meet the threshold of an armed attack for two reasons.[94] Firstly, the missile could not have been aimed precisely at the vessel, but only at the Kuwait Harbor generally.[95] Secondly, an attack on a private vessel not flying a state's flag could not be interpreted as an attack on the flag-state.[96] In relation to the USS *Samuel B. Roberts*, the I.C.J. declined to determine whether mining a single military vessel constituted an armed attack, but did not exclude the possibility that it could.[97]

2. Application

The chief executive of international cable telecommunications company Seacom, Byron Clatterbuck, is skeptical about the possibility of an attack on cable causing a major outage.[98] For example, the fact that the United Kingdom is connected to more than 50 submarine cables means that an attack would need to be executed simultaneously on multiple cables in order to be effective.[99] Clatterbuck's point is strong for highly-connected countries such as the United Kingdom and the United States (which is connected to approximately 40 cables).[100] The difficulty inherent in sabotaging a sufficient number of cables to thwart telecommunications service means that it is unlikely that such countries would ever suffer an attack on their cables of sufficient severity to properly constitute an "armed attack." Additionally, submarine cables normally operate with reserve

91. Nicar. v. U.S., 1986 I.C.J. at 191.

92. *See* GRAY, *supra* note 50, at 139.

93. Iran v. U.S., 2003 I.C.J. at 191.

94. *Id.*

95. *Id.*

96. *Id.*

97. *See id.* at 195.

98. James Griffiths, *The Global Internet is Powered by Vast Undersea Cables. But They're Vulnerable*, CNN (July 26, 2019, 11:30 AM), https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html.

99. *Id.*

100. *See* DOUGLAS R. BURNETT & LIONEL CARTER, INTERNATIONAL SUBMARINE CABLES AND BIODIVERSITY OF AREAS BEYOND NATIONAL JURISDICTION 4 (2017).

capacity, so states with a multitude of cables (such as the United Kingdom) would be able to simply increase the capacity of their remaining cables in the event of an attack.[101] Moreover, states with access to other cable systems pursuant to mutual restoration agreements can access those in the event of a cable fault. Moreover, states with access to other cable systems pursuant to mutual restoration agreements can access those in the event of a cable fault.[102]

However, Clatterbuck's point is less applicable to smaller countries with few submarine cable connections. For example, New Zealand is connected to the outside world through five submarine cables, which all land in or near Auckland.[103] Only two submarine cables connect the South Island to the smaller North Island (and consequently the rest of the world).[104] It is therefore foreseeable that an attack on even one of the submarine cables connecting New Zealand would have a significant effect on its telecommunications—particularly given that it also has no land borders and therefore could not gain alternative telecommunications access through land cables in an emergency.[105] Furthermore, a coordinated attack on all of its cables would be much more achievable, due to there being only five. The same would be true for numerous other states—particularly those that are small, remote and/or island states (for example, Kiribati is only connected to one submarine cable)[106] or those with aforementioned "chokepoints."[107]

The effects of a near or total shutdown on a smaller, less well-connected state could be catastrophic, with a shutdown lasting for several days or even weeks.[108] Although there have been some suspected intentional cable attacks (by individuals), these mostly occurred in the 2000s.[109] Given that usership of the Internet is increasing at approximately ten percent annually,[110] analysis of the effects of the most recent government-enforced domestic internet shutdowns provide more assistance in determining the grassroots gravity of

101. *See* SUNAK, *supra* note 17, at 21 (discussing the spare capacity to reroute cables between the United States and United Kingdom in the event of an attack).

102. *See* Davenport, *supra* note 2, at 78 (discussing states that use the same network operating center).

103. *See Submarine Cable Map*, *supra* note 24.

104. *Id.*

105. SUNAK, *supra* note 17, at 18.

106. *Id.*

107. Tsuruoka, *supra* note 69.

108. *Key Actions to Protect Submarine Cables from Criminal Activity Identified at UNODC Global Expert Meeting*, U.N. OFFICE ON DRUGS & CRIME (Feb. 7, 2019), https://www.unodc.org/unodc/en/frontpage/2019/February/key-actions-to-protect-submarine-cables-from-criminal-activity-identified-at-unodc-global-expert-meeting.html.

109. *See* Davenport, *supra* note 2, at 80–81.

110. INT'L TELECOMM. UNION, *supra* note 4.

an internet shutdown. It is important to note, however, that these consequences are only relevant to states that would have essentially no access to the Internet if their cables were cut. Large states with vital servers located there, such as the United States, would not be so affected, as internal internet communications would still both function *and* have utility.[111] As such, a state such as the United States would likely have difficulty in proving sufficient gravity in the absence of a widespread, coordinated attack.

3. Consequences of Internet Shutdowns

India is by far the world's most frequent deployer of domestic internet shutdowns, with approximately two-thirds of 2018 shutdowns occurring there.[112] In early August 2019, the Government of India shut down internet and phone service in the then-state of Jammu and Kashmir for at least two weeks.[113] While Kashmiris were unable to access news media, both houses of the Parliament of India passed the Jammu and Kashmir Reorganisation Act, which demoted the state from full state status to two mere 'union territories' (Jammu and Kashmir, and Ladakh).[114] Although this denial of civil and political rights is distinct to national security concerns, it demonstrates the severity of what can be achieved while people are unable to mobilize and communicate. In the context of an attack on submarine cables, this example highlights the likelihood that a state would be unable to effectively mobilize its military reservists and communicate any national security threats to other parts of the country. This would be of grave concern to any state experiencing a near or total internet shutdown.

Moreover, such a shutdown would have grave impacts for people. Eleven days into the shutdown in Kashmir, *The New York Times* documented that shopkeepers were running short on vital supplies, such as insulin and baby food, as they usually ordered them online.[115] The shutdown forced banks and automated teller machines—which are reliant on the Internet for all transactions—to close, causing shortages of cash (which Kashmiris no

111. *See* Louise Matsakis, *What Would Really Happen If Russia Attacked Undersea Internet Cables*, WIRED (Jan. 5, 2018, 7:00 AM), https://www.wired.com/story/russia-undersea-internet-cables/.

112. ACCESS NOW, THE STATE OF INTERNET SHUTDOWNS AROUND THE WORLD 2 (2019). For a report on internet shutdowns in India, *see generally* SOFTWARE FREEDOM LAW CTR., INDIA, LIVING IN DIGITAL DARKNESS: A HANDBOOK ON INTERNET SHUTDOWNS IN INDIA (2018).

113. *See* Vindu Goel et al., *India Shut Down Kashmir's Internet Access. Now, 'We Cannot Do Anything.'*, N.Y. TIMES (Aug. 14, 2019), https://www.nytimes.com/2019/08/14/technology/india-kashmir-internet.html.

114. Jammu and Kashmir Reorganisation Act, 2019, No. 34, Acts of Parliament, 2019 §§ 3–4 (India).

115. Goel et al., *supra* note 113.

doubt required to purchase necessary supplies while the shutdown rendered card payment unavailable).[116]

In Zimbabwe, the government shut down the Internet for six days in January 2019.[117] The difficulty in making required payments and communicating with business partners caused one fuel merchant, for example, to lose his contract with a South African supplier.[118] This meant that he had to make 27 of his 35 workers redundant, close three of his four branches and lose 90 percent of his monthly profits.[119] People were unable to purchase food without a functional electronic payment system.[120]

In Sudan, the military junta that assumed governance following the 2019 Sudanese coup d'état shut down the Internet for an entire month.[121] Doctors were unable to order new medicine, causing a shortage of supplies for treatment of diabetic patients.[122] Meanwhile, protest leaders in the Sudanese Revolution were unable to use WhatsApp to request medical assistance.[123]

4. Analysis

In light of the above, a cable attack would have catastrophic effects on a state that would endure a near or full internet shutdown for longer than a few days. This fact is best stated by Robert Fonow, who summarized the consequences that would ensue if a "chokepoint" cable landing site was attacked:

> [C]ascading failures could immobilize much of the international telecommunications system 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 transactions and international bank reconciliations would slow to a crawl. When apprised of this possibility, a senior official

116. *Id.*

117. Patrick Kingsley, *Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards*, N.Y. TIMES (Sept. 2, 2019), https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html.

118. *Id.*

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *See id.*

> of The Economist in London suggested that such an event would cause a global depression.[124]

In this respect, the potentially catastrophic effects of a cable attack are much graver than the effects of wiretapping submarine cables, which has been perceived to not amount to an "armed attack" for the purposes of Article 51.[125] The key difference is that wiretapping only compromises a state's privacy and creates a risk to national security, whereas a cable attack is an actual attack on critical telecommunications infrastructure that has immediate effects on a state, its people and its economy. Hence, a cable attack is essentially the equivalent of a missile strike on other critical state infrastructure, such as energy production plants, as opposed to intelligence-gathering. It is notable that the authors of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* agreed that a cable attack by a state would violate international customary law, whereas wiretapping submarine cables is permissible.[126]

Despite the I.C.J.'s aforementioned note in *Oil Platforms* that there could not be an armed attack on a private ship not displaying its flag, the fact that submarine cables are privately-owned and not flagged to a state does not defeat the potential for a cable attack to constitute an armed attack. A state executing a cable attack would surely know exactly which state's or states' connections it was severing.[127] Moreover, a strike on one private vessel is more likely to be perceived as similar to a "cross-border skirmish" that does not amount to an armed attack, due to its effect on only one ship; whereas a cable attack is an attack on a state's critical infrastructure and could affect the entire victim state.

In light of the above, a cable attack will meet the gravity requirement if it causes a severe reduction in a state's access to the Internet and other telecommunications for a substantial period of time. A bright-line test is inappropriate, however, as circumstances will vary between attacks.

---

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

125. *See* Davenport, *supra* note 2, at 101; Pete Barker, *The Challenge of Defending Subsea Cables*, MAR. EXEC. (Mar. 20, 2018, 9:27 AM), https://www.maritime-executive.com/editorials/the-challenge-of-defending-subsea-cables.

126. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 257 (Michael N. Schmitt ed., 2d ed. 2017) ("The rules and principles of international law applicable to submarine cables apply to submarine communication cables.").

127. The locations and routes of submarine cables are publicly available. *See Submarine Cable Map*, *supra* note 24.

VI. LEGAL USE OF FORCE IN SELF-DEFENSE

A. Necessity & Proportionality

A state that suffers a sufficiently grave cable attack, that can be attributed to another state, will need to quickly determine whether it is necessary to use force in self-defense and what level of force is proportionate. Although the I.C.J. treats necessity and proportionality separately, they are considered together here because the concepts are, in practice, entwined.[128]

Necessity can be defined as "the requirement that no alternative response to an armed attack be possible."[129] Meanwhile, proportionality relates "to the size, duration, and target" of the use of force in response.[130] Christine Gray notes that there is consensus among scholars about some principles regarding these requirements: "necessity and proportionality mean that self-defense must not be retaliatory or punitive; the aim should be to halt and repel an attack."[131] Nonetheless, "the defending state is [not] restricted to the same weapons or the same numbers of armed forces as the attacking state; nor is it necessarily limited to action on its own territory."[132]

1. Previous Cases

Nonviolent aid will not justify the use of force. Despite finding that the United States did have a right to use self-defense under Article 51, the I.C.J. still considered necessity and proportionality in *Nicaragua*.[133] Regarding necessity, the I.C.J. held that U.S. force against Nicaragua was unnecessary to protect the Government of El Salvador because the armed rebellion against that government had already been defeated some months prior.[134] Regarding proportionality, it determined that the United States' response, in mining and attacking Nicaraguan ports, was not proportionate to Nicaraguan aid for El Salvadorian rebel groups.[135] This case clearly establishes that the use of force in response to nonviolent aid will not be a proportionate response.[136]

---

128. *See* GRAY, *supra* note 50, at 159.
129. *Id.*
130. *Id.*
131. *Id.*
132. *Id.* at 159–60.
133. Nicar. v. U.S., 1986 I.C.J. at 237.
134. *Id.*
135. *Id.*
136. *See id.*

In *Oil Platforms*, the I.C.J. rejected the necessity of the United States' targeting of oil platforms, as the United States had not complained to Iran of military activities on the platforms (whereas it had complained of minelaying and attacks on neutral shipping).[137] The failure to raise the matter with Iran in such a way "does not suggest that the targeting of the platforms was seen as a necessary act."[138] The I.C.J. further considered that it was possible that the United States' response to the *Sea Isle City* attack was proportionate, but its response to the *USS Samuel B. Roberts* striking a mine could not be proportionate.[139] That was because the mine did not sink the ship and did not cause loss of life, whereas the United States' response destroyed two Iranian frigates and several other naval vessels and aircrafts.[140]

Armed Activities provides another example of a disproportionate response to an armed attack. The I.C.J. observed that "the taking of airports and towns many hundreds of kilometers from Uganda's border would not seem proportionate to the series of transborder attacks it claimed had given rise to the right of self-defense, nor to be necessary to that end."[141]

2. Application

Necessity could be challenging to satisfy in the event of a cable attack, given the practical difficulty that a victim state could face in exhausting diplomatic avenues when its means of international communication are severely limited. Nevertheless, it would seem counterintuitive to allow an aggressor state to claim that diplomatic avenues had not been exhausted, if it was responsible for making those avenues impossible to exhaust in the first place. It is therefore expected that the concept of necessity could be applied with a practical bent in the case of a cable attack. Thus, in the event that diplomatic communications are not possible, it is likely that it would be permissible for a victim state to neutralize any naval vessels of the aggressor state *if* they posed an imminent threat.

Separately, in light of the I.C.J.'s finding in *Oil Platforms* as to disparaging human consequences of attacks, a victim state could encounter difficulty regarding proportionality if its use of force caused unnecessary loss of life. This is because, despite the criticality of the Internet to states, their people, and economies, a cable attack alone (without other use of force) would likely need to cause several weeks of non-connectivity for any loss of life to occur.

137. Iran v. U.S., 2003 I.C.J. at 198.

138. *Id.*

139. *Id.* at 198–99.

140. *Id.*

141. Dem. Rep. Congo v. Uganda, 2005 I.C.J. at 223.

As such, states acting in self-defense must be aware of their duty to exhaust all other avenues first (to the extent possible in the absence of international telecommunications) and must be very cautious to avoid loss of human life and disparaging damage to infrastructure.

B. A Bona Fide Military Target

In *Oil Platforms*, the legitimacy of the United States' targeting of oil platforms was at issue. The parties agreed that Iranian military personnel and equipment were present on some of the platforms, but differed as to whether Iran's motive in arranging that was aggressive or defensive.[142] The I.C.J. held that the United States presented insufficient evidence to support its contentions as to the significance of Iran's military presence and activity on the platforms.[143]

In light of reports of China and Iran using civilian vessels as quasi-naval vessels in the South China Sea and Persian Gulf respectively,[144] it is foreseeable that an attack on submarine cables might be executed by non-naval or unflagged ships. In this regard, a relevant principle is the I.C.J.'s determination in *Nicaragua* that "'the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to' (*inter alia*) an actual armed attack conducted by regular forces, 'or its substantial involvement therein'" can amount to an armed attack.[145]

Given the requirement that targets be bona fide military targets, it is unlikely that it would be lawful to attack the aggressor state's submarine cables, as they are generally privately-owned and transmit primarily civilian and commercial data. Even if the aggressor state owned the cables landing there, that would not make them legitimate military targets in the same way that other non-military, publicly owned assets, such as public hospitals, would not be legitimate military targets. Moreover, cutting submarine cables in retaliation would likely cause a loss of bandwidth in third-party countries, too. It would also give the aggressor state an offsetting claim in any resulting lawsuit for compensation in the I.C.J.

In conclusion, a victim state with the right to use force in self-defense should target only military (or military-instructed) vessels or other infrastructure capable of causing further or repeat damage to submarine cables.

142. Iran v. U.S., 2003 I.C.J. at 161, 196–97.

143. *Id.* at 198.

144. *See* SUNAK, *supra* note 17, at 10.

145. Nicar. v. U.S., 1986 I.C.J. at 195.

C. The Duty to Report

As a final note, it is important for states to comply with their Article 51 duty to report the use of force in self-defense to the U.N. Security Council.[146] In *Armed Activities*, the I.C.J. "observe[d]" that Uganda did not report its retaliatory actions in claimed self-defense to the U.N. Security Council.[147] However, the "observation" has been interpreted as the I.C.J. clearly implying that this was a factor indicating noncompliance with Article 51.[148] Accordingly, victim states should practice care in reporting to the U.N. Security Council as soon as they can transmit communications to their diplomatic missions at the United Nations.

VII. CONCLUSION

Whether or not a state will be daring enough to execute a malicious attack on the submarine cable system remains to be seen. Nevertheless, states—particularly those with few cables or cable "chokepoints"—would be prudent to prepare their defense strategies and legal justifications for the unlikely event that such an attack occurs. This is of critical importance, with people, economies and national security becoming ever-more dependent on the Internet.

In order to use force in self-defense, a state that suffers from the effects of a cable attack will firstly need to prove that the attack was an intentional act of another state (as opposed to accidental or environmentally-caused damage) and that the alleged state was, in fact, responsible. Secondly, the cable attack must cause a severe reduction in the victim state's access to the Internet and other telecommunications for a substantial period of time. Anything less would likely be a matter to be resolved through diplomatic processes. Only if a victim state can establish these two elements will it be able to prove that it has suffered an "armed attack" to which it can respond with force in self-defense pursuant to Article 51 of the U.N. Charter.

Highly connected states, such as the United States and United Kingdom, are unlikely to be able to meet this threshold unless they suffer a truly severe attack. Pacific Island states, in comparison, will likely meet this threshold in the event that one or a handful of cables are attacked.

If a victim state establishes the right to self-defense, it may only use force if it is necessary and if it does so in a manner that is proportionate to the attack(s) it has suffered. Victim states wishing to use force in self-defense will need to exercise caution in not acting too hastily (so as to not have

146. U.N. Charter art. 51.

147. Dem. Rep. Congo v. Uganda, 2005 I.C.J. at 222.

148. GRAY, *supra* note 50, at 129.

exhausted all other options) nor too late (so as to have lost the necessity of using force). They will also need to be careful to avoid human casualties, given the likelihood that an initial cable attack will not cause casualties. The victim state may also attack only legitimate military targets, which would likely not include the aggressor state's submarine cables.

As a final note, states considering engaging in cable attacks should be cognizant of the likelihood that victim states will contend that such attacks amount to an "armed attack" pursuant to Article 51 of the U.N. Charter—even if they do not meet the threshold set out above.[149]

149. *See, e.g., Request for Information: Critical Foreign Dependencies (Critical Infrastructure and Key Resources Located Abroad)*, *supra* note 31 (indicating the seriousness with which the United States, for example—a highly connected country—would likely consider an attack on its "critical infrastructure").