The Targeting of Undersea Communications Cables: Armed Conflict, Developing States, & the Need for a TWAIL Approach

Stephen Floyd*

Abstract

800,000 miles of undersea communications cables cross the ocean floor and bind the world together. Modern society increasingly depends on these fragile fiber optic tubes for economic growth, effective governance, and critical services. But while wealthy states in the "global north" enjoy redundant cable connections, much of the developing world lacks such robust infrastructure. Indeed, for many low-income states, a single fault can disrupt telecommunications and wreak havoc across an entire region.

Yet despite their critical importance, undersea communications cables receive no special protection under international humanitarian law (IHL). Some states, like Russia, have reportedly developed dedicated capabilities to target cables in international waters during armed conflict, and non-state actors have demonstrated the capacity to do so in the littoral zone. In the developing world, such attacks could have devastating effects for civilians, non-combatants, and neutral states. Nevertheless, the targeting of undersea cables may be justified under existing IHL targeting principles that emphasize military necessity and fail to consider non-lethal, second-order effects. The developing world requires a new approach for the digital

---

* The author served as an active-duty naval intelligence officer for thirteen years and is currently a Lieutenant Commander in the United States Navy Reserve. He holds a joint J.D./LL.M. in National Security Law from Georgetown University Law Center and practices national security law for an international law firm. The author would like to express his profound thanks to Professor David Koplow for his guidance and support in writing this article. The views expressed in this article are those of the author and do not reflect the official policy or position of the firm or its clients, the Department of Defense (DoD), or the U.S. Government. The appearance of external hyperlinks does not constitute DoD endorsement of the linked website or information contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

age.

Employing a Third World Approach to International Law (TWAIL) framework, this paper argues that regional courts and local jurists are best positioned to interpret IHL in ways that reflect the developing world's unique circumstances. For what constitutes a lawful attack among advanced industrial economies may have very different consequences for the world's most vulnerable populations. After reviewing current IHL treatment of undersea cables and dual-use infrastructure, the paper considers the African Commission on Human and Peoples' Rights as a case study. Although the Commission lacks binding authority, it possesses a broad mandate to consider IHL and international human rights law together and has found that the African Charter's economic and social rights cannot be derogated during armed conflict. For this reason, the Commission is well situated to consider attacks on dual-use telecommunications infrastructure, articulate an IHL approach that respects the 21st-century needs of developing states, and protect digital access for civilians and non-combatants. Though non-binding, such a statement might catalyze the emergence of new customary international law norms and an IHL regime founded in truly global values.

INTRODUCTION

On January 15th, 2022, Tonga's 100,000 citizens abruptly lost internet connectivity with the outside world. A submarine volcano had violently erupted in the South Pacific and spawned a cataclysm of damage. As Hunga Tonga-Hunga Ha'apai sent particles into the upper atmosphere, thick layers of ash soon blanketed the island nation. Water supplies were disrupted. Crops were ruined.[1] The explosion's shock wave circled the globe,[2] and the tsunami it triggered killed three people, damaged 600 structures, and devasted entire Tongan villages.[3] But some damage was not so easily seen. As the ash settled,

1. Press Release, Tonga Volcanic Eruption and Tsunami: World Bank Disaster Assessment Report Estimates Damages at US$90M, WBG (Feb. 14, 2022), https://www.worldbank.org/en/news/press-release/2022/02/14/tonga-volcanic-eruption-and-tsunami-world-bank-disaster-assessment-report-estimates-damages-at-us-90m#:~:text=Around%20600%20structures%20in%20total,homes%20destroyed%20or%20severely%20damaged.

2. Alexandra Witze, *Why the Tongan Eruption Will Go Down in the History of Volcanology*, NATURE (Feb. 9, 2022), https://www.nature.com/articles/d41586-022-00394-y.

3. *Tonga Volcano: New Images Reveal Scale of Damage after Tsunami*, BBC NEWS (Jan. 19, 2022), https://www.bbc.com/news/world-asia-60034179.

Tongans discovered that they had lost connectivity to the wider world. For far beneath the ocean's surface, the eruption had severed the submarine telecommunications cables connecting Tonga with the rest of humanity.[4] In all, the tsunami damaged 56 miles of cable.[5] With the closest cable repair ship 2,900 miles away,[6] a people struggling to rebuild lacked reliable internet and telephone service for five weeks.[7]

Mother Nature bore responsibility for Tonga's sudden isolation. But the eruption demonstrates the critical importance of subsea telecommunications infrastructure, highlights its fragility, and suggests its potential as a military target. Indeed, on the eve of Russia's Ukraine invasion, Moscow announced its intention to conduct naval exercises near transatlantic cables in Ireland's Exclusive Economic Zone. According to Irish military officials, Moscow wanted NATO to understand that it could "cut [the cables] anytime they want."[8] In recent years, policy makers have paid increased attention to such vulnerabilities, and pundits frequently cite the threat potential adversaries pose to undersea cables.[9] But this risk is not new.

Belligerents have targeted undersea cables for more than a century. In fact, the United States employed such tactics to great effect during the Spanish-American War, while British and German forces conducted similar attacks in World War I. International humanitarian

---

4. Linny Folau, *Additional Breaks to Tonga Cable Push Repair Date Back*, SUBMARINE TELECOMS F. (Feb. 9, 2022), https://subtelforum.com/additional-breaks-to-tonga-cable-push-repair-date-back/.

5. *Tonga's Internet is Restored Five Weeks After Big Volcanic Eruption*, NPR (Feb. 22, 2022), https://www.npr.org/2022/02/22/1082483555/tongas-internet-restored-5-weeks-after-big-eruption.

6. Jane Wakefield, *How Will Tonga's Broken Internet Cable be Mended?*, BBC NEWS (an. 24, 2022), https://www.bbc.com/news/technology-60069066.

7. NPR, *supra* note 5.

8. Conor Gallagher & Simon Carswell, *Russian Naval Drills to Still Take Place over Vital Cables, Experts Believe*, THE IRISH TIMES (Jan. 31, 2022 07:44 A.M.), https://www.irishtimes.com/news/environment/russian-naval-drill-to-still-take-place-over-vital-cables-experts-believe-1.4789421; *see also* Justin Sherman, *Cord-Cutting, Russian Style: Could the Kremlin Sever Global Internet Cables?*, NEW ATLANTICIST (Jan. 31, 2022), https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/ ("[i]n the most globally damaging scenario, the Russian military could target any of the dozens of submarine cables linking other parts of Europe to the global internet . . . to damage global internet traffic . . . and distract those countries from other world events.").

9. *See e.g.*, Presidential Directive on Critical Infrastructure Security and Resilience, 2013 Daily Comp. Pres. Doc. 92 (Feb. 12, 2013) (calling for a "national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure").

law did not prohibit these attacks, and such actions are not off-limits under international humanitarian law (IHL) today. The cables provided a clear military advantage, and the attacks posed little harm to civilians.

But while submarine cables still constitute targets of military value, their social and economic importance has changed dramatically. In 1898, the technology was only thirty years old. Sending trans-oceanic telegraphs was slow and remained the exclusive province of governments and elites.[10] In 2022, however, 800,000 miles of fiber optic cable (FOC) crisscross the ocean floor.[11] Private commerce, government administration, and essential services depend on these hair-width glass fibers that transmit 160 terabits of data per second.[12] Billions of civilians rely on undersea FOC for cellular connectivity and internet access. Critical government services require data stored in overseas sites, and financial transactions necessitate instantaneous connectivity to international banks and markets.[13] Moreover, militaries, diplomats, and intelligence agencies rely on undersea cables to execute foreign policy and coordinate operations.

If a belligerent severed these undersea links, the consequences would be widespread. Military forces might lose access to vital intelligence or lack guidance from higher headquarters. But civilians would suffer the most. Financial transactions could grind to a stop. Critical infrastructure could fail. Essential services could fall into disarray. Such sweeping effects implicate the IHL principle of proportionality, which seeks to balance military necessity with the protection of neutrals and non-combatants. Yet despite growing importance of subsea cables, the legal regime governing their

---

10. THREATS TO UNDERSEA CABLE COMMUNICATIONS, OFF. OF THE DIR. OF NAT'L INTEL. PAPER 37 (Sept. 28, 2017) (noting that it took sixteen hours to transmit the first 99-word transmission between Queen Victoria and President Buchanan in 1858), https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf.

11. James Griffiths, *The Global Internet is Powered by Vast Undersea Cables. But They're Vulnerable*, CNN (July 26, 2019, 7:30 AM), https://www.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html.

12. *Id.*

13. SUSAN ARIEL AARONSON, DATA IS A DEVELOPMENT ISSUE, (2019) (noting that "in many developing countries, the infrastructure is in the cloud and the cloud servers are located abroad – most likely in industrialized countries."); *Strategic Importance of, and Dependence on, Undersea Cables,* NATO COOP. CYBER DEF. CTR. OF EXCELLENCE (Nov. 2019) ("[m]odern societies put more and more emphasis on cloud computing . . . [t]he cloud . . . in reality . . . may be on another continent but linked to you via cables."), https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.

targeting has not evolved since the age of telegraphs. This incongruence threatens global society as a whole, but the citizens of developing nations and geographically isolated states are vulnerable most of all.

IHL targeting principles must adapt to new technological realities to address the needs of vulnerable populations. Like Tonga, low-income states often lack redundant undersea cable connections and rarely possess dedicated infrastructure for military communications. In such situations, an attack on undersea cables can have far-reaching, indiscriminate effects for the civilian population. Therefore, targeting analysis must fully account for the critical role undersea infrastructure provides for a region's social and economic life and holistically consider an attack's second-order effects on non-combatants. To be sure, submarine cables support military command and control and will often constitute a lawful military target. As such, an outright prohibition on attacks would prove naïve and unworkable. But a more nuanced proportionality analysis could broadly consider a cable's importance and reflect the unique aspects of communications infrastructure in the developing world.

IHL seeks to assuage humanity's worst impulses, and its precepts provide a civilizing restraint during civilization's darkest moments. But IHL emerged from the European and American experience of war, and Western jurists have predominantly shaped its contours. This perspective matters. As the targeting of dual-use infrastructure like undersea cables demonstrates, armed conflict affects civilians in low-income states differently than in the rich, industrialized world. Third World Approach to International Law (TWAIL) theorists seek to rectify this imbalance. Highlighting non-Western jurisprudence, TWAIL scholarship incorporates underrepresented perspectives to inform the development of international law. While increasingly common in fields like international economic law, TWAIL has had limited influence on IHL scholarship and jurisprudence. But such voices are the best way for IHL to ensure its precepts reflect on-the-ground realities and effectively protect vulnerable populations during armed conflict.

In part one, the paper provides an overview of submarine communications cables and outlines their critical importance for modern society. Part two then discusses historic attacks on submarine cables and contemporary threats to this critical infrastructure. The United States, Germany, and the United Kingdom have all targeted cables in conflict, and Russia has reportedly developed an array of surface and subsurface capabilities to threaten undersea infrastructure; however, less well-resourced states and even non-state actors can easily sever cables in the littoral as well.

After a brief examination of the legal framework that protects cables during peacetime, the third part therefore explores how IHL governs the targeting of submarine cables during armed conflicts. Without recognizing the widespread importance of today's subsea telecommunications infrastructure, the existing IHL framework fails to address the devastating second-order effects undersea cable attacks could have on neutrals and non-combatants.

Part four then weighs recent legal and policy proposals to address these gaps, to include cable protection zones, an expanded definition of piracy, flag-state liability for economic damages, and the designation of cable-repair ships as neutral vessels. Unfortunately, while such proposals may help, they do not provide a holistic solution to the problem. They either require sweeping changes that would prove unworkable or fail to address the specter of attacks during armed conflict.

Ultimately, the paper concludes that existing IHL principles for targeting dual-use infrastructure can suffice; however, they require a broader interpretative lens that incorporates emerging human rights norms and better accounts for second-order effects on non-combatants and neutrals. A TWAIL approach can provide that lens. Using the African Commission on Human and Peoples' Rights as a case study, part five argues that regional bodies empowered to consider both international human rights law (IHRL) and IHL are well positioned to lead on this front. They can give voice to populations most vulnerable to such adverse effects, and their mandate enables them to fuse IHL principles with international human rights law. Such an approach could forge new norms to govern armed conflict and might someday constitute a foundation for new customary international law.

I. BACKGROUND ON CABLES

A. WHY CABLES MATTER

Undersea cables gird the globe together. Although hidden beneath the waves, they constitute "the true skeleton and nerve of our world."[14] More than seven hundred thousand miles of fiber optic

14. Press Release, United Nations General Assembly, General Assembly Concludes Annual Debate on Law of the Sea Adopting Two Texts Bolstering United Nations Regime Governing Ocean Space, its Resources, Uses, U.N. Press Release GA/11031 (Dec. 7, 2010), http://www.un.org/News/Press/docs/2010/ga11031.doc.htm.

cables (FOC) span the ocean floor,[15] and much of modern civilization rests upon this oft-forgotten foundation.[16] Ninety-nine percent of intercontinental communications travels across the submarine FOC infrastructure,[17] and satellites could support only a small fraction of this bandwidth in their absence.[18] Such infrastructure is of critical importance to 21st century military, diplomatic, and intelligence efforts. While military assets still employ radio and satellite-based communications for tactical coordination, their leaders inevitably rely on undersea cables to receive and transmit vast amount of digital data that guide decision making. Indeed, one U.S. military officer has observed that "the Department of Defense's net-centric warfare and Global Information Grid rely on the same undersea cables that service the information and economic spheres."[19] If those cables were cut, "the capability of modern U.S. warfare that encompasses battle space

---

15. James Kraska, *The Law of Maritime Neutrality and Submarine Cables*, EUR. J. OF INT'L L.: TALK! (July 29, 2020) [hereinafter Kraska], https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejil-talk-newsletter-post-title_2.

16. "We live in an age where the Internet constitutes critical infrastructure for many (possibly almost all) aspects of society. Reliable internet access has become a key necessity for . . . economic activity, education, political involvement, and provision of government services. Such internet access is underpinned by submarine cables." *See* Tamsin Phillipa Paige et al., *The Final Frontier of Cyberspace: Ensuring that Submarine Data Cables are Able to Live Long and Prosper (Part I)*, OPINIO JURIS (Oct. 20, 2016), http://opiniojuris.org/2020/10/16/the-final-frontier-of-cyberspace-ensuring-that-submarine-data-cables-are-able-to-live-long-and-prosper-part-i/.

17. Doug Brake, *Submarine Cables: Critical Infrastructure for Global Communications*, INFO. TECH. & INNOV. FOUND. (Apr. 2019), http://www2.itif.org/2019-submarine-cables.pdf ; NATO COOP. CYBER DEF. CTR. EXCELLENCE, *supra* note 13 (stating that cables carry greater than ninety-seven percent of global internet traffic).

18. Douglas Burnett et al., *Why Submarine Cables? in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 3 (Douglas R. Burnett et al. eds., 2014) (noting that transmission delays and other technical limitations mean that "every single satellite in the sky" could only accommodate seven percent of U.S. internet traffic in the absence of undersea cables). Of note, private industry is actively pursuing the commercialization of low earth orbit communications satellites. Such constellations could provide internet access with much shorter delays than standard high earth orbit constellations. If successful (and affordable), the technology could also facilitate access to millions of people in isolated areas that lack terrestrial infrastructure, such as large portions of the developing world. Nevertheless, wide-spread, cost-effective implementation remains several years away. Moreover, the IHL targeting issues discussed in this paper are as relevant to communications satellite as they are for undersea cables. For a discussion of this technology, WORLD ECONOMIC FORUM, *How Low-Earth Orbit Satellite Technology Can Connect the Unconnected (Feb. 18, 2022)*, https://www.weforum.org/agenda/2022/02/explainer-how-low-earth-orbit-satellite-technology-can-connect-the-unconnected/.

19. Michael Matis, *The Protection of Undersea Cables: A Global Security Threat*, U.S. ARMY WAR COLL. PROJECT 10 (Mar. 07, 2012), https://apps.dtic.mil/sti/pdfs/ADA561426.pdf.

communications . . . would be at risk."[20] Diplomatic cable traffic, near-real-time video feeds from unmanned aerial vehicles, and a host of other capabilities rely on this submarine infrastructure.

To be sure, some wealthy countries may lay dedicated undersea cables to facilitate sensitive strategic communications. In such instances, there is no question that an attack on military-operated cables would constitute a lawful target during armed conflict. But the situation is rarely so clear cut. A significant portion of U.S. and allied military communications ultimately relies on the same backbone as private citizens and commercial actors.[21] Furthermore, the dual military-civilian use of undersea communications infrastructure is undoubtedly even more pronounced for developing countries that lack the resources for parallel military systems. Thus, any targeting decision must account for the vital non-military data that transits cables.

Without undersea cables, the global economy could not function. As the former Federal Reserve Chairman's Chief of Staff remarked in 2012, "[w]hen communications networks go down, the financial services sector does not grind to a halt, rather it snaps to a halt."[22] Every day more than $10 trillion in global commerce transits submarine cables.[23] For instance, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) transmits 20 million messages to over 8,000 financial institutions across the globe.[24] Similarly, financial markets rely on Intercontinental Exchange, a global network of currency exchanges, to execute more than ten million contracts every day.[25] Such instantaneous transactions are not possible without the undersea cable networks,

---

20. *Id.*

21. *See Id.*; Sean O'Malley, *Vulnerability of South Korea's Undersea Cable Communications Infrastructure: A Geopolitical Perspective*, 50 KOR. OBSERVER (2019) ("[a]s an isolated, peninsular state surrounded by rivals and aggressors, South Korea depends heavily on these cables, which carry everything from financial transactions to critical military communications."); Brendan Nicholson, *Undersea Cables Key to Security*, THE AUSTRALIAN (Sept. 2, 2011) (discussing the importance of undersea cable to Australian defense efforts).

22. Stephen Malphrus, Keynote Address at the Reliability of Global Undersea Communication Cables Infrastructure Summit (Oct. 19, 2009).

23. 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?searchResultPosition=1.

24. Robert Martinage, *Under the Sea: The Vulnerability of the Commons*, 94 FOREIGN AFF. 117, 119 (Jan. 2015), http://www.foreignaffairs.com/articles/142491/robert-martinage/under-the-sea.

25. *Id.*

and their swift execution is critical to the global economy. Deloitte estimates that a temporary internet shutdown would cost a highly connected country $23.6 million per 10 million people per day.[26] Even for countries with low-to-medium levels of connectivity, internet commerce still constitutes between 2.3 and 5.2 percent of GDP, and the effects of a temporary shutdown might cost .6 million dollars per 10 million people per day.[27] Furthermore, even partial disruptions would exact a significant toll. According to Deloitte, a 30% or 50% reduction in internet speed for 10 million people would result in a .09% to .15% loss of daily GDP.[28]

Undersea cables also provide the broadband internet access and mobile connectivity on which government services, domestic jobs, and civil society increasingly rely. The Covid 19 pandemic highlighted the vital role such access plays in the developed world, as business meetings, school classrooms, and government hearings shifted to an online environment. But the potential benefits are even greater in developing and least developed countries.[29] The proliferation of mobile phones has enabled wide-spread access to banking services,[30]

---

26. The same study concluded that for "medium and low Internet connectivity economies" the cost would amount to $6.6 million per 10 million population and $0.6 million per 10 million population economies with the lowest levels of connectivity. DELOITTE, *The Economic Impact of Disruptions to Internet Connectivity: A Report for Facebook* 4 (Oct. 2016), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/economic-impact-disruptions-to-internet-connectivity-deloitte.pdf.

27. *Id.*

28. *Id.* at 7.

29. The United Nations Committee for Development defines Least Developed Countries (LDC) as "low-income countries which are highly vulnerable to economic and environment shocks." The U.N. reviews these designations every three years and employs three criteria: income per capita, human assets, and economic vulnerability. As of 2021, 46 states meet the criteria for LDC status. THE UN LEAST DEVELOPED COUNTRY CATEGORY, UNITED NATIONS: DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS. Similarly, the World Bank has begun to classify countries as low income, lower-middle income, upper-middle income, and high income. Nada Hamadeh, Catherine Van Rompaey & Eric Metreau, *New World Bank Country Classifications by Income Level: 2021-2022*, WORLD BANK BLOGS: DATA BLOG (July 01, 2021), HTTPS://BLOGS.WORLDBANK.ORG/OPENDATA/NEW-WORLD-BANK-COUNTRY-CLASSIFICATIONS-INCOME-LEVEL-2021-2022. To streamline readability, this paper will employ the terms "developing countries," "the developing world," and "low-income countries" to refer to both categories of states. Readers should bear the distinction in mind, however, as LDCs inevitably have fewer undersea cable landings and less redundant infrastructure than developing states. Thus, the risks discussed in this paper are even more acute for citizens living in LDCs.

30. *See e.g.*, Jay Rosengard, *A Quantum Leap over High Hurdles to Financial Inclusion: The Mobile Banking Revolution in Kenya*, HARVARD KENNEDY SCHOOL FACULTY RESEARCH WORKING PAPER SERIES 12 (June 2016), https://www.hks.harvard.edu/publications/quantum-leap-over-high-hurdles-financial-inclusion-mobile-banking-

facilitated entrepreneurship,[31] and fostered human rights accountability.[32] But high-bandwidth mobile connectivity depends on cellular towers connected to fiber optic cables.

Cable access engenders massive social benefits for LDCs and developing states in particular. RTI International, a nonprofit research institute, estimates that the 2Africa cable, a project slated for completion in 2023, will expand the availability of high-skilled jobs and improve public access to education and healthcare.[33] Cable access also benefits the labor market in the developing world. One study attributed Democratic Republic of Congo's (DRC) recent 8.2% increase in employment and 19% growth in GDP per capita to the 2012 landing of the West African Cable System, the country's first – and only - undersea cable connection.[34] The study also suggests that the submarine cable access can engender more responsive government, as the DRC parliament plans to expand terrestrial FOC networks and digitize an array of government services.[35] To be sure, broadband internet access is likely only one of many factors driving

---

revolution-kenya (finding that Kenyans with access to financial accounts increased by thirty-three percent between 2011 and 2014 due to mobile banking). Many praise the benefits of mobile banking for poorer citizens, praising the "magic . . . in its simplicity and low cost." Diana Brazzel, *How mobile banking is transforming Africa,* HARV. KENNEDY SCH. https://www.hks.harvard.edu/faculty-research/policy-topics/public-finance/how-mobile-banking-transforming-africa (last visited Feb. 20, 2023). But such simplicity belies the fact that mobile banking relies on undersea cables to connect the mobile tower and bank to international financial institutions.

31. Matthew Van Niekerk, *How Blockchain Can Help Dismantle Corruption in Government Services*, WORLD ECONOMIC FORUM (July 05, 2021), https://www.weforum.org/agenda/2021/07/blockchain-for-government-systems-anti-corruption/ (discussing the potential for blockchain-based digital services to mitigate public corruption, enhance property rights, streamline procurement processes, and ultimately encourage more citizens to participate in the broader economy).

32. See e.g., *Evidence Suggests Ethiopian Military Carried Out Massacre in Tigray*, BBC NEWS (Apr. 01, 2021), https://www.bbc.com/news/world-africa-56603022 (analyzing cell phone footage that appears to depict soldiers carrying out mass executions of unarmed men).

33. *Analysis of the Economic Impact of Subsea Internet Cables in Sub-Saharan Africa*, RTI INTERNATIONAL (Nov. 2020), https://www.rti.org/impact/analysis-economic-impact-subsea-internet-cables-sub-saharan-africa; *Economic Impact of 2Africa*, RTI INTERNATIONAL (Nov. 2020), https://www.rti.org/publication/economic-impact-2africa/fulltext.pdf.

34. Alan C. O'Connor et al., *Economic Impacts of Submarine Fiber Optic Cables and Broadband Connectivity in the Democratic Republic of Congo*, RTI INTERNATIONAL 16 (Nov. 2020), https://www.rti.org/publication/economic-impacts-submarine-fiber-optic-cables-and-broadband-connectivity-democratic/fulltext.pdf. Of note, the DRC does have indirect access to subsea cables via Rwanda and Zambia.

35. *Id.* Although telecommunications infrastructure remains woefully inadequate through much of the country, the DRC parliament has also passed laws to expand terrestrial FOC and bring these benefits to a larger swath of the population.

economic growth and more responsive governance. But it is surely a significant catalyst. Moreover, as infrastructure and services continue to evolve, the importance of undersea cable connections will only grow more important.

B. THE DESIGN AND USE OF UNDERSEA COMMUNICATION CABLES

At the outset, it is helpful to understand the function, design, and installation of undersea cables. Their unique attributes are relevant to their status as targets in armed conflict in several ways. First, although our digital lives rely on fiber optical cables, it is virtually impossible to predict how data will travel across any particular cable. When transmitting information across the internet, data are broken down into discrete packets.[36] But these packets do not travel together or transit any set route. Rather, complex algorithms select the most efficient path at any given moment. Thus, before being reassembled at a destination, each data packet will traverse its own unique route. This path often crosses borders and transits oceans.[37]

Similarly, while a 5G phone connects with the closest tower via microwave radiation, the digital information it transmits ultimately reaches its destination via fiber optic networks. Thus, if someone in New York uses a mobile phone to place an overseas call, that data will travel across an undersea cable. Likewise, as most of the world's data storage centers are located in North America and Europe, much of the world's access to the "cloud" relies on undersea cables.[38] For each of these scenarios, it is impossible to know what path data packets will take. Therefore, targeting cables inevitably affects neutral countries and non-combatants and implicates IHL.

Second, submarine telecommunication cable systems are also expensive to build. The creation of a new cable system – to include route planning, procurement of regulatory clearances, installation of the cable and associated repeaters, and the construction of cable landing stations - is an expensive endeavor, with costs approaching $1 billion.[39] For every new system, ships must first survey the route,

---

36. Lazaro Gamio, *How Data Travel Across the Internet*, WASHINGTON POST (May 31, 2015), http://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp/.

37. *Id; See also* Adam Satariano, *How the Internet Travels Across Oceans*, N.Y. TIMES (Mar. 10, 2019), https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html.

38. Petroc Taylor, *Number of Data Centers Worldwide in 2022, by Country*, STATISTA (Feb 10, 2023), https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/.

39. Mick Green, *The Submarine Cable Industry: How Does it Work? in* SUBMARINE

assess currents, and identify bottom topography that could cause breaks.[40] Due to the cost of laying cable, undersea cables invariably follow the most direct route between two points;[41] nevertheless, planners will seek to avoid geological impediments, such as areas of known seismic activity, sea pinnacles, and submarine sediment flows, as well as economic and political concerns like fisheries and contested waters.[42] However, every detour can cost $75,000 per additional kilometer.[43] For this reason, cables usually follow highly predictable routes across the ocean.

To defray these substantial costs, cable systems are often owned by multinational consortia.[44] With as many as forty stakeholders, such consortia mitigate the costs of developing and operating the cable systems. As there is no global registry of cable owners, the actual owners may be known only to the landing state (and ultimate ownership may remain opaque even then).[45] Additionally, owners subsequently lease their rights to other companies, and this arrangement is rarely made public.[46] Thus, as commercial interests in

---

CABLES: THE HANDBOOK OF LAW AND POLICY, *supra* note 18, at 51.

40. Graham Evans and Monique Page, *The Planning and Surveying of Submarine Cable Routes* in SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY, *supra* note 18, at 93 (describing the importance of feasibility surveys and route planning to cost).

41. In navigation, this is known as a "great circle route," and it is why cable routes generally mirror international sea lanes.

42. Evans & Page, *supra* note 40, at 95; *Threats to Undersea Cable Communications, supra* note 10.

43. Wolff Heintschel von Heinegg, *Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 291, 306 (Katharina Ziolkowski, ed., 2013).

44. *See* Burnett et al., *supra* note 18, at 9 ("[o]f the billions of dollars spent to finance cable systems, currently less than five per cent is provided by governments or international agencies. The 95 per cent balance is provided by private consortiums (49 percent), carriers (32 percent) and non-governmental investors (14 percent)"). Nevertheless, government and international organizations can prove critical in connecting remote regions to this undersea network. For instance, the U.S., Japan, and Australia agreed to finance a cable to Palau at an estimated cost of $30 million. *Fact Sheet: The United States Partners with Australia and Japan to Expand Reliable and Secure Digital Connectivity in Palau*, U.S. DEP'T OF STATE (Oct. 29, 2020), https://2017-2021.state.gov/the-united-states-partners-with-australia-and-japan-to-expand-reliable-and-secure-digital-connectivity-in-palau/index.html; *Australia, Japan, U.S. to fund cable for Pacific island of Palau*, REUTERS (Oct. 28, 2020), https://www.reuters.com/article/palau-cable-australia-int/australia-japan-u-s-to-fund-cable-for-pacific-island-of-palau-idUSKBN27D0FK.

45. Elizabeth Anne O'Connor, *Underwater Fiber Optic Cables: A Customary International Law Approach to Solving the Gaps in the International Legal Framework for Their Protection*, 66 NAVAL L. REV. 29, 49 (2020).

46. Burnett et al., *supra* note 18, at 9; *see also* Green, *supra* note 39, at 58 (explaining indefeasible right of use and leases as methods to sell capacity on cable

a cable are so broad and opaque, it is nearly impossible to know what states' nationals are involved. During armed conflict, the targeting of such cables therefore implicates the laws of neutrality and the discrimination principle, as will be discussed in Part III.

Third, undersea telecommunications cables are fragile. In fact, approximately 200 unintentional cable breaks occur per year.[47] The glass fibers through which digital information travels are the width of a human hair. Bundled together, these fibers are sheathed in copper to conduct power, and a thin layer of polyethene-coated steel adds strength. Yet even then, the entire diameter is no more than 17-22 millimeters.[48] When laid in the deep sea, the garden hose-sized cables are unarmored and often lie proud – without being buried in a protective trench – on the ocean floor.[49] But for segments that transit the shallower continental shelf at depths less than 2,000 meters, a thicker steel-wire armor casing encloses the cable to furnish an extra layer of protection.[50]

Nevertheless, errant anchors[51] and commercial fishing gear[52] regularly sever armored cables. To minimize damage from environmental hazards and human activity, cable ships can also employ remotely operated vehicles (ROV) and plows to bury cables in a trench. But the ability to bury a cable depends on sea bottom type, and it is not possible where the ocean floor is especially rocky. Furthermore, some fishing activities, such as the use of stow nets, can still damage a well buried cable.[53] Thus, although detailed route

---

systems).

47. Burnett et al., *supra* note 18, at 7.

48. Lionel Carter et al., *The Relationship Between Submarine Cables and the Marine Environment*, *in* SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY, *supra* note 18, at 179.

49. *Id.*

50. *See* BARRY J. ELLIOTT, CABLE ENGINEERING FOR LOCAL AREA NETWORKS 198–199 (2000).

51. Anchors are the second most common cause of cable faults and commonly occur in two situations. First, when a ship anchors outside of an approved anchorage. This is a common problem, as cable landing sites typically exist close to major shipping lanes. Second, when a ship fails to properly secure its anchor, it can drag across the sea floor and sever cables. For instance, in 1986, a merchant vessel's improperly stowed anchor severed three of four trans-Atlantic cables. Robert Wargo & Tara Davenport, *Protecting Submarine Cables from Competing Uses* in SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY, *supra* note 18, at 255, 257–58.

52. Fishing is responsible for more than sixty percent of cable faults caused by forces external to the system. *Id.* at 256–57 (discussing several commercial fishing practices that trawl or drag the ocean floor and can result in cable breaks at depths of more than 1,000 meters).

53. *Id.* at 257 (describing numerous faults along the coast of China caused by stow nets).

planning and technology can mitigate risk, undersea cables are delicate, and breaks are an inherent part of the business. This fragility renders undersea cables an inviting military target.

Finally, although repairs are routine, they remain costly and are subject to the tyranny of distance. On average, it costs between one and three million US dollars to repair a cable break, and the rate for chartering a cable repair ship runs between $45,000 and $70,000 per day.[54] If weather and sea states permit, a cable may be repaired in fewer than 24 hours[55]; however, it can take longer than a week in some instances.[56] As every cable serves as a potential backup for disabled routes, swift maintenance and rapid repairs are critical to the entire network.

To defray these costs and ensure expeditious repairs, cable owners typically form clubs that share the cost of maintaining cable ships on 24/7 standby for a given geographic region.[57] Yet the vast majority of such ships are staged in key commercial sea lanes and near the wealthiest developed nations. For instance, a 2020 study showed that 66 percent of cable repair ships currently underway were located in the vicinity of China, Western Europe, or North America.[58] Conversely, only four of the forty-seven ships underway during the study were operating off the coast of Africa.[59] One solitary ship was located in the South Pacific.[60] While it makes sound business sense to stage more cable repair ships in areas with the greatest density of cables, this commercial reality means that it will take longer and cost more to repair cables serving geographically isolated regions or low-income countries. The prospect of such delays means a coordinated attack on cables could yield longer lasting effects and increase incentives to target them.

---

54. Burnett et al., *supra* note 18, at 7.

55. Sarah Whiteford, *How is a Subsea Cable Repaired*, ONE STEP POWER (Apr. 25 2021), https://www.onesteppower.com/post/subsea-cable-repair (describing the process by which cable repair ships use remotely operated vehicles to locate a cable break, a grapnel to cut and hoist both ends of the cable to the surface, and dynamic positioning systems to maintain position while splicing new cable to the loose ends).

56. Vaughan O'Grady, *Undersea Cable Repairs Planned – But it Could Take Two Weeks*, DEVELOPING TELECOMS (Jan. 24, 2020), https://developingtelecoms.com/telecom-technology/optical-fixed-networks/9131-undersea-cable-repairs-planned-but-it-could-take-two-weeks.html.

57. Burnett et al., *supra* note 18, at 33.

58. Rebecca Spence, *Where in the World are Those Pesky Cable Ships*, 111 SUBMARINE TELECOMS F. 12, 13 (Mar. 16, 2020), https://subtelforum.com/where-in-the-world-are-those-pesky-cable-ships/.

59. *Id.*

60. *Id.*

C. UNDERSEA CABLE INFRASTRUCTURE IN DEVELOPING AND LEAST DEVELOPED COUNTRIES

Despite the fragility of cables and the cost of repairs, wealthy nations benefit from multiple, redundant cable connections, creating a "built-in resilience for standard, operational single point cable failures."[61] Therefore, for much of the developed world, the loss of a single cable will not impact overarching connectivity, as providers have pre-arranged plans to reroute traffic through other cables.[62] Indeed, some observers have argued that the recent focus on cable vulnerability is overblown for this reason.[63] This may be partially true for the developed world.[64] But cable fragility presents a much more pressing concern for low-income countries.[65] This vulnerability will grow more challenging as the internet becomes an increasingly indispensable part of life in the developing world.

Three factors exacerbate cable vulnerability in the developing world: a lack of redundancy; less robust terrestrial infrastructure; and limited funding. First, fewer cables serve the developing world, rendering entire regions susceptible to discrete, well-planned attacks.[66] As NATO's Cooperative Cyber Defence Centre of Excellence noted in a 2019 paper, "protecting cables becomes even more important where resilience and redundancy are low and countries or islands are only connected through one or two cables."[67] Indeed, accidental breaks have engendered outsized consequences due to this

---

61. OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 10.

62. Heintschel von Heinegg, *supra* note 43, at 294 ("[the] loss of connectivity through a single submarine cable will . . . have but a minor impact on global communications because, as often service can be rerouted through other cables, and because broken cables can be repaired comparatively speedily.").

63. Louise Matsakis, *What Would Really Happen if Russia Attacked Undersea Internet Cables*, WIRED (May 1, 2010 7:00 AM), https://www.wired.com/story/russia-undersea-internet-cables/.

64. *But see* Angus Eckstein, *Securing Australia's Submarine Communications Infrastructure*, 32 ROYAL AUSTL. NAVY: SEA POWER SOUNDINGS 16 (2021), https://www.navy.gov.au/sites/default/files/documents/Soundings_Papers_32_2021.pdf (highlighting the strategic vulnerability of Australian subsea cable infrastructure that is concentrated primarily in two cable landing stations).

65. Due to their geographic setting, some developed countries, like Australia, are also likely to suffer disproportionate effects from coordinated cable attacks. *Id.*

66. Heinstchel von Heinegg, *supra* note 43, at 294 ("[m]any countries do not have the funds necessary to support multiple cable landing stations or routes . . . . [t]herefore, a large percentage of overall bandwidth has been concentrated in a few major cable systems and cables come ashore in only a few places. Hence, interference with a single cable or with one of its landing points can have far reaching effects . . . ").

67. NATO COOP. CYBER DEF. CTR. EXCELLENCE, *supra* note 13, at 2.

lack of redundancy.[68] In 2018, an accidental break along the African Coast to Europe cable left Mauritania without internet access for two days and reduced bandwidth for nine West Africa states.[69] Moreover, developing states typically lack the resources and infrastructure to support multiple landing stations and routes.[70] Thus, connectivity hinges upon relatively few cables located in narrow choke points.

Second, some of the world's poorest regions lack a robust network of terrestrial cables that connect coastal cities with the interior and integrate the broader region.[71] Unlike the developed world, when a break occurs, data may not be easily rerouted across terrestrial cables to landing stations in neighboring countries and adjacent regions.[72] For instance, when the West Africa Cable System (WACS) and South Atlantic 3/West Africa Submarine Cable (SAT-3) suffered a series of consecutive breaks in 2020, providers were able to reroute data through cables on the continent's east coast. Users experienced higher latency and slow speeds, but service was not interrupted; however, if both cables had been severed

68. Heinstchel von Heinegg, *supra* note 43, at 294 (noting that India, Pakistan, Egypt, Vietnam, Maldives, Qatar, Taiwan, and several [West African states] experienced 80% reduction in overall bandwidth at various points between 2005 and 2010).

69. Chris Baynes, *Entire Country Taken Offline for Two Days After Undersea Internet Cable Cut*, THE INDEPENDENT, Apr. 11, 2018, https://www.independent.co.uk/news/world/africa/mauritiana-internet-cut-underwater-cable-offline-days-west-africa-a8298551.html.

70. Heintschel von Heinegg, *supra* note 43, at 294. Some developed countries have tried to diversify the geography of cable landing stations to achieve greater resiliency. For instance, after Hurricane Sandy affected the concentration of cable landing stations near New York City, at least one cable consortium directed a cable route to Virginia instead. Similarly, Australia is actively trying to diversify its cable landing stations for security purposes.

71. Scholars have repeatedly documented the colonial legacy of "outward" facing infrastructure that reflects metropole connections over regional integration. JAMES M. CYPHER & JAMES L. DIETZ, THE PROCESS OF ECONOMIC DEVELOPMENT 90 (2014). In sub-Saharan Africa, such realities have impeded the growth of trans-continental trade corridors and associated infrastructure that would better integrate the continent. The growth of fiber optic cables has mirrored this orientation, and the "last mile" often remains incomplete. Emmanuel Paul, *Subsea Internet Cables and the Race to Connect Africa to the Internet*, TECHPOINT (Aug. 18, 2020), https://techpoint.africa/2020/08/18/subsea-internet-cables-africa/ (discussing the importance of telecommunications infrastructure going "the last mile" in sub-Saharan Africa); Kraska, *supra* note 15 (describing mutual restoration agreements in which cable operators negotiate and plan for split-second rerouting of data in the event of a cable break).

72. *See generally* Brian Browdie, *South Africans Under Lockdown Have to Deal With Slow Internet After Another Undersea Cable Break*, QUARTZ AFRICA (Mar. 30, 2020), https://qz.com/africa/1828436/lockdown-south-africa-internet-slows-as-submarine-cable-snaps/.

simultaneously, the situation may not have been mitigated so easily.[73] As Hunga Tonga-Hunga Ha'apai's recent eruption demonstrated, archipelagic and island states exist in an even more precarious situation.[74] Such regions may maintain internet access if a single cable is severed; however, multiple simultaneous breaks could have devastating effects.[75] Thus, these regions will not be able to mitigate the effects of intentional attacks as well as wealthy states with terrestrial infrastructure that connects them to alternative CLS.

Third, smaller LDCs – especially for archipelagos and island nations - may not possess markets large enough to entice private investment in cable infrastructure. International organizations like the World Bank have sought to fill this gap. For instance, the World Bank approved a $29 million grant for the Tuvalu Telecommunications and ICT Development Projects in 2019.[76] Similarly, commercial banks account for five percent of undersea cable finance, most of which has focused on connecting African

---

73. *See generally* Baynes, *supra* note 69.

74. In January 2022, reports indicated that one of the two cables connecting mainland Norway with the arctic island of Svalbard inexplicably failed. Space Norway, which operates the cables, noted that a failure of the second cable would completely cut off the island. David Averre, *Undersea Cable Connecting Norway and Arctic Satellite Station is Mysteriously Damaged*, DAILY MAIL (Jan. 11, 2022, 09:06 AM), https://www.dailymail.co.uk/news/article-10390555/Undersea-cable-connecting-Norway-Arctic-satellite-station-mysteriously-damaged.html. Similarly, a violent volcanic eruption in Tonga completely severed undersea cables connecting the remote Pacific island to the outside world in January 2022. Industry experts feared that repairs could take weeks. Praveen Menon & Tom Westbrook, *Undersea Cable Fault Could Cut Off Tonga from Rest of World for Weeks*, REUTERS (Jan. 18, 2022,04:42 AM), https://www.reuters.com/markets/funds/undersea-cable-fault-could-cut-off-tonga-rest-world-weeks-2022-01-18/.

75. Lixian Loong Hantover, *The Cloud and the Deep Sea: How Cloud Storage Raises the Stakes for Undersea Cable Security and Liability*, 19 OCEAN & COASTAL L. J. 1, 7 (2014) (observing that when a 2006 earthquake severed nine cables on the Taiwanese coast, communications were "seriously impaired," six hundred gigabytes of capacity was lost, and trading of the Korean won ceased); *see also* Martinage, *supra* note 24, at 119 (noting that eleven ships spent forty-nine days to restore the nine cable connection).

76. Press Release, The World Bank, Affordable, Faster Connectivity for Tuvalu (Jan. 15, 2019), https://www.worldbank.org/en/news/press-release/2019/01/15/affordable-faster-connectivity-for-tuvalu; *see also* Press Release, The World Bank, World Bank Supports Submarine Communications Cable and Helps Unlock High-Speed Opportunities (Oct. 4, 2011) https://www.worldbank.org/en/news/feature/2011/10/04/world-bank-supports-submarine-communications-cable-and-helps-unlock-high-speed-opportunities (discussing a $31 million grant to connect Sierra Leone to the global undersea cable network); *see also* Press Release, The World Bank, *Underwater Cable to Bring High-Speed Internet to Samoa* (June 19, 2015) https://www.worldbank.org/en/news/press-release/2015/06/19/underwater-cable-to-bring-high-speed-internet-to-samoa (leading to the approval of $31 million grant for the Sierra Leone component of WARCIP).

states.[77] In the event of armed conflict and attacks on undersea cable infrastructure serving an LDC, limited financing may compound the problems of time, distance, and cost and make immediate repairs unlikely.

Thus, undersea cable attacks pose far greater risks for citizens of developing states – and neutral states whose data travels across their cable infrastructure – than citizens of developed countries who enjoy more redundant infrastructure and local data storage. As the next section will show, these risks are real. Great powers, regional opponents, and criminal actors all possess the capability to cut cables, and low-income states have few means to protect such vital infrastructure.

II. THREATS TO UNDERSEA CABLES DURING ARMED CONFLICT

Targeting submarine cables during armed conflict is not a new concept. Indeed, belligerents have always sought to disrupt enemy communications. But modern fiber optic cables play a far more critical role in society than analog cables of the 19th and 20th centuries. Moreover, while all states depend on undersea FOC, developing states have much less redundant capability. Attacks can therefore have far broader and more lasting effects for non-combatants and neutrals in their territory. This section will briefly review the history of undersea cable attacks before exploring the current threat posed by Russia, which has developed unique capabilities in this sphere. Finally, the section will highlight examples of low-tech attacks and accidents that proved equally disruptive to undersea communications infrastructure.

As soon as the first transatlantic telegraph cables were installed, adversaries recognized the importance of undersea cables for military communications and allied coordination. In 1894, the U.S. Naval War College observed that cables constituted a critical vulnerability for enemies.[78] Although cables could be repaired, planners envisioned a wartime posture in which U.S. war ships could deny access to repair ships.[79] When the U.S. declared war on Spain, the Navy and Army

77. Brake, *supra* note 17, at 4.

78. *Spanish-American War: Telegraphy and Cable Cutting*, NAVAL HIST. AND HERITAGE COMMAND, https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html (last visited Feb. 6, 2023).

79. *Plan of Operations Against Spain Prepared by Lieutenant William W. Kimball (1896, 6/1/1897)*, NAVAL HIST. AND HERITAGE COMMAND, https://www.history.navy.mil/content/history/nhhc/research/publications/documentary-histories/united-

Signal Corps carried out this strategy.

U.S. tactics in the Spanish-American War highlight the unique cable characteristics discussed above. First, due to the fragility of cables, the attacks required neither advanced technology nor specialized tools. In fact, the U.S. Navy had no intelligence about cable locations. One officer simply appreciated the cost of laying cables and deduced that they would follow the most direct path between two landing stations. Small ships outfitted with improvised grappling hooks then dragged the sea bottom in these areas and quickly severed four of five cables servicing Puerto Rico.[80] Even where cables were buried in trenches, enterprising sailors jury-rigged unique multi-pronged tools to reach the cables.[81] Similarly, while cable attacks off Cuba's southern coast required great bravery – Marines and Sailors in small boats found and cut cables in the surf while warships and coastal defenses traded gunfire overhead – standard saws sufficed for their success.[82]

Second, the U.S. attacks implicated neutral parties. Although the cables connected Spain and its territories, British companies actually owned and operated them.[83] Recognizing the strategic benefit of cable

---

states-navy-s/pre-war-planning/plan-of-operations-a.html ("[c]able communication with the island should be promptly cut off . . . any auxiliary or light cruiser fitted with a cutter of the regular jaw pattern or with a gun-cotton cutter would answer well. Although the cables could be quickly repaired, any repairing could be readily prevented by the cruising squadron."); *see also* Jonathan Reed Winkler, *Silencing the Enemy: Cable-Cutting in the Spanish-American War*, WAR ON THE ROCKS (Nov. 6, 2011), https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/ ("[U.S. attacks on Spanish cables] reflected careful and innovative thinking by naval officers about the strategic significance of a technology central to the global economy of the day."); Caspar F. Goodrich, *The St. Louis' Cable-Cutting*, 26 U.S. NAVAL INST. PROCEEDINGS 157, 157–66 (1901), available at https://www.google.com/books/edition/Naval_Institute_Proceedings/05ojAQAAIAAJ?hl=en&gbpv=1&dq=caspar+goodrich+st.+louis+cable&pg=PA157&printsec=frontcover (providing a first-hand account of the USS Saint Louis' efforts to cut undersea cables landing at both Cuba and Puerto Rico); Cameron Winslow, *Cable-Cutting at Cienfuegos*, 57 THE NAT'L GEOGRAPHIC MAG. 708, 708–17 (1901) https://www.google.com/books/edition/The_National_Geographic_Magazine/-z4PAAAAIAAJ?hl=en&gbpv=1&dq=george+squier+coal+cables&pg=PA1&printsec=frontcover (describing the author's experience leading a small boat operations to locate and sever cables on the southern coast of Cuba).

80. Goodrich, *supra* note 79 at 158–59.

81. *Id.* at 160 (describing so-called "centipedes" as jury-rigged pieces of steel pipe designed to grapple cables amidst bottom obstructions).

82. *Id.* at 163 ("We were practically a stationary target, for the St. Louis was fast to the cable . . . we were some forty odd minutes under fire – and exposed to large shells sent from guns beyond our range, whose accuracy of aim became painfully threatening.").

83. *See* Eastern Extension, Australasia and China Telegraph Co. (Great Britain) v. United States, 6 R.I.A.A. 112, 113–15 (1923).

attacks, the United Kingdom did not lodge a diplomatic complaint and declared that the cables were lawful wartime targets.[84] Nevertheless, the episode still demonstrates that attacks on submarine communications cables inevitably involve non-combatants and neutrals. Furthermore, the U.S. attacks definitively proved the military benefits of such attacks. After the war, one officer commented that "[t]he story of the Spanish-American War is largely a story of 'coal and cables'" and believed that the conflict "demonstrated the dominating influence of submarine cable communications in the conduct of naval war."[85] The prediction proved prescient.

As telegraph use expanded in the early 20th century, militaries increasingly employed on undersea cables for command and control.[86] Submarine cables became an increasingly enticing target, and little could be done to defend such critical infrastructure. Even Britain, which relied on the world's largest undersea cable network to manage its colonies, still recognized the strategic value of attacking an enemy's cables.[87] Fifteen years after the U.S. severed U.K.-owned cables, Britain embraced the same strategy, ordering General Post Office cable ships to locate and cut German cables at the start of World War I.[88] For its part, Germany employed a U-boat to sever the undersea cables connecting New York City with Nova Scotia and Panama,[89] and a German cruiser destroyed Indian Ocean cables that

---

84. *Id.*

85. George O. Squier, *The Influence of Submarine Cables upon Military and Naval Supremacy*, 12 NAT'L GEOGRAPHIC MAG. 1, 2 (1901), https://www.google.com/books/edition/The_National_Geographic_Magazine/-z4PAAAAIAAJ?hl=en&gbpv=0 ("[T]he submarine telegraph is a powerful instrument of war, more powerful, indeed, than battleships and cruisers, since by its wonderful and instantaneous communications of thought, it brings distant countries together in sympathy, which is the only true and permanent tie.").

86. Between 1898 and 1918, the U.S. Army Signal Corps grew from sixty to 200,000 personnel. Chief Signal Officer Brigadier General Adolphus Greely attributed this growth to "the insistent demands of the age for instant communication," Susan Thompson, *Signal Corps Birthday*, U.S. ARMY (Jun. 29, 2021), https://www.army.mil/article/247979/signal_corps_birthday.

87. Gordon Corera, *How Britain Pioneered Cable-Cutting in World War One*, BBC NEWS (Dec. 15, 2017), https://www.bbc.com/news/world-europe-42367551 ("At the outbreak of World War One, Britain had the most advanced undersea telegraph cable system . . . wrapp[ing] around the world, due to the reach of the British Empire."). Of note, Britain also used its global telegraph system to surveil German transmissions and collect invaluable intelligence, *id.*

88. *See* JONATHAN REED WINKLER, *The Information Network and the Outbreak of War*, *in* NEXUS: STRATEGIC COMMUNICATIONS AND AMERICAN SECURITY IN WORLD WAR I 5 (2018) (describing how nations including Britain and United States used cables and radio in war against Germany).

89. John A. Hutcheson Jr., *U-Boat Operations, U.S. Coastal Waters (May–October 1918)*, *in* GERMANY AT WAR: 400 YEARS OF MILITARY HISTORY 1322, 1323 (David T.

linked Britain to Australia.[90]

Since the advent of FOCs in the 1980s, states have accelerated efforts to develop technologies for targeting cables in the deep ocean.[91] In particular, Russia has dedicated significant resources to such efforts.[92] According to Katarzyna Zyzk, the head of the Institute for Defense Studies at Norway's Center for Security Policy, Moscow envisions "sowing chaos in the financial system of an adversary" during a conflict, and undersea cable attacks "would certainly fit into [that] objective."[93] Moscow has constructed state of the art deep-sea research vessels and converted ballistic missile submarines to serve as motherships for smaller mini-submarines.[94]

The Russian Navy's Directorate of Deep Sea Research (GUGI)[95]

Zabecki ed., 2014).

90. Angus Eckstein, *Securing Australia's Submarine Communications Infrastructure*, 32 ROYAL AUSTL. NAVY: SEA POWER SOUNDINGS 3, 8 (2021).

91. The installation of undersea fiber optic cables increased the data that could be transmitted via terrestrial means and exceeded the capability of satellites. These developments also coincided with the "dot com boom" and commercial success of the internet.

92. *See* Sebastien Roblin, *Russian Spy Submarines Are Tampering with Undersea Cables that Make the Internet Work: Should We Be Worried?*, NAT'L INT. (Aug. 19, 2018), https://nationalinterest.org/blog/buzz/russian-spy-submarines-are-tampering-undersea-cables-make-internet-work-should-we-be ("Russian military activity around the submarine cables surely reveals that they are perceived as a valuable avenue for asymmetric attack . . . and a capacity to launch a more targeted attack against selected cables could cause significant disruptions."); Sanger & Schmitt, *supra* note 23 ("What worries Pentagon planners most is that the Russians appear to be looking for vulnerabilities at much greater depths, where the cables are hard to monitor and breaks are hard to find and repair.").

93. James Glanz & Thomas Nilsen, *A Deep-Diving Sub, a Deadly Fire and Russia's Secret Undersea Agenda.*, N.Y. TIMES (Apr. 21, 2020), https://www.nytimes.com/2020/04/20/world/europe/russian-submarine-fire-losharik.html. If such purposes served as the exclusive motivation for a cable attack, it would not meet the threshold for military necessity and would violate the IHL targeting principles discussed in section three; however, any belligerent can make a legitimate argument that a strategic leadership and military forces rely on communications cables to coordinate operations and sustain their war-making capacity. Therefore, such attacks--regardless of ancillary effects--could reasonably be justified under standard IHL interpretations.

94. Michael Birnbaum, *Russian Submarines are Prowling around Vital Undersea Cables: It's Making NATO Nervous*, (Dec. 22, 2017), https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?utm_term=.a57f9e4f495f.

95. GUGI is the acronym for the Directorate's Russian name: *Glavnoye Upravleniye Glubokovodnykh Issledovaniy*. According to some reports, it is also referred to as Military Unit 40056. H. I. Sutton, *Five Ways the Russian Navy Could Target Undersea Internet Cables*, (Apr. 7, 2021), https://www.navalnews.com/naval-news/2021/04/5-ways-the-russian-navy-could-target-undersea-internet-cables/ (noting that GUGI is "widely suspected of being in charge of more than research")

reportedly operates special operations submarines for this purpose.[96] For instance, Losharik, a nuclear-powered mini-submarine, launches from one of the converted mother submarines and may be able to operate independently for several days.[97] Designed for depths somewhere between 8,200 and 20,000 feet, Losharik may be able to manipulate objects on the ocean floor.[98] This could theoretically enable Russia to manipulate or attack cables covertly. In 2019, Losharik suffered a catastrophic fire, and 14 lives were lost.[99] Moscow claimed that the vessel was conducting sea-bed studies in the Barents Sea.[100] However, the unusual number of senior naval officers who perished aboard the vessel suggests a more sensitive purpose. Indeed, senior U.S. military officials have expressed concern about Russia's increasingly persistent submarine presence near cables in the north Atlantic.[101]

GUGI also operates two Yantar-class oceanographic research vessels, but analysts believe that their true purpose is more nefarious.[102] According to reports, the Yantar carries two three-

---

[hereinafter Sutton 2021].

96. H. I. Sutton, *How Russian Spy Submarines Can Interfere with Undersea Internet Cables*, (Aug. 19, 2020), https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/ (detailing Russia's use of mini-submarine like Paltus and Losharik to conduct operations on the ocean floor) [hereinafter Sutton 2020].

97. Sutton 2021, *supra* note 95.

98. Glanz & Nilsen, *supra* 93; Birnbaum, *supra* note 94 (quoting Rear Adm. Andrew Lennon, the commander of NATO submarine forces); Sutton 2021, *supra* note 95; Alice Fuller, *Russian Spy Ship that Can 'Cut Undersea Cables' Spotted in English Channel*, (Sept. 13, 2021), https://nypost.com/2021/09/13/russian-spy-ship-that-can-cut-undersea-cables-spotted-in-english-channel/ ("[the mini-subs] are carried beneath an enormous "mothership" . . . built to lurk at the bottom of the ocean . . . [and] then use robotic arms to tamper with or even cut key cables . . . ").

99. Glanz & Nilsen, *supra* note 93.

100. Ivan Nechepurenko, *Damaged Russian Submersible Has Nuclear Power Unit, but It's Intact, Kremlin Says*, (Jul. 4, 2019), https://www.nytimes.com/2019/07/04/world/europe/russia-nuclear-sub-fire.html.

101. Birnbaum, *supra* note 94 ("'We are now seeing Russian underwater activity in the vicinity of undersea cables that I don't believe we have ever seen,' said U.S. Navy Rear Adm. Andrew Lennon, the commander of NATO's submarine forces . . . 'Russia is clearly taking an interest in NATO and NATO nations' undersea infrastructure.").

102. Sutton 2021, *supra* note 95; Roblin, *supra* note 92; James Kraska, *Submarine Cables in the Law of Naval Warfare*, (Jul. 10. 2020), https://www.lawfareblog.com/submarine-cables-law-naval-warfare#:~:text=Article%2054%20of%20the%201913,blockade%20of%20the%20enemy%20state ("Russia's ship Yantar . . . is monitored by Western naval forces since it is outfitted with cable-cutting gear and deep-sea submersibles."). *But see* Sanger & Schmitt, *supra* note 23 (quoting Alexei Burilichev, Head of Russian Defense Ministry's Deepwater Research Department, as saying "Yantar is equipped with a unique onboard scientific research complex which

person mini-submarines that can reach depths of six thousand meters. The ship also deploys with advanced autonomous underwater vehicles (AUV) and remotely operated vehicles (ROV).[103] U.S. Navy officials believe this suite of capabilities enables Yantar to identify and potentially cut cables in the deep ocean.[104] In 2016 and 2017, Yantar followed undersea cables near Guantanamo Bay, Turkey, and the southeastern United States.[105] Experts believe the vessel may have been searching for sensitive U.S. military cables.[106] Similarly, in 2021, the vessel loitered between two commercial cables in the Irish Sea, sparking concern among the U.K., Ireland, and NATO.[107]

Some observers insist that "fear of a massive cable attack is probably over-hyped," noting that Russia's limited GUGI assets could never sever the myriad redundant cables that connect the United States to its allies.[108] Indeed, even if an adversary severed every cable servicing the U.S. east coast, internet traffic would automatically be routed across the Pacific Ocean. Moreover, Jonathan Hiembo, a senior analyst with Telegeography, notes that such an attack "would hurt the Russians perhaps even more . . . [because] they're far more dependent on international networks" and most U.S. content is stored locally.[109]

But such arguments often assume that malicious actors lack the requisite knowledge to conduct such attacks. For instance, Nicole Starosielski, an expert on undersea cable networks at New York University, believes "[i]f somebody knew how these systems worked and . . . staged an attack in the right way, then they could disrupt the

---

enables it to collect data on the ocean environment, both in motion and on hold. There are no similar complexes anywhere."), http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=1.

103. Sutton 2021, *supra* note 95.

104. Roblin, *supra* note 92; Sanger & Schmitt, *supra* note 23 ("Navy officials said the Yantar and the submersible vehicles it can drop off its decks have the capability to cut cables miles down in the sea.").

105. Roblin, *supra* note 92.

106. *Id.*

107. John Mooney, *Russian Spy Ship Monitored Off Coast of Donegal* (Aug. 18, 2021) https://www.thetimes.co.uk/article/russian-spy-ship-monitored-off-coast-of-donegal-thvg8pg8k (observing that the ship traveled "in a zig zag fashion, suggesting it was searching for something beneath the waves using [sonar]") https://www.thetimes.co.uk/article/russian-spy-ship-monitored-off-coast-of-donegal-thvg8pg8k;; Adrian Zorzut, *Vladimir Putin's Spy Ship Armed with Steal Subs Lurking Above UK Internet Cables Sparking Fears Lines Could be Cut*, (Aug. 20, 2021) https://www.thesun.co.uk/news/15919153/putins-spy-ship-lurks-above-uk-internet-cables/ (citing automated identification tracking data publicly available on MarineTraffic.com).

108. Roblin, *supra* note 92; *see also* Matsakis, supra note 63.

109. Matsakis, *supra* note 63.

entire system . . . ."[110] Furthermore, skeptics often downplay the importance of cables and the potential for second-order harms as well.[111] For its part, NATO takes the threat seriously. While serving as Commander of U.S. Naval Forces in Europe, Admiral James Foggo emphatically stated that the cable protection constitutes a core mission for the U.S. Sixth Fleet.[112] Russia's GUGI clearly possesses the sufficient knowledge and capability to conduct such an attack, and states like China may soon develop similar systems.[113]

Ultimately, whatever one's assessment of advanced technologies and the ability to sever redundant cables in the deep sea, the Spanish-American War shows successful attack does not require sophisticated technologies. Crude, low-tech solutions can be equally effective in the littoral or when attribution is not a concern. Such risks are especially acute in remote regions and the developing world. Indeed, even those who find the threat to U.S. interests hyperbolic recognize the acute risk for regions lacking redundant undersea cable infrastructure.[114] Indeed, several incidents have highlighted the vulnerability of undersea cable infrastructure in the developing world:

> In 2007, Vietnamese fishermen seeking to salvage copper wire stole 27 miles of active submarine cable – along with critical optical amplifiers – from two active systems.[115] Their actions degraded Vietnam's internet access for 79 days, and the country only maintained baseline connectivity due to a

110. *Id.*

111. *Id.* ("[P]people in Europe wouldn't see your silly cat video you posted [to] Facebook.").

112. Sutton 2020, *supra* note 96.

113. Regional powers fear that China may be developing similar capabilities. For instance, a scholar at Taiwan's Institute for National Defense and Security has warned that "[t]he likelihood of the PRC damaging or corrupting submarine cables and related infrastructure that connect Taiwan to the outside world should not be underestimated nor overlooked by the international community." *Taiwan Fears China Could Cut Undersea Cables*, ASIA SENTINEL (Feb. 1, 2019), https://www.asiasentinel.com/p/taiwan-fears-china-cut-undersea-cables.

114. Matsakis, *supra* note 63 ("That's not to say that the world's undersea cables aren't at risk, or that they don't need protection – especially in areas of the world with less internet infrastructure, like Africa and some parts of Southeast Asia. When a fault happens there, the consequences can be more severe, including genuine internet disruption.").

115. Hantover, *supra* note 75, at 10; Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 CATHOLIC UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY 57, 80–81 (Dec. 2015); Heintschel von Heinegg, *supra* note 43, at 294.

second subsea cable.[116]

In 2007, a cable in Bangladesh was sabotaged. The nation lost all internet access and international communications for one week. Bangladesh Telegraph and Telephone Board lost $1.05 million.[117]

In 2008, Cable and Wireless Jamaica lost $1.5 million due to theft of active fiber optic cables.[118] A similar theft occurred in South Africa during the same year.[119]

In 2008, multiple subsea cables were mysteriously severed near Egypt and Dubai during a three-day period. Fourteen countries experienced a significant bandwidth reduction, and the Maldives lost all connectivity with the rest of the world.[120]

In 2010, terrorists attacked the beach manhole housing a submarine cable that connected the Philippines and Japan.[121]

In 2013, three men in SCUBA gear attempted to sever cables off the coast of Alexandria.[122] Their actions reportedly caused a sixty percent drop in internet speeds. For one Egyptian MP, the attack "demonstrate[d]... the low degree of sophistication required for determined individuals to cause serious disruptions to internet communications."[123]

Although some of these incidents occurred on land, a coherent threat picture emerges when viewed holistically.

---

116. Matsakis, *supra* note 63. Nor are such incidents limited to the maritime environment. In 2011, an Armenian accidentally severed an underground cable while savaging for copper. As Armenia relied on one cable from Georgia for all internet access, this small act precipitated a five-hour outage. *Id.*

117. Davenport, *supra* note 115, at 81.

118. *Id.*

119. Heintschel von Heinegg, *supra* note 43, at 294.

120. Heintschel von Hantover, *supra* note 75, at 10.

121. Hantover, *supra* note 75, at 10; Davenport, *supra* note 115, at 81.

122. Elizabeth Anne O'Connor, *Underwater Fiber Optic Cables: A Customary International Law Approach to Solving the Gaps in the International Legal Framework for Their Protection*, 66 NAVAL L. REV. 29, 34 (2020); Amanda Williams, *Three Egyptian Divers 'Tried to Hack Through Internet Ocean-Floor Cables in Attack that Could Have Taken Entire Continent Offline'*, DAILY MAIL (Mar. 28, 2013), https://www.dailymail.co.uk/sciencetech/article-2300595/Pictured-Egyptian-divers-tried-hack-cables-attack-crashed-internet-worldwide.html.

123. O'Connor, *supra* note 122.

These incidents demonstrate the vulnerability of cables, prove that advanced technology is not a prerequisite for success, and highlight the devastating impact of attacks for the developing world. Indeed, Douglas Burnett, a noted expert on undersea cables, emphasizes that "it is naïve to assume that submarine-cable landing stations, cables, the cable ships . . . will escape asymmetric terrorist acts."[124] But terrorism is far from the only concern. States and other non-state actors that lack Russia's sophisticated deep-sea technologies could conduct cable attacks just like the divers in Egypt or fishermen in Vietnam. Moreover, an actor need not have full control of the maritime environment to stop cable ships from conducting repairs. For instance, the Houthis' use of sea mines and cruise missiles on Yemen's Red Sea coast provides a stark example of how non-state groups can project risk into key shipping lanes.[125] In such an environment, cable repairs could be delayed indefinitely, while neutrals and non-combatants suffer the prolonged consequences of denied internet access. Poor, isolated states will remain vulnerable to such attacks unless IHL targeting principles fully account for the importance of submarine cable communications.

III. THE LEGAL FRAMEWORK GOVERNING UNDERSEA CABLES DURING PEACETIME AND ARMED CONFLICT

Cyrus Field, founder of the first transatlantic telegraph company, believed that undersea telegraph cables "should be regarded as a sacred thing, protected by unanimous consent against all attack or damage."[126] Sir Travers Twist, an English lawyer who once served as Advocate-General of the Admiralty, considered submarine telegraph cables the world's "great arterial lines . . . indispensable for the circulation of the political life blood so necessary . . . to the vitality of our modern international State system."[127] Field and Twist were not alone in appreciating the critical importance of undersea cables.

As this new technology emerged, several states sought legal

124. Hantover, *supra* note 75, at 10.

125. Phil Stewart, *U.S. Navy Ship Targeted in Failed Missile Attack from Yemen*, REUTERS (Oct. 9, 2016), https://www.reuters.com/article/us-yemen-security-usa-ship/u-s-navy-ship-targeted-in-failed-missile-attack-from-yemen-u-s-idUSKCN12A082 (discussing a Houthi cruise missile attack on a U.S. Navy guided missile destroyer); *Yemen: Houthis Claim Attack on UAE Military Vessel*, AL JAZEERA (Oct. 2, 2016), https://www.aljazeera.com/news/2016/10/2/yemen-houthis-claim-attack-on-uae-military-vessel (providing details on Houthi missile attack that destroyed a UAE warship in the Bab al-Mandeb strait).

126. Burnett, Davenport & Beckman, *supra* note 18, at 65.

127. *Id.* at 63.

protection for undersea cables during war. For instance, in an 1864 treaty, France, Brazil, Haiti, Italy, and Portugal vowed not to attack a shared cable during an armed conflict.[128] But the signatories only committed to protect cable landing stations and portions of the cable within their territory.[129] The text did not address attacks on the high seas, and contemporary observers doubted whether signatories would have observed the treaty obligations during war.[130] Similarly, most states rejected an 1869 U.S. proposal to treat open ocean cable attacks as acts of piracy.[131] Thus, despite broad appreciation for the importance of undersea telegraph cables, states declined to grant them unique war time protection. States have crafted several treaties to address the status of undersea cables in peacetime; however, only two provisions from that line of treaties holds relevance for the status of cables during conflict.

A. INTERNATIONAL LAW AND THE PEACETIME USE OF UNDERSEA CABLES

Soon after the first transatlantic telegraph cables were laid, the international community sought to clarify their legal status. In 1884, the International Convention for the Protection of Submarine Cables (1884 Convention) met in Paris and established provisions to protect the installation, operation, and maintenance of cables. Article II requires signatories to criminalize intentional harm to cables in their territory and establishes a culpable harm negligence standard for accidental breaks.[132] The Convention also mandates that cable operators provide restitution for fishermen who ditch equipment to avoid a break[133] and indemnifies owners for damages caused by the installation or repair of other cables.[134] Such provisions provided much needed clarity for the safe and efficient operation of the nascent industry.

But the Convention provided no wartime protection for cables. In fact, Article 15 explicitly states that "the stipulations of the present

128. M. Louis Renault, LA PROTECTION DES TELEGRAPHES SOUS-MARINS ET LA CONFERENCE DE PARIS 5 (1882) ("*Les États contractants s'engagent á ne pas couper ou détruire en cas de guerre les câbles immergés par M. Pier-Alberto Balestrini, et* à *reconnaitre la neutralité de la ligne télégraphique.*").

129. *Id.*

130. *Id.* at 6.

131. *Id.* at 7.

132. Convention for the Protection of Submarine Telegraph Cables, art. 2, Mar. 14, 1884, 24 Stat. 989, T.S. 380 (entered into force May 1, 1888) [hereinafter 1884 Convention].

133. 1884 Convention art. 7.

134. 1884 Convention art. 4.

Convention do not in any way restrict the freedom of action of belligerents."[135] That said, Article 10 does empower states to board *commercial* vessels suspected of breaking a cable. Therefore, under Article 10, a state could board a suspect vessel, conduct questioning, and collect evidence. This is a useful authority should a hostile power, like Russia, employ merchant vessels to disrupt cables covertly;[136] however, the right does not extend to warships. Moreover, the ultimate exercise of jurisdiction remains with the suspect vessel's flag state.[137] As a hostile power is not going to investigate and prosecute its own covert acts, evidence collected through an Article 10 boarding would only prove useful in the court of public opinion. Nevertheless, Article 10 may provide a legal foundation to build upon for the contemporary security environment and will be considered further below.

Forty years later, an arbitral tribunal reinforced Article 15 and couched it in terms of customary international law. In *Eastern Extension v. United States*, the tribunal found that Admiral Dewey's destruction of British-owned cables in Manilla Bay was lawful and that the United States did not owe damages to the owner. According to the tribunal, Article 15 embodies a "general principle of international law" that "a belligerent's principal object in maritime warfare is to deprive the enemy of communication over the high seas."[138] As the Spanish military relied on the Eastern Extension cable for communications, the cable became "impressed with a hostile character" and constituted a lawful target under customary international law and the 1884 Convention.[139] Despite this deferential

135. As one contemporary observed, the treaty "made no provision defining the rights and immunities of cable property in time of war," Squier, *supra* note 85, at 8. Of note, the British delegation made an unequivocal reservation that "a belligerent, a signatory to the convention, shall be free to act in regard to submarine cables as if the convention did not exist." *Id.* at 8. The Belgian government expressed a similar reservation. *Id.*

136. *See* Sutton (2020), *supra* note 96. For instance, the U.S. Navy relied on Article 10 to justify its boarding of the Soviet-flagged fishing trawler that had damaged multiple transatlantic cables. Heintschel von Heinegg, *supra* note 43, at 298–99.

137. *See* 1884 Convention art. 8; *id.* art. 10; *see also* Heintschel von Heinegg, *supra* note 43, at n.52.

138. Great Britain v. U.S., 6 R.I.A.A. at 113–15 ("[T]he severance of the cable between Manila and Hong Kong, as well as between Manila and Capiz, was a proper military measure on the part of the United States, taken with the important object of interrupting communication wither with other parts of the Spanish possessions in the Philippine Islands or with the Spanish Government and the outside world.").

139. *Id.* (reasoning that a belligerent "is even entitled to prevent [a cable's use] by neutrals, who use it to afford assistance to the enemy either by carrying contraband, by communicating with blockaded coasts, or by transporting hostile dispatches, troops, enemy agents, and so on").

approach to military necessity, the court did note one constraint on such attacks. When targeting enemy communications on the high seas, belligerents must exhibit "a due respect for innocent neutral trade." [140] The paper will return to this caveat in Part Four, but it highlights one possible route to constrain the targeting of undersea cables in the 21st century.

After World War II, the international community forged two agreements that clarified maritime rights and the peacetime status of cables: the United Nations Convention on the High Seas[141] (1958 Convention) and the 1982 U.N. Convention on the Law of the Sea (UNCLOS).[142] Both treaties explicitly incorporate aspects of the 1884 Convention. For instance, Article 27 of the 1958 Convention and Article 113 of UNCLOS require signatories to criminalize intentional or negligent damage to cables.[143] Neither treaty, however, addresses the status of cables in wartime or provides additional legal protection. Indeed, unlike the 1884 Convention, the 1958 Convention does not authorize warships and other government ships to board vessels suspected of breaking cables.

Nevertheless, some observers consider the 1884 Convention to be customary international law and argue that provisions not incorporated into the 1958 Convention or UNCLOS remain in force.[144] Article 30 of the 1958 Convention explicitly states that prior agreements shall continue in force and were incorporated into the treaty. Indeed, President Eisenhower initially objected that the 1954 Convention only incorporated three provisions from the 1884 Convention; however, when submitting the treaty for Senate

---

140. *Id.* at 115.

141. United Nations Convention on the High Seas, *opened for signature* Apr. 29, 1958, 450 U.N.T.S. 11 (entered into force Sept. 30, 1962) [hereinafter 1958 Convention].

142. United Nations Convention on the Law of the Sea, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994) [hereinafter UNCLOS].

143. 1958 Convention, *supra* note 141, at art. 27; *see also* O'Connor, *supra* note 122, at 36 (noting that the "inclusion of Article IV and Article V illuminate the concerns of the time that the majority of damage would be caused by other cable laying companies.").

144. Of note, some have questioned whether the 1884 Convention actually constitutes customary international law, as only 40 states – with Japan as the one non-Western state – were parties. *See e.g., Burnett, Davenport &* Beckman, *supra* note 18. Nevertheless, few treaties in the colonial era had more than a few dozen signatories. Furthermore, the convention remains in force. As one scholar notes, "it still constitutes the international legal basis for domestic legislation for the protection of submarine cables," Heintschel von Heinegg, *supra* note 43, at 297; *see also* Kraska, *supra* note 102 ("[I]t is also possible to suggest that Article 10 persists even now by virtue of Article 30 of the 1958 convention, which states that prior agreements already in force shall continue.").

ratification, the administration noted that "existing conventions or other international agreements already in force would not be affected."[145] Thus, although Article 10 of the 1884 Convention differs from the UNCLOS regime of flag state jurisdiction on the high seas, it may well remain in force. Therefore, states may still have right to board, verify nationality, and collect statements from non-military vessels suspected of harming cables.

The 1884 Convention, the 1958 Convention, and UNCLOS represent a remarkable achievement of international cooperation. Their focus on the installation, maintenance, and liability for undersea cables highlights the importance of such infrastructure for the modern world. But their silence on conflict-related protections is deafening. Indeed, Elizabeth O'Connor, an officer in the Navy Judge Advocate General's Corps, notes that although "UNCLOS is . . . [a] foundational document for . . . governing underwater [FOC], neither it, nor its predecessor documents in 1958 or 1884, could ever have anticipated the importance underwater [FOC] would have to the global economy."[146] For this reason, undersea cables receive no special protection during armed conflict, and IHL governs as the *lex specialis*.

Granting belligerents wide discretion for targeting dual-use infrastructure, IHL makes no accommodation for the critical reliance non-belligerents, neutrals, and civilians place on undersea cables. The next section will explore IHL's approach to dual-use infrastructure, demonstrate its inadequacy for the unique importance of undersea cables, and consider the efficacy of proposed solutions. The final section will then outline proposals to address these gaps and better protect the most vulnerable states.

B. INTERNATIONAL HUMANITARIAN LAW AND THE TARGETING OF UNDERSEA CABLES

Under IHL, the right of states "to choose [the] methods or means of warfare is not unlimited."[147] As the scope and scale of modern

145. *See* O'Connor, *supra* note 45, at 36 ("Thus, in order for the United States to sign and ratify the 1958 treaties, it was agreed that no provisions in the 1958 treaties would impact the 1884 Cable Convention.").

146. *Id.* at 37 (observing that during the time of UNCLOS negotiations and ratification, satellites carried most global communications).

147. *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* art. 38, (Jun. 12, 1994), 309 Int'l Rev. of Red Cross 583–94, https://ihl-databases.icrc.org/assets/treaties/560-IHL-89-EN.pdf [hereinafter San Remo Manual]; *see also* Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, art. 22,

warfare expanded in the 19th century, states sought to mitigate the horrors of war and minimize civilian suffering. Four IHL principles gradually emerged to guide targeting during armed conflict: military necessity; distinction; proportionality; and humanity.[148] These principles limited the impact of armed conflict for civilians, non-combatants, and neutral states. But they do little to constrain attacks on dual-use infrastructure that provides critical services for such groups. This part will explore these IHL principles, consider their application for the targeting of undersea cables, and highlight the shortcomings of this framework for low-income states whose populations rely on such infrastructure.

The principles of distinction, necessity, proportionality, and humanity emerged from longstanding custom and steadily evolved into formal, codified treaties. For instance, in 1863 the Union Army adopted General Order 100 – known as the Lieber Code – and articulated the principles of distinction, military necessity, and proportionality.[149] Mandating the "distinction between the private individual . . . and the hostile country itself," Article 22 required the Union Army to spare "the unarmed citizen . . . in person, property, and honor."[150] According to Article 14, military necessity renders any target not "indispensable for securing the ends of the war" unlawful.[151] The Lieber Code also incorporates the idea of proportionality, prohibiting "wanton devastation" and actions that make "the return to peace unnecessarily difficult."[152] Similarly, the 1868 St. Petersburg Declaration set forth the necessity principle, declaring "[t]hat the only legitimate object" of an attack "is to weaken the military forces of the enemy."[153] Providing one of the earliest statements of the humanity principle, the 1868 Declaration also affirms that military attacks causing unnecessary suffering and

---

adopted on Oct. 18, 1907 ("The right[s] of belligerents to adopt means of injuring the enemy is not unlimited.") [hereinafter Hague IV].

148. Of note, some states now observe a fifth principle – precaution – which requires states to avoid harm to civilians and civilian property and will be discussed briefly below. *See generally* GEOFFREY S. CORN *et al.*, THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 49–61 (2nd eds., 2019).

149. General Orders No. 1000, The Lieber Code Instructions for Government of Armies of the United States in the Field, art. 15 (Apr. 24, 1863) (recognizing that "[m]en who take up arms . . . do not cease . . . to be moral beings, responsible to one another and to God.") [hereinafter Lieber Code].

150. *Id.* at art. 22.

151. *Id.* at art. 14.

152. *Id.* at art. 16.

153. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, St. Petersburg, Nov. 11–Dec. 29, 1868 [hereinafter 1868 ST. PETERSBURG DECLARATION].

superfluous injury are unlawful.[154]

During the 20th century, formal treaties and state practice clarified the application of these four principles. The 1907 Hague Convention (Hague IV) prohibited the use of arms or "material calculated to cause unnecessary suffering,"[155] forbid unnecessary destruction of enemy property,[156] and required belligerents to take "all necessary steps" to protect civilian infrastructure, like hospitals, schools, and museums.[157] Fifty years later, Additional Protocol I (AP I) to the Geneva Conventions provided the most comprehensive statement of these four principles. Ratified by 174 states, AP I reinforced the principles of humanity, distinction, proportionality, and military necessity.[158] Military lawyers, law manuals, and war crimes tribunals frequently rely on the following provisions to assess targeting decisions, and our analysis merits a closer look at AP I's language:

> **Military Necessity.** Article 52 establishes a two-part definition to determine what constitutes a lawful military objective: 1) objects "which by their nature, location, purpose, or use make an effective contribution to military action"; and 2) objects "whose total or partial destruction . . . offers a definite military advantage."[159]
>
> **Humanity & Precaution.** Article 57(1) requires belligerents to take "constant care . . . to spare the civilian populations . . . and civilian objects." Furthermore, prior to an attack, combatants must "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects."[160]
>
> **Distinction.** Article 48 provides that parties "shall at all times distinguish between the civilian population and combatants

154. *Id.*

155. Hague IV, *supra* note 147, at art. 23I.

156. *Id.*at art. 23(g).

157. *Id.* at art. 27.

158. Of note, the United States signed the Protocol in 1977, but the Senate has not ratified it. Nevertheless, numerous administrations have indicated that they consider many AP I provisions as customary international law, and its precepts for targeting inform much of U.S. Defense Department Law of War Manual.

159. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 52, June 8, 1977, 1125 U.N.T.S. 17512 [hereinafter AP I].

160. *Id.* I art. 57(1)–(2)(a)(i).

> and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Similarly, Article 51(4) prohibits "indiscriminate attacks," which are defined as "those which are not directed at a specific military objective . . . those which employ a method or means of combat which cannot be directed at a specific military objective . . . or those which employ a method or means of combat the effects of which cannot be limited as required" [161]
>
> **Proportionality.** Article 51(5)(b) prohibits attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[162]

At first glance, these IHL principles seemingly constrain the targeting of dual-use infrastructure on which civilians, non-combatants, and neutrals rely. Indeed, as discussed in Part I, the destruction of cables can wreck the economy of an entire region, disrupt critical government services for civilians, and imperil the livelihood of non-combatants and neutrals. This is especially true in less developed regions where limited cable infrastructure is concentrated in vulnerable chokepoints. Such indiscriminate effects seem to implicate the principles of humanity, proportionality, and distinction envisioned by these core IHL treaties.

But military necessity consistently creates caveats that swallow the other three principles. Early on, the Lieber Code recognized that some harm to non-combatants will prove "incidentally unavoidable," and protection for unarmed civilians and private citizens extends only "as much as the exigencies of war will admit."[163] Similarly, Hague IV prohibits destruction of enemy property "unless such destruction . . . be imperatively demanded by the necessities of war,"[164] and the Hague IV obligation to spare civilian infrastructure extends only "as far as possible" and does not cover dual-use infrastructure.[165] Thus,

---

161. *Id.* at art. 48; *id.* at art. 51(4).

162. *Id.* at art. 51(5)(b).

163. Lieber Code, *supra* note 149, art. 15; *id.* at art. 22. *See also id.* at art. 23 ("Private citizens . . . and the inoffensive individual is as little disturbed in his private relations as the commander of the hostile troops can afford to grant *in the overruling demands of a vigorous war.*") (emphasis added).

164. Hague IV, *supra* note 147, art. 23(g).

165. *Id.* at art. 27 (limiting the prohibition to targets that are "not being used at the time for military purposes.").

although a civilian hospital may rely on undersea cables to access critical information, the cable can be targeted if some military units also communicate via the cable.

Nor does AP I resolve this inherent tension between military necessity and the humanity principle. To be sure, AP I called on signatories to "do everything feasible to verify that the objectives to be attacked are . . . [not] civilian objects."[166] But feasibility constitutes an amorphous standard, and such language does nothing to address objects that serve a military and civilian purpose. Indeed, under Article 52's two-part definition, any cable that makes "an effective contribution" to an enemy's communications and the destruction of which would provide a "definite military advantage" constitutes a lawful military target, irrespective of its civilian functions.

Furthermore, AP I's proportionality requirements do not easily apply to such "dual-use" objects. Under AP I, proportionality analysis must consider "reasonably . . . foreseen" second-order injuries to civilians when attacking a dual-use object.[167] But AP I does not define injury. Notably, the Protocol's definition of "incidental harm" does not include adverse effects from attacks that impaired a dual-use object's civilian function.[168] Some observers have called for proportionality assessments to account for such second-order effects and weigh the impairment of an object's civilian function; however, state practice, military manuals, and tribunals have yet to apply such a broad interpretation.[169]

The International Criminal Tribunal for the former Yugoslavia (ICTY) confronted the challenge of applying such mercurial standards to dual-use infrastructure.[170] Considering claims that NATO

166. AP I, *supra* note 159, art. 57(2)(a)(i)); *see also* U.S. DEPT. OF DEF., LAW OF WAR MANUAL 5.2.3. (2016).

167. *See* Emanuela-Chiara Gillard, *Proportionality in the Conduct of Hostilities: The Incidental Harm Side of the Assessment* 35 (Chatham House Int'l L. Programme ed., 2018).

168. *Id.*

169. *Id. See also* LAURENT GISEL, THE PRINCIPLE OF PROPORTIONALITY IN THE RULES GOVERNING THE CONDUCT OF HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 38–40 (Laurent Gisel ed., 2016); *The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare*, 93 INT'L L. STUD. 322, 335–36 (2017).

170. FINAL REPORT TO THE PROSECUTOR BY THE COMMITTEE ESTABLISHED TO REVIEW THE NATO BOMBING CAMPAIGN AGAINST THE FEDERAL REPUBLIC OF YUGOSLAVIA ¶2 [hereinafter ICTY REPORT] (considering claims that "NATO forces deliberately attacked civilian infrastructure targets . . . and deliberately or recklessly caused excessive civilian casualties in disregard of the rule of proportionality . . . "); *see also* Prosecutor v. Kupreškić et al., Case No. IT-95-16-T, Judgement, ¶ 524 ('nt'l Crim. Trib. for the Former Yugoslavia Jan. 14, 2000) (discussing proportionality and civilian precaution principle). *See generally* GILLARD, *supra* note 167.

unlawfully bombed civilian telecommunications infrastructure, an ICTY Investigative Committee relied on AP I language and found that IHL permitted the alliance's actions. In its report, the Investigative Committee employed AP I's two-part definition that lawful military targets must "make an effective contribution to military action" and "whose total or partial destruction . . . offers a definite military advantage."[171] But the Committee found it difficult to classify dual-use objects with "some civilian uses and some actual or potential military use . . . [such as] communications systems."[172] The ICTY report noted that military commanders must take all "practicable precautions . . . to minimize[e] incidental civilian casualties or civilian property damage," use "available technical means to properly identify targets," and refrain from attacks where disproportionate effects are expected.[173] Yet the committee also recognized that the "application of the principle of proportionality is more easily stated than applied in practice."[174] Citing a 1956 ICRC commentary that deemed "installations of broadcasting and television stations; telephone and telegraph of fundamental military importance" as lawful military objectives, the report ultimately concluded that U.S. attacks on media and telecommunications infrastructure did not violate IHL principles.[175]

In accordance with AP I, such interpretations afford states the flexibility to justify attacks on dual-use infrastructure where the object makes "an effective contribution" to an enemy's war-making ability.[176] Given the structure of FOC and the nature of digital data flows, no technical means can discern the proportion of neutral, non-combatant, and military-related data that transits an undersea cable. As such, belligerents can easily justify attacks on undersea cables with a reasonable belief that they facilitate military communications. If the disruption of such cables renders a "definite military advantage," an attack is justified under standard IHL interpretations.[177] Hospitals relying on cloud data; financial transactions between neutral states; human rights observers sharing real-time footage; the business needs

171. *Id.* at 35–37 (noting that the AP I definition only provides an objective standard for "simple cases" and not more nuanced assessments of dual-use objects).

172. *Id.* at 37; *see also id.* at 48 ("Unfortunately, most application of the principle of proportionality are not quite so clear cut . . . one cannot easily assess the value of innocent human lives as opposed to capturing a particular military objective.").

173. *ICTY* REPORT, *supra* note 170, at 28–29.

174. *Id.* ¶ 19.

175. *Id.* ¶ 39(I)(7).

176. OFF. OF THE CHIEF OF NAVAL OPERATIONS, U.S. DEP'T OF THE NAVY, COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 5.3.1 (2017).

177. *Id.* ¶ 8.2.

of neutral citizens and non-combatants – all such concerns disappear in the face of military necessity.[178] Under this framework, military necessity becomes a most malleable concept, and the humanity, proportionality, and distinction principles can do little to constrain attacks against the subsea dual-use infrastructure on which civilians and neutrals rely.

C. SOFT LAW CONTRIBUTIONS TO IHL & THE TARGETING OF UNDERSEA CABLES

More recent contributions to IHL have come in the form of soft law. Non-binding documents composed by legal experts, such as the *Tallinn Manual 2.0*,[179] the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*,[180] and the *Oslo Manual on Select Topics on the Law of Armed Conflict*[181] have sought to state the law as currently applicable. But they have also provided some novel recommendations for applying IHL to the modern technological landscape. Customary international law, comprised of state practice and *opinio juris*, is binding on states, and these documents, as indications of emerging *opinio juris*, may represent the future of IHL. Unfortunately, when it comes to the targeting of undersea cables, the documents do not change the underlying IHL calculus: the *Tallinn Manual* misdiagnoses the problem, and the *San Remo Manual* maintains broad caveats for military necessity. The *Oslo Manual*, however, does seem to appreciate the limitations of IHL targeting principles when applied to submarine cables and perhaps indicates the need for a new interpretation.

The Tallinn Manual includes several progressive recommendations to guide targeting in the modern, digital world. For instance, the manual expands the definition of injury for assessing

178. *See e.g., Id.* ¶ 8.3, 8.6.2.2 (justifying a broad range of dual-use targets under the "war-sustaining effort" rationale). *But see* San Remo Manual, *supra* note 147, ¶ 40 (rejecting such a broad catch-all as a legitimate tool for distinguishing military and civilian objects). *See generally,* Yusuke Saito, *Reviewing Law of Armed Conflict at Sea and Warfare in New Domains and New Measures: Submarine Cables, Merchant Missile Ships, and Unmanned Marine Systems*, 44 TUL. MAR. L.J. 107, 114–16.

179. INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter Tallinn Manual 2.0].

180. San Remo Manual, *supra* note 147.

181. YORAM DINSTEIN & ARNE WILLY DAHL, OSLO MANUAL ON SELECT TOPICS OF THE LAW OF ARMED CONFLICT: RULES AND COMMENTARY (2020) [hereinafter Oslo Manual].

cyber attacks, arguing that physical injury alone is insufficient.[182] Rather, the Tallinn Manual builds on AP I 51(2)'s prohibition on attacks that "spread terror among the civilian population"[183] and argues for the inclusion of "severe mental suffering" as an analogous form of psychological injury.[184] Article 92 also includes "serious illness" within the scope of injury.[185] These are welcome suggestions. As modern life becomes inextricably entwined with digital infrastructure, a more expansive definition of injury is critical to protecting the life, property, and well-being of non-combatants.[186] Nevertheless, an even broader definition of injury – one that recognizes economic harm, data destruction, and lack of digital access – is necessary to guide the targeting of undersea cables and address the widespread harm such attacks may cause in the developing world.[187]

The International Group of Experts (IGE) behind the manual specifically considered the application of IHL and CIL to undersea cables as well.[188] Two provisions merit discussion. First, rule 150 states that the law of neutrality prohibits belligerents from attacking

---

182. Tallinn Manual 2.0, *supra* note 179, at 417; *see also* Gillard, *supra* note 167, at 31 n.89 (noting that the Tallinn Manual is "the only document that addresses the notion of 'injury'").

183. AP I, *supra* note 159, art. 51(2) (prohibiting "acts or threats of violence the primary purpose of which is to spread terror among the civilian population.").

184. Tallinn Manual 2.0, *supra* note 179, at 417.

185. *Id.*

186. *See* Gillard, *supra* note 167. *But see* Todd Emerson Hutchins, *Safeguarding Civilian Internet Access During Armed Conflict: Protecting Human'ty's Most Important Resource in War*, 22 COLUM. SCI. & TECH. L. REV. 127, 159 (2020) (arguing that attempts to measure civilian harms from cyber-attacks challenge application of the proportionality principle [and] that the humanity principle provides insufficient protection, as it "traditionally only appl[ies] to 'indispensable objects' which, if deprived, would result in physical starvation").

187. Of note, some members of International Group of Experts (IGE) who drafted the Tallinn Manual called for a broader definition of "armed attack." Rejecting the traditional notion that only serious death, injury, damage, or destruction met the definition of armed attack, this minority argued that cyber warfare required a broader conceptual approach that considered non-physical harms, such as economic damage. The IGE recognized the value of such an interpretation; however, the majority considered it to be *lex ferenda* and not *lex lata*. *See* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L. J. 13, 22 (2012).

188. Of note, rule 54 reiterates the 1884 Convention's authorization for states "to take measures to identify vessels suspected of breaking a cable and to establish the relevant facts" during boardings. Tallinn Manual 2.0, *supra* note 179, at 257. This suggests that, according to the Tallinn Manual drafters, some provisions of the 1884 Convention may have gained the status of CIL. Unfortunately, as discussed above, the ability to board and question such vessels on the high seas serves little deterrent value when only the flag-state holds jurisdiction to prosecute.

neutral submarine cables in enemy territory or on the high seas.[189] But James Kraska, an expert in international maritime law at the U.S. Naval War College, has argued that the law of neutrality – and its implications for targeting analysis – cannot be applied so neatly to submarine cables in the cyber era.[190] Kraska argues that neutrality focuses on physical space and physical objects. Fiber optic cables, however, are analogous to air, as digital information packets transit the web of cables just as radio waves "propagate at will" through the ether.[191] Furthermore, modern undersea cables are not bi-polar. Unlike telegraph cables, they do not only serve the two states at either landing station.[192] As discussed in Part Two, the nature of digital data means that information traveling from myriad states can transit any undersea cable. Thus, it may not be possible to apply rule 150 so clearly in practice.

Second, the Manual's drafters declare that "the infliction of damage to cables by a State is prohibited as a matter of customary international law."[193] According to the manual, such actions would "run contrary to the object and purpose of the law governing submarine cables."[194] The group of experts, however, caveats that such prohibitions come "without prejudice to the rules applicable during armed conflict."[195] Therefore, the prohibition would cover covert attacks or "hybrid" warfare that do not meet the threshold for armed conflict. However, it does not alter existing IHL targeting provisions and implicitly recognizes the lawfulness of such attacks during an armed conflict.[196]

The San Remo Manual also captures many of the AP I targeting requirements but specifically applies them to the targeting of undersea cables on the high seas as well. [197] Three areas stand out. First, in Article 37, the San Remo Manual states that "[b]elligerents

189. Tallinn Manual 2.0, *supra* note 179, at 555.

190. Kraska, *supra* note 15 (observing that the "operation and administration of submarine cables in the cyber era magnifies uncertainty in applying the neutrality law").

191. *Id.*

192. *Id.*

193. Tallinn Manual 2.0, *supra* note 179, at 256.

194. *Id.* ("[T]he law of the sea does not provide a legal basis for a State to cut another State's submarine fibre optic cable in order to reduce trans-continental Internet traffic in times of tension.").

195. *Id.*

196. *See* NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *supra* note 13, at 5 (2019) ("[W]ithin a hybrid warfare scenario, actions taken which may be attributed to a state would therefore fall under this rule.").

197. *See* San Remo Manual, *supra* note 147, ¶ 40 (incorporating the two-step definition of lawful military objectives set forth in AP I art. 52(2)).

shall take care to avoid damage to cables . . . laid on the sea-bed which do not exclusively serve the belligerents."[198] Such language, however, implicitly recognizes that "cables . . . exclusively serving one or more of the belligerents might be legitimate military objectives."[199] Although it remains unclear how to interpret "exclusively serving."

Second, the San Remo Manual echoes the AP I definition of military objective as that which provides "an effective contribution to military action."[200] However, the manual expands its scope and argues that there is no requirement for a direct connection with combat operations.[201] Some observers have criticized the San Remo Manual's formulation as too broad, and the ICRC interprets the phrase much more narrowly.[202] Nevertheless, other countries – such as the United States – employ this broad approach to justify an extensive array of targets.[203] Third, the San Remo Manual builds upon the 1884 Convention boarding authority and declares that cutting undersea cables on behalf of an enemy "may render enemy merchant vessels [as] military objectives."[204] Such authority is a welcome expansion and helps address gray zone operations. Though it provides little comfort to developing states with scarce naval resources, as they will not be able to consistently protect the undersea cables on which they rely.

Finally, the Oslo Manual – the most recent contribution to IHL soft law – aimed to provide a "methodical restatement" of IHL[205] and dedicated one of its sixteen sections entirely to submarine cables and undersea infrastructure.[206] Rule 69 addresses the targeting of submarine communications cables and closely resembles the San Remo convention's language.[207] At first glance, the Oslo Manual does not provide any new insight regarding the ambiguities of AP I and IHL targeting principles. Still, the commentary provides an insightful

198. *Id.* ¶ 37.

199. Saito, *supra* note 178, at 112.

200. San Remo Manual, *supra* note 147, ¶ 40.

201. *Id.*

202. Saito, *supra* note 178, at 115 (citing CLAUDE PILLOUD ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 636 (Yves Sandoz et al. eds., 1987)).

203. *Id.* at 114–16 (noting that the United States "war-sustaining effort" rationale to target a range of civilian facilities whose infrastructure indirectly support an enemy's military, such as bridges, power generation plants, storage areas, etc., was rejected by the ICRC).

204. San Remo Manual, *supra* note 147, ¶ 59–60.

205. Oslo Manual, *supra* note 181, at vi.

206. *Id.* at 61–64.

207. *Id.* at 63 ("Belligerent States must take care to avoid damage to such cables, unless they qualify as lawful targets.").

synopsis of the difficulties in applying such principles to undersea cables:

> It is, however, doubtful whether the 1907 Hague Regulations and the San Remo provisions also apply to submarine communications cables [as opposed to submarine pipelines and high voltage cables]. Other than telegraphic cables, modern submarine communications cables are the backbone of global data traffic. Although they may physically connect the territories of two States, it will only in rare circumstances be possible to determine that they are "exclusively serving one or more belligerents" or one or more Neutral States. Today's submarine communications cables are interconnected. Hence, data packages will travel over routes that are unpredictable. Accordingly, it is important to distinguish between submarine communications cables and other submarine cables.[208]

Although the Oslo Manual represents non-binding soft law, it reflects the consensus of a body of IHL experts who consulted with multiple governments and non-state actors. Thus, while the commentary may not reflect a unified sense of *opinio juris*, it raises doubts about the traditional IHL targeting interpretations and illuminates interpretative space in which military manuals and international tribunals could adopt a narrower approach.

The final section will briefly discuss legal and policy proposals to better protect undersea cables. After highlighting the limitations of these approaches, the paper will discuss the potential for jurists in the developing world to articulate IHL interpretations that cabin the military necessity principle, more effectively weigh second-order effects, and better protect the vulnerable, dual-use infrastructure on which their populations rely.

IV. A TWAIL PATH FORWARD & THE POTENTIAL FOR A NEW IHL INTERPRETATION

At this point, the paper has discussed the critical importance of undersea cables for modern society, examined their acute importance for the developing world, and outlined current threats against this critical infrastructure. The preceding section then explored the limitations of IHL targeting principles when applied to dual-use

208. *Id.*

targets like fiber optic cables. As discussed, belligerents can justify attacks on undersea cables so long as there is a reasonable belief that they "make an effective contribution" to enemy communications and that their destruction would yield a "definite military advantage." There is no indication that the world's leading military powers wish to reinterpret IHL and develop new norms for targeting dual-use infrastructure. Broadly defined military objectives ensure targeting flexibility and operational freedom during armed conflict, and wealthy states possess a redundant communications infrastructure that provides a degree of defensive resilience. But citizens in the developing world may not feel so confident.

The Oslo Manual recognized the limits of this approach, and the legal status quo may trouble many readers as well. Perhaps you are reading this paper on the same computer where you just emailed a colleague, completed a stock trade, or accessed sensitive medical records. Or perhaps you used your mobile phone to place a phone call overseas. Some – possibly all – of these actions traveled upon undersea cables. As the Oslo Manual commentary notes, fiber optic cables are qualitatively and quantitatively different from telegraph cables in the late 19th and early 20th centuries. An unfathomable amount of data transits today's cables, and nearly every part of modern life depends on the connectivity they bring. To apply hoary IHL principles to 21st-century digital infrastructure seems wildly anachronistic and potentially dangerous. This paper believes there is another way.

Regional human rights courts with a mandate to adjudicate IHL violations may prove the most realistic avenue to explore new targeting interpretations. More attuned to the peculiar concerns and strategic reality of their region, these bodies are well-positioned to interpret IHL targeting principles in ways that meet the unique needs of their member states and citizens. Such rulings may not represent a sweeping change to international law or suddenly deter undersea cable attacks. But they could spark an incremental shift in legal approach. If other courts or military manuals eventually adopt similar views, these interpretations could constitute a new *opinio juris*, guide state practice, and one day form customary international law.[209] After a brief examination of other proposals to address undersea cable attacks under international law, this section will explore the unique potential of regional courts using the African Commission as a case study.

---

209. Although the creation of CIL is often a slow process, *see* North Sea Continental Shelf (Fed. Rep. of Ger. v. Neth.), Judgment, 1968 I.C.J. (Apr. 26) for a discussion of how CIL can be established very quickly in some instances.

A. PROPOSALS TO MITIGATE THE THREAT TO UNDERSEA CABLES

Over the past decade, a growing body of literature has discussed the vulnerability of undersea cables and proposed myriad policy and legal solutions. Many authors have identified sensible policy solutions based on best practices: increase communications infrastructure redundancy; establish an interagency lead to coordinate domestic and multinational responses;[210] improve collaboration between the government and cable industry; or forge maritime partnerships to patrol cable routes.[211]

While such policy proposals may help, they fail to address the underlying vulnerability of submarine cables or address their status in armed conflict. For instance, Australia and New Zealand took the lead in establishing cable protection zones within their exclusive economic zones (EEZ).[212] Some have debated whether enforcement of such zones violates UNCLOS rights,[213] but these efforts certainly limit the likelihood of accidental breaks. Unfortunately, even the most well-funded navies have difficulty maintaining perfect situational awareness within their EEZ. A motivated criminal and non-state actor will easily avoid such patrols, and cable protection zones will not affect a belligerent state once hostilities commence. Additionally, cable integrity is an international problem and demands an international solution. For even if one country protects the cable and landing stations within its control, its access to global networks can still be severed on the other side of the ocean. Thus, while cable protection zones are a unique proposal to address peacetime concerns, they do little to address the norms of attacking such infrastructure during armed conflict.

But creative solutions to protect cables from attack do exist. Some observers have suggested that the international community should declare peacetime attacks as acts of piracy.[214] With a piracy

---

210. O'Connor, *supra* note 122, at 39.

211. Douglas R. Burnett, *Cable Vision*, U.S. NAVAL INST. PROCEEDINGS, Aug. 2011, at 70–71.

212. Heintschel von Heinegg, *supra* note 43, at 313 (describing the cable corridor/protection zones that Australian and New Zealand established on one mile of either side of cable routes in their territorial seas and EEZ).

213. *Id.* at 312–13 (finding that protection zones would have no basis in international law if enacted beyond a state's territorial seas).

214. O'Connor, *supra* note 122, at 39; Laurence Reza Wrathall, *The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward*, 12 SAN DIEGO INT'L L.J. 223, 256 (2010) (arguing that the piracy definition should be expanded and the "private ends limitation should be eliminated to deter signatory states and their inhabitants from looting and possibly inciting economic and environmental shock at the margins of antiquated definitions"); Tara Davenport,

designation, states anywhere could prosecute offenders outside their territorial sea under universal jurisdiction, irrespective of flag or nationality.[215] A conviction would likely carry a higher penalty than theft and might deter criminal actors like the Vietnamese fishermen discussed in section two. But an expanded piracy designation still holds little relevance for the broader array of intentional threats to cables. For instance, the existing definition of piracy in both UNCLOS and the 1958 convention only covers actions committed for "private ends."[216] Thus, it would not apply to commercial vessels or pleasure crafts which a state tasks to conduct covert attacks against cables. Most importantly, in the context of developing nations, it is unlikely that a poor littoral state has the means to effectively patrol its EEZ, identify malicious actors, and carry out a boarding and arrest. Thus, the proposal lacks the scope to serve as an effective deterrent in the developing world.

Others have looked at ways to hold states liable for damage to undersea cables. Three Australian law professors have argued that flag states should be liable for damages resulting from incidents that do not rise to the level of criminal conduct or armed attack.[217] Relying on the famous *Trail Smelter* arbitration, the authors analogize the harm from cable damage to transboundary air pollution.[218] They argue that a vessel's flag establishes attribution under UNCLOS article 92 and conclude that a flag state can be liable for unintentional cable damage unless they show that they "took all reasonable steps and exercised due diligence to prevent it."[219] Such approaches certainly

---

Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis, 24 CATH. U. J. L. & TECH. 57, 84 (2015) ("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."); BECKMAN, SUBMARINE CABLES—A CRITICALLY IMPORTANT BUT NEGLECTED AREA OF THE LAW OF THE SEA 15-16 (ISIL Conference, Jan. 2010).

215. *But see* Heintschel von Heinegg, *supra* note 43, at 298 (noting that UNCLOS limits jurisdiction to the flag state or nationality of perpetrator and therefore cannot be reconciled with the existing piracy definition in Article 101).

216. UNCLOS, *supra* note 142, art. 101 (defining 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 . . . directed . . . on the high seas, against another ship . . . or against persons or property on board such ship . . . outside the jurisdiction of any State").

217. Paige et al., *supra* note 16.

218. *Id.* (referencing *Trail Smelter* (U.S. v. Can.) 3 R.I.A.A. 1905 (Int'l Joint Comm'n 1938)) ("We argue, in line with *Trail Smelter*, that losses caused by damage to submarine cables render the flag state responsible for the vessel that caused the damage liable not only for the cost of repairing the cable, but all losses stemming from the cable damage.").

219. *Id.*

have merit. They might incentivize some flag states to better control, investigate, and prosecute negligent activity in accordance with UNCLOS and 1884 Convention responsibilities. But as mentioned previously, developing states will often lack the maritime and intelligence resources for effective maritime domain awareness. As such, these states will not be able to effectively identify, track, or collect data from the responsible vessels. Furthermore, this approach does not deter the actions of non-state actors and criminal activity outlined in section two, and it certainly does not address the threat to cables during armed conflict. Ultimately, to provide holistic legal protection for undersea cables, one must consider the application of IHL.

Some of the most interesting proposals to address undersea cable during armed conflict involve parts of IHL other than targeting principles. Todd Hutchins, an officer in the U.S. Navy JAG Corps, recognizes the limitations of applying IHL to digital, dual-use infrastructure. He believes that specialized humanitarian protection regimes could provide a legal basis for protecting neutral and non-combatant internet access.[220] Noting that IHL has created special protection regimes for injured people, humanitarian workers, medical professionals, and cultural artifacts, Hutchins argues that a similar regime would prove "a uniquely effective way to provide heightened protections" for physical internet infrastructure like cables under IHL.[221] This solution presents a certain elegance. But such aspirations ignore the reality of warfare. Unlike medical professionals, injured soldiers, or cultural artifacts, the destruction of undersea communications cables does provide a military advantage for attacking forces. For this reason, such restrictions would be unlikely to shape behavior during armed conflict.

Similarly, Douglass Burnett, Chief Counsel of the Department of Transportation's Maritime Administration and an expert on the law of submarine cables, has suggested that cable repair ships be provided wartime protections similar to hospital ships under IHL.[222] According to Burnett, this "modest step" would foster humanitarian objectives by ensuring communications and internet access are restored in a timely fashion.[223] But two problems exist with Burnett's proposal. First, few corporations will risk sending their ships into an active

220. Hutchins, *supra* note 186, at 168–69.

221. *Id.*

222. Naval War College Symposium, *Disruptive Technologies and International Law: A Conversation with Douglas Burnett*, YOUTUBE (Dec. 9, 2020), https://www.youtube.com/watch?v=s7GXXtKrRdY.

223. *Id.*

combat zone to carry out repairs. There will be even less urgency to do this for developing countries with smaller markets. Second, states would be unlikely to support such protections. Unlike hospital ships, belligerents can reasonably view cable repair ships as supporting a critical military function. Indeed, that is why states seek to target cables in the first place.

Whether practical or aspirational, these policy proposals and legal solutions would certainly help if implemented. But they fail to provide a holistic international solution or concern only one aspect of the threat. Ultimately, they do not address the greatest impediment to submarine cable safety: the broad interpretation of military necessity under IHL targeting principles. A new approach is needed for an enduring system that affords greater consideration to second-order effects of cable attacks. Indeed, as Hutchins has noted, "the failure to . . . proactively [build a new global consensus] may result in the practices of bad actors being tolerated by the global community . . . establishing norms under customary international law that would permits depriving civilians of internet access during conflict."[224] As internet blackouts have become common in many armed conflicts, it appears that this normalization may already be underway. Regional human rights courts may provide an avenue to craft new IHL interpretations, reflect the unique circumstances of developing states, and halt this dangerous trend.

B. A THIRD WORLD APPROACH TO INTERNATIONAL LAW (TWAIL) & INTERNATIONAL HUMANITARIAN LAW

Over the last twenty years, some legal scholars – often hailing from the world of international economic law – have characterized international law as a discipline constrained by a "limited geography of places and ideas . . . in both scholarship and practice."[225] Others have gone further and condemned the "recolonization" and "ideological domination of Northern academic institutions" in international legal discourse. [226] Collectively known as Third World Approaches to International Law (TWAIL), these scholars have attempted to shift the locus of legal discourse and acknowledge the

224. Hutchins, *supra* note 186, at 174.

225. James Thuo Gathii, *Twenty-Second Annual Grotius Lecture: The Promise of International Law: A Third World View*, (Aug. 29, 2020), 36 AM. U. INT'L L. REV. 377, 380 (2020).

226. B.S. Chimni, *Third World Approaches to International Law: A Manifesto*, 8 INT'L CMTY. L. REV., 3, 3–4 (2006) (expressing concern over the "regressive role of globalizing international law" and its effect on legal voices in Global South).

developing world "as an epistemic site of production and not merely a site or reception of legal knowledge."[227] Their analyses cast doubt on "international law's assumed neutrality and universality" and seek a "new set of tools . . . to address the material and ethical concerns of third world peoples."[228] By expanding beyond "the insularity of international law" and "embrac[ing] the practice and scholarship . . . about and from the Third World," the TWAIL perspective seeks to elevate previously marginalized voices and establish an international legal framework that better reflects global discourse.[229]

Although TWAIL has rarely been applied to IHL, the discipline constitutes the ideal candidate for a fresh, outside perspective. Indeed, from Grotius to the Lieber Code to the Hague and Geneva Conventions, IHL has been developed, interpreted, practiced, and imposed almost entirely by the developed world. Yet in the post-World War II environment, international armed conflicts and non-international armed conflicts have primarily occurred in the developing world.[230] When it comes to critical dual-use infrastructure like undersea cables, it is the developing world that stands on the front lines. The paper has already shown that 19th-century targeting principles do not capture the complexities of the modern digital world; however, from a TWAIL perspective, prevailing IHL interpretations may also prove incongruous with the social, economic, and political realities developing countries confront. "Third World" jurisprudence and scholarship can provide unique interpretations to reconcile IHL to the needs of the 21st – century developing states. To explore this possibility, the paper will consider the African Commission on Human and People's Rights and its jurisprudence on the targeting of dual-use infrastructure as a case study.

---

227. Gathii, *supra* note 225, at 379 ("Recognizing the Third World as a site of knowledge production and of the practice of international law disrupts the assumptions that international legal knowledge is exclusively produced in the West for consumption and governance of the Third World.").

228. Luis Eslava, *TWAIL Coordinates*, CRITICAL L. THINKING (Apr. 2, 2019), https://criticallegalthinking.com/2019/04/02/twail-coordinates/ (Identifying TWAIL scholarship as a "challenge [to] international law's complacent linearity and unidimensionality by showing the skewed power dynamics that criss-cross the international legal order").

229. Gathii, *supra* note 225, at 379.

230. *See* Mohamed Nagy & Max Roser, *Civil Wars*, OUR WORLD IN DATA, https://ourworldindata.org/civil-wars (last visited Feb. 19, 2023); *see* Thomas S. Szayna et al., *What are the Trends in Armed Conflicts, And What do They Mean for U.S. Defense Policy*, RAND CORP. (2017), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1904/RAND_RR1904.pdf.

C. CASE STUDY: THE AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS

For years, African leaders, scholars, and jurists have claimed that global security structures inadequately address the continent's needs. In 1994, George Ayitteh, a Ghanaian economist, lambasted foreign interventions and declared that "African problems" require "African solutions."[231] Such perspectives infused negotiations surrounding the Organization of African Unity's (OAU) adoption of the African Charter on Human and Peoples' Rights (African Charter) in 1981 and the founding of its successor organization, the African Union (AU), in 2002.[232] Some observers believe the same "disillusionment with the . . . global security architecture" guided the AU's efforts to create the African Court of Human Rights (African Court) in 2006 and efforts to establish a consolidated African Court of Justice and Human and Peoples' Rights under the 2012 Malabo Protocol.[233] Such efforts merit excitement; however, only 24 states have adopted the Malabo protocol and the African Court has not heard any cases that address IHL targeting principles.[234] At present, its jurisprudence contains limited relevance for this topic. But one element of the African human rights system does address these issues: the African Commission on Human and Peoples' Rights (African Commission).

In 1986, the OAU established the African Commission under Article 30 of the African Charter.[235] During the African Charter's negotiations, some member states, like Guinea, argued for a more robust body that would have criminal jurisdiction over serious human rights violations.[236] Ultimately, OAU members rejected such

---

231. George B.N. Ayittey, *The Somali Crisis: Time for an African Solution*, CATO INST. (Mar. 28, 1994), https://www.cato.org/policy-analysis/somali-crisis-time-african-solution.

232. Charles C. Jalloh, Kamari M. Clarke & Vincent O. Nmehielle, *Introduction: Origins and Issues of the African Court of Justice and Human and Peoples' Rights*, *in* THE AFRICAN COURT OF JUSTICE AND HUMAN AND PEOPLES' RIGHTS IN CONTEXT: DEVELOPMENT AND CHALLENGES 1, 5–11 (Chares C. Jalloh et al. eds., 2019).

233. *Id.* at 11.

234. HURST HANNUM ET AL., INTERNATIONAL HUMAN RIGHTS: PROBLEMS OF LAW, POLICY, AND PRACTICE 1000 (6th ed. 2018).

235. This should not be confused with the African Court on Human and Peoples' Rights which began to operate in 2006 and only decided one case on its merits between 2006 and 2013. Frans Viljoen, *The Relationship Between International Human Rights and Humanitarian Law in the African Human Rights System: An Institutional Approach*, *in* CONVERGENCE AND CONFLICTS: OF HUMAN RIGHTS AND INTERNATIONAL HUMANITARIAN LAW IN MILITARY OPERATIONS 303, 305 (Erika De Wet & Jan Klefner, eds. 2014).

236. Charles C. Jalloh, *The Place of the African Court of Justice and Human and Peoples' Rights in the Prosecution of Serious Crimes in Africa*, *in* THE AFRICAN COURT OF

proposals.[237] As a "quasi-judicial" body, the African Commission's findings are merely recommendations.[238] But under the Revised Rules of Procedure promulgated in 2008, the Commission does have the ability to monitor compliance with its decisions. Moreover, the Commission must inform the AU Executive Council of non-compliance, and it can refer cases to the African Court. Perhaps most importantly, the Charter endows the African Commission with a uniquely broad mandate that includes IHL. As such, it is empowered to investigate claims involving alleged IHL targeting violations. If the Commission were to develop a consistent approach to such thorny IHL issues, its findings could represent nascent *opinio juris* and suggest new IHL interpretations that are more responsive to the needs of Africa and developing states writ large.[239] For these reasons, the African Commission merits a closer look.

Comprised of eleven independent commissioners and seated in Banjul, The Gambia, the Commission is charged with "formulat[ing] . . . principles and rules aimed at solving legal problems relating to human and peoples' rights" and to "ensure the protection of human and peoples' rights under . . . [the] Charter."[240] A communications process enables the Commission to carry out this work. Article 56 of the African Charter sets forth a "communication procedure" through which individual(s), non-governmental organizations, and states can petition the Commission over alleged human rights violations, and article 45(4) empowers the Commission

---

HUMAN AND PEOPLES' RIGHTS IN CONTEXT: DEVELOPMENT AND CHALLENGES 57, 77 (Chares C. Jalloh et al. eds., 2019).

237. HANNUM ET AL., *supra* note 234, at 971 (quoting Christof Heyns, *The African Regional Human Rights System: The African Charter*, 108 PENN ST. L. REV. 679, 686 (2004)) (comparing the "idealistic explanation" that states desired a more "traditional way of solving disputes . . . through mediation and conciliation" with the more practical view that newly independent states were jealous of their sovereignty).

238. African Charter on Human and Peoples Rights, Art. 58, June 27, 1981, 2 U.N.T.S. 256 [hereinafter African Charter] ("The Assembly and Heads of State and Government may . . . request the Commission to undertake an in-depth study of [special cases which reveal the existence of serious or massive violations of human rights] and make a factual report, accompanied by its finding and recommendations.").

239. For a discussion on the role of *opinio juris* in the development of customary international law, *see* HANNUM ET AL., *supra* note 234, at 142–43.

240. *History*, AFR. COMM'N ON HUMAN AND PEOPLES' RTS., https://www.achpr.org/history (last visited Feb. 13, 2023) (discussing African Charter art. 45(1)(b) and art. 45(2)); *see also* Charles C. Jalloh, Kamari M. Clarke & Vincent O. Nmehielle, *supra* note 232, at 3 (describing the Commission as a "quasi-judicial oversight body tasked with interpreting the charter and hearing complaints of human rights violations brought by individuals against their home states").

to interpret Charter provisions at the request of a state party.[241] Once the Commission determines that a communication "reveal[s] the existence of a series of serious or massive violations of human and peoples' rights," it must bring the situation to the attention of member states.[242] The AU Assembly may then request that the Commission investigate the alleged incidents, provide a factual report, and make recommendations.

Although a growing body of scholarship about the African Commission exists, citations to its decisions remain rare in international law casebooks and litigation.[243] Indeed, TWAIL scholars find that the international law produced [in Africa] is "marginalized doctrinally and theoretically."[244] To be sure, the African Commission heard a mere 250 cases between 1986 and 2011, and only a handful of decisions address IHL. But that limited jurisprudence has established two key findings: 1) the African Charter's human rights are non-derogable during armed conflict, and 2) the African Commission can draw upon IHL treaties and related CIL in its cases. This expanded mandate and IHRL-IHL fusion hold the potential for novel IHL interpretations that better suit the needs of Africa, non-combatants, and neutrals. One specific case addressed armed attacks on dual-use infrastructure and highlights the Commission's unique potential.

In *Democratic Republic of Congo v. Burundi, Rwanda and Uganda (DRC Case),*[245] the African Commission addressed the intersection of IHL and International Human Rights Law (IHRL) for the first time. Considering the actions of the belligerents during an international civil war, the Commission concluded that it was not empowered to find violations of IHL. But the Commission still found that the belligerents' actions fell "not only within the province of [IHL], but also within the mandate of the commission."[246] The Commission arrived at this formulation after determining that the Charter's rights

241. *History*, AFR. COMM'N ON HUMAN AND PEOPLES' RTS., https://www.achpr.org/history (last visited Feb. 13, 2023).

242. African Charter, *supra* note 238, art. 58.

243. *See* Viljoen, *supra* note 235, at 303 ("[M]ost academic writing dealing with the convergence of IHRL and IHL and extra-territorial application of IHRL makes sparse reference to the African Charter and its interpretation.").

244. Gathii, *supra* note 225, at 383 (citing ANTHEA ROBERTS, IS INTERNATIONAL LAW INTERNATIONAL? 271 (2018)).

245. Democratic Republic of Congo v. Burundi, Rwanda, Uganda, Communication 227/99, African Commission on Human and Peoples' Rights [Afr. Comm'n H.P.R.], ¶ 51 (May 29,2003) [hereinafter DRC Case], https://www.achpr.org/sessions/descions?id=138.

246. *Id.* ¶ 64.

are non-derogable during international and non-international armed conflict.[247] Additionally, the Commission interpreted the African Charter as authorizing it to incorporate core IHL treaties into its findings. Article 61 states that:

> The Commission shall also take into consideration, as subsidiary measures to determine the principles of law, other general or *special international conventions*, laying down rules expressly recognised by Member States of the Organisation of African Unity, African practices consistent with international norms on Human and Peoples' Rights, *customs generally accepted as law*, *general principles of law* recognised by African States as well as legal precedents and doctrine.[248]

Although the Commission is specifically chartered to protect human rights, this article expands its mandate to include "special international conventions" and customary law accepted by member states. The Commission has interpreted Article 61 as applying to the four Geneva Conventions, Additional Protocols 1 and 2, and customary international law, thereby creating an opportunity to fuse IHRL and IHL jurisprudence.

In the DRC case, the Commission relied on this Article 61 interpretation to adjudicate an attack on dual-use infrastructure.[249] Rwandan and Ugandan forces had sieged a hydroelectric dam, precipitating a widespread electricity outage, disrupting power for civilians, schools, and hospitals, and causing the death of patients on life support systems.[250] The Commission found that the siege violated the DRC's right to "national and international peace and security"

---

247. Viljoen, *supra* note 235, at 308 (explaining that the African Commission's reasoning for prohibiting any derogation is based on the absence of a derogation clause in the African Charter); *see also* Article 19 v. The State of Eritrea, Communication 275/2003, African Commission of Human and Peoples' Rights [Afr. Comm'n H.P.R.], ¶ 87 (May 16–30, 2007), https://www.achpr.org/sessions/descions?id=182 (finding that the African Charter does not permit states to derogate from its provisions even in the context of armed conflict). Of note, the European Convention on Human Rights, the Inter-American Human Right Convention, the Inter-American Human Rights Commission, and the International Covenant on Civil and Political Rights all permit states to derogate from some rights under certain circumstances.

248. African Charter, *supra* note 238, art. 61 (emphasis added).

249. DRC Case, *supra* note 245, ¶ 70; *see* Viljoen, *supra* note 235, at 316 ("[The African Commission] used the specific formulations under humanitarian law to breathe life into the much more general and open-ended Charter provisions.").

250. DRC Case, *supra* note 245, ¶¶ 3, 88.

under Article 23 of the African Charter.[251] Due to the article's broad sweep and ambiguous language, the Commission relied on AP I's prohibition against attacking dams to give shape and meaning to this right.[252] Interestingly, the commission goes on to cite Hague II's prohibition on the destruction of "the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war."[253] But the Commission's analysis does not even analyze the principle of military necessity in passing. Furthermore, applying its core mandate of charter-based rights, the Commission also found that the siege violated the African Charter's right to physical and mental health and the right to education.[254]

This fusion of charter-based human rights and IHL is striking. The Commission seamlessly switches between the two fields of law, drawing on both lines of jurisprudence to condemn the dam attack and its second-order effects. In this case, the Commission's reading of AP I Article 56 may have proved dispositive on its own. But the fact that the Commission also assessed the attack's second-order effects – to include intangible harms like disrupting the right to health – shows the jurisprudential flexibility of the two-pronged approach. If the Commission were petitioned for a case involving an undersea cable attack, this approach would provide analytic flexibility to re-interpret traditional IHL approaches to proportionality analysis. Indeed, the fact that the Commission did not address military necessity could indicate a wariness towards such arguments when widespread second-order effects are at issue.

Moreover, the Commission's rights-based mandate could enable it to incorporate new rights. Most dramatically, the Commission could find that a right to internet access exists. Indeed, some have argued that the recent addition of "freedom of expression" and "access to information" to Article 19 of the Universal Declaration of Human Rights implicitly establishes internet access as a human right.[255] By seeking to balance such an affirmative right against the military necessity of an attack, the African Commission could carve out a proportionality analysis that better accounts for the unique importance of submarine cables for the developing world.[256]

---

251. *Id.* ¶ 73.

252. DRC Case, *supra* note 245, ¶ 83 ("[T]aking Article 56 . . . into account, and by virtue of Articles 60 and 61 of the African Charter, the [African] Commission concludes that in besieging the hydroelectric dam in Lower Congo province, the Respondent States have violated the [African] Charter.").

253. *Id.* ¶ 84.

254. *Id.* ¶ 88.

255. Paige et al., *supra* note 16.

256. Numerous scholars and advocates have called for international

In fact, in other areas of human rights law, the African Commission has shown a willingness to forge new rights from the Charter's fabric. In *The Social and Economic Rights Action Center and the Center for Economic and Social Rights v. Nigeria*, the Commission found that the government of Nigeria failed to protect the Ogoni people's right to housing or shelter.[257] Although the Charter does not identify such a right, the Commission reasoned that such a right exists through the combination of "the right to enjoy the best attainable state of mental and physical health . . . , the right to property, and the protection accorded to the family forbids the wanton destruction of shelter because when housing is destroyed, property, health, and family life are adversely affected."[258] According to the Commission, "the combined effect of Articles 14, 16, and 18(1) reads into the [African] Charter a right to shelter or housing which the Nigerian Government . . . violated."[259] Noting the "uniqueness of the African situation," the Commission observed that "collective rights, environmental rights, and economic and social rights are essential elements of human rights in Africa" and pledged to "apply any of the diverse rights contained in the African Charter."[260]

The African Commission need not wait long to address the importance of digital access during armed conflict. It has become increasingly common for governments to block internet access to entire regions during NIACs,[261] and the Commission can receive petitions from non-governmental organizations and individuals. For instance, in May 2021, the African Commission accepted a petitioner's request to establish a Commission of Inquiry into the conflict in Ethiopia's Tigray region.[262] During that conflict, Ethiopian Prime

---

organizations to recognize internet access as a human right. *See, e.g.*, Mertin Reglitz, *The Human Right to Free Internet Access*, 37 J. APPLIED PHIL. 314, 314 (May 2020) ("Internet access is itself a moral human right that requires that everyone has unmonitored and uncensored access to this global medium . . . "); Stephen Tully, *A Human Right to Access the Internet? Problems and Prospects,* 14 HUM. RTS. L. REV. 175 (2014) (reviewing proposals for a human right to internet access).

257. The Social and Economic Rights Action Center and the Center for Economic and Social Rights v. Nigeria, Communication 155/96, African Commission on Human and Peoples' Rights [African Comm'n H.P.R.] (Oct. 27, 2001), https://www.achpr.org/sessions/descions?id=134.

258. *Id.* ¶ 60.

259. *Id.*

260. *Id.* ¶ 68.

261. *E.g.*, CPJ Africa and Asia Program Staff, *Journalists Struggle to Work Amid Extended Internet Shutdowns in Myanmar, Ethiopia, Kashmir*, COMM. TO PROTECT JOURNALISTS (May 3, 2021, 7:09 AM), https://cpj.org/2021/05/journalists-shutdowns-myanmar-ethiopia-kashmir/.

262. ACHPR/Res. 482, *Resolution on the Fact-Finding Mission to the Tigray Region of the Federal Democratic Republic of Ethiopia* (May 12, 2021),

Minister Abiy Ahmed executed an internet blackout against the Tigray province for several months in late 2020 and early 2021.[263] Although petitioners did not specifically address the internet blackout, the Commission's resolution noted the "allegations of human rights violations against the civilian population, including attacks against civilian infrastructure [and the] destruction of property . . . which may constitute war crimes and crimes against humanity."[264] This could provide a window for the Commission to consider whether the intangible, second-order effects of a communications blackout violated the African Charter. Such a finding would be directly applicable to attacks on undersea communications infrastructure and could begin the incremental march to a new TWAIL approach. With its broad mandate and unique approach to Africa's challenges, the African Commission is well suited to this task.

CONCLUSION

In assessing proportionality, no two people will balance military necessity and the protection for non-combatants and neutrals the same way. These views are born of personal experience, culture, and tradition. Indeed, the ICTY Review Committee remarked that "[i]t is unlikely that a human rights lawyer and an experienced combat commander would assign the same relative values to military advantage and to injury to noncombatants."[265] This recognition is what motivates TWAIL scholarship. IHL has historically been dominated by a western perspective, and scholars and courts have paid little attention to IHRL and IHL jurisprudence in the developing world. Such jurisprudence could provide new insights for applying IHL principles to the digital infrastructure of the 21st century.

Since its conception, IHL has sought to protect civilians from the ravages of war. But the predominant interpretations of IHL targeting principles place great emphasis on military necessity and fail to appreciate the changing circumstances of our modern digital world. Digital infrastructure like undersea communications cables is integral to safe, productive modern societies. But traditional IHL approaches have insufficiently considered second-order effects of attacks on such critical dual-use infrastructure. Such reasoning could justify attacks on submarine cables, which would prove especially ruinous for large swaths of the developing world. Regional human rights bodies, like

---

https://inquiry.achpr.org/resolution/. [hereinafter Tigray Resolution].

263. CPJ Africa and Asia Program Staff, *supra* note 261.

264. Tigray Resolution, *supra* note 262.

265. ICTY Report, *supra* note 170, ¶ 50.

the African Commission, can interpret existing IHL, infuse it with new perspectives fit for the modern, digital world, and provide a voice for the most vulnerable. NGOs should petition the Commission to address instances where combatants have attacked telecommunications cables or other dual-use communications infrastructure.

Such efforts will not prove a panacea. A century of state practice, coupled with strong tactical and strategic incentives, weighs against a legal framework that limits dual-use infrastructure as targets. In armed conflict, states will exploit any advantage available, and submarine communications cables will remain an alluring target for years to come. Yet while easy solutions may not exist, regional courts and local actors are best positioned to channel the concerns of their people, articulate an interpretation that reflects their unique strategic reality, and catalyze incremental changes to customary international law.