TARGETING SUBMARINE CABLES: NEW APPROACHES TO THE LAW OF ARMED CONFLICT IN MODERN WARFARE

LIEUTENANT COMMANDER DENNIS E. HARBIN III*

It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy. . . . [W]e have allowed this vital infrastructure of undersea cables to grow increasingly vulnerable. This should worry us all.[1]

I. Introduction

On 1 July 2019, fourteen Russian sailors tragically died when their submarine caught fire.[2] The submarine is the *Losharik*, an unarmed, nuclear-powered vessel designed to operate at depths greater than 10,000 feet.[3] According to U.S. officials,[4] the *Losharik* is not just an undersea research vessel, but also a submarine designed specifically to disrupt the "global infrastructure system that transmits 99 percent of the international data sent over the internet."[5] Its mission is to target submarine cables as a means to wage cyber warfare—at sea.

---

* Judge Advocate, United States Navy. Presently assigned to the Joint Staff. J.D., 2014, The Pennsylvania State University, Dickinson School of Law, Carlisle, Pennsylvania; B.A., 2008, Virginia Military Institute, Lexington, Virginia. A previous version of this article was submitted in partial fulfillment of the Master of Laws requirements of The Judge Advocate General's School, U.S. Army. This article was awarded the 2021 Richard R. Baxter Military Prize in recognition that it significantly enhances the understanding and implementation of the law of war. The author thanks the Lieber Society on the Law of Armed Conflict and the American Society of International Law for consideration and selection. The views expressed herein are solely those of the author and do not reflect the views or opinions of the Department of the Navy, the Department of Defense, or any other institution.

[1] James Stavridis, *Foreword* to RISHI SUNAK, UNDERSEA CABLES: INDISPENSABLE, INSECURE 9 (2017).

[2] Alexandra Ma & Ryan Pickrell, *The Russian Submarine that Caught Fire and Killed 14 May Have Been Designed to Cut Undersea Cables*, BUS. INSIDER (July 3, 2019, 8:33 AM), https://www.businessinsider.com/russia-submarine-losharik-undersea-cables-media-speculation-2019-7.

[3] *Id.*

[4] *Id.*

[5] Garrett Hinck, *Evaluating the Russian Threat to Undersea Cables*, LAWFARE (Mar. 5, 2018, 7:00 AM), https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.

In recent decades, academics and practitioners have spilled much ink discussing the character of warfare in the cyber age. Due to the unique aspects of the cyber battlespace, it continues to challenge national security law practitioners in the application of traditional law of armed conflict (LOAC) [6] principles, such as distinction and proportionality. The scholarship has focused primarily on the applicability of LOAC to either (a) operations that use cyber weapons to achieve cyber effects[7] or (b) operations that use cyber weapons to achieve tangible, kinetic effects. Missing from the discussion is how LOAC applies to a third form of cyber warfare:[8] military operations that use conventional weapons to achieve cyber effects.

One example of such a military operation is the 2019 Israeli Defense Force's bombing of a building containing Hamas hackers.

> The assault seems to be the first true example of a physical attack being used as a real-time response to digital aggression . . . . That makes it a landmark moment, but one that analysts caution must be viewed in the context of the conflict between Israel and Palestine, rather than as a standalone global harbinger.[9]

---

[6] This article uses the phrase "law of armed conflict (LOAC)" to refer to (a) the coherent system of the law of war principles (i.e., military necessity, humanity, honor, distinction, and proportionality) and (b) treaties and customary State practice that relate to the means and methods of warfare, as well as the protection of civilians and their objects. *See* OFF. OF GEN. COUNS., U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL §§ 1.3, 2.1 (12 June 2015) (C3, 13 Dec. 2016) [hereinafter LAW OF WAR MANUAL].

[7] An effect is the "result, outcome, or consequence of an action." *See* JOINT CHIEFS OF STAFF, DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 69 (Jan. 2021).

[8] For the purposes of this article, "cyber warfare" is the conduct of military operations between belligerents that occur in the "cyber domain" or "cyberspace." Cyberspace is a "global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." *Id.* at 55.

[9] Lily Hay Newman, *What Israel's Strike on Hamas Hackers Means for Cyberwar*, WIRED (May 6, 2019, 4:43 AM), https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar.

Although the Israeli Defense Force strike may have been a "landmark moment," the United States reserved the right to retaliate against cyber attacks using conventional weapons as early as 2011.[10]

Regardless of whether the Israeli Defense Force's strike is isolated to only that conflict, this third form of cyber warfare could exist in other places and in other domains. Arguably, more threatening is the use of kinetic weapons, such as a deep-submersible submarine, to target submarine cables either in the opening salvos of a war or during the conflict. The only legally binding treaty in force today that relates to the targeting of submarine cables in wartime is the 1907 Hague Regulations, which pertain only to the seizure or destruction of submarine cables connecting occupied and neutral territories.[11] That treaty permits targeting submarine cables "in the case of absolute necessity."[12] Moreover, through historical precedent and the application of LOAC developed in the Industrial Age, submarine cables remain lawful targets.

In the cyber age, however, reliance by States and the civilian populations on submarine cables cannot be overstated. Approximately 400 garden-hose-sized cables transfer an estimated 97 percent of international communication.[13] In addition to carrying electronic mail, submarine cables transmit information that is necessary to carry out almost every facet of modern life, such as accessing social media data, streaming live video, or transmitting financial transactions.[14] This ability to share data globally via undersea telecommunications infrastructure is vital during moments of international crisis, such as a global pandemic with little thought on how much society relies on this network of fiber-optic garden hoses on the ocean floor. Thus, the targeting of just a few of these submarine cables, especially

---

[10] David Alexander, *U.S. Reserves Right to Meet Cyber Attack with Force*, REUTERS (Nov. 15, 2011, 7:48 PM), https://www.reuters.com/article/us-usa-defense-cybersecurity/u-s-reserves-right-to-meet-cyber-attack-with-force-idUSTRE7AF02Y20111116.

[11] 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. 54, Oct. 18, 1907, 36 Stat. 2277 [hereinafter 1907 Hague Regulations].

[12] *Id.*

[13] DOUGLAS BURNETT ET AL., SUBMARINE CABLES: THE HANDBOOK OF LAW AND POLICY 2 (2014). Although there are submarine cables that transmit electrical power, this article is primarily focused on submarine telecommunications cables.

[14] Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 CATH. UNIV. J.L. & TECH 57, 58 (2015).

those connecting developing States and economies to the global marketplace, can have drastic and injurious consequences.

The fact that the security of submarine cables are threatened by both kinetic effects in the sea domain as well as cyber effects in the cyber domain is illustrative of the new reality that modern warfare no longer consists of lines on a battlefield.[15] The concept of "all-domain operations" combines the traditional domains of warfare (i.e., land, sea, and air) with "space, cyber, deterrent, transportation, electromagnetic spectrum operations, missile defense—all of these global capabilities together . . . to compete with a global competitor and at all levels of conflict."[16] To keep pace with battlefield realities and emerging concepts related to the use of force, LOAC must reflect modern warfare.

The current LOAC approach focuses on domain warfare, such as the laws of land, naval, air and missile, cyber, and space warfare. However, the Russian *Losharik* is an example of how advanced technologies can threaten multiple domains. In 2018, the Chairman of the Joint Chiefs of Staff wrote that "[w]hile the fundamental nature of war has not changed, the pace of change and modern technology, coupled with shifts in the nature of geopolitical competition, have altered the character of war in the 21st century."[17] As the character of warfare has changed, so too have the effects of destroying objects that have historically been lawfully targeted, such as submarine cables. The targeting of submarine cables is illustrative of how modern warfare—specifically all-domain operations—has outpaced the ability of LOAC to adequately protect critical civilian infrastructure. To thoroughly understand the legal issues related to targeting submarine cables, one must not simply apply a single-domain LOAC framework (e.g., the law of naval warfare for operations in the sea domain), but rather take an all-domain approach and analyze the target under (or at least consider

---

[15] Aaron Mehta, *'No Lines on the Battlefield': Pentagon's New War-Fighting Concept Takes Shape*, DEF. NEWS (Aug. 14, 2020), https://www.defensenews.com/pentagon/2020/08/14/no-lines-on-the-battlefield-the-pentagons-new-warfighting-concept-takes-shape.

[16] Colin Clark, *Gen. Hyten on the New American Way of War: All-Domain Operations*, BREAKING DEF. (Feb. 18, 2020, 7:01 AM), https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations.

[17] General Joseph F. Dunford Jr., *The Character of War and Strategic Landscape Have Changed*, 89 JOINT FORCES Q., no. 2, 2018, at 2.

the relevance of) the laws applicable to military operations in the cyber domain as well.

Upon considering the civilian population's reliance on submarine cables and the modern threat during armed conflict, it is clear that current LOAC rules and interpretations are unsatisfactory when applied to the targeting of submarine cables. Therefore, taking feasible precautions[18] during all-domain operations and mitigating harm to civilians in the cyber age requires adopting a new approach to LOAC. One approach, which is arguably the simplest, is to recognize "data" as an "object." This approach, however, has far-reaching consequences beyond the protection of submarine cables. A second, more targeted approach is to develop a special legal regime designed to protect the tangible networks that transfer data, such as submarine cables. This article focuses on the development of a new legal regime.[19]

This article explores a *lex ferenda* [20] that places submarine communication cables under special protection in the event of armed conflict.[21] Moreover, it focuses on the *jus in bello* targeting of submarine cables and presupposes that the intentional destruction of a submarine cable during peacetime, especially by a State's armed force, constitutes a belligerent act justifying the use of force in self-defense under the United Nations Charter and *jus ad bellum* principles.[22] Part II provides background on the development and use of submarine cables and their importance within today's global economic and social order. Part III presents a brief overview of the international legal regime that protects submarine cables in peacetime,

---

[18] "Combatants must take feasible precautions in planning and conducting attacks to reduce the risk of harm to civilians and other persons and objects protected from being made the object of attack." LAW OF WAR MANUAL, *supra* note 6, § 5.11.

[19] Whether the LOAC should consider "data" a type of "object" is a complex issue deserving extensive research and analysis. How the LOAC principles of distinction and proportionality would apply to the specific data transmitted through submarine cables is outside the scope of this article.

[20] *Lex Ferenda*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining the term as "law proposed for enactment").

[21] This article will not discuss whether hacking or some other form of interference with submarine cables in wartime violates international law.

[22] *See* INT'L INST. OF HUMANITARIAN L., SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Lousie Doswald-Beck ed., 1994), *reprinted in* 309 INT'L COMM. RED CROSS 595 (1995). Paragraph 60 of the *San Remo Manual* lists various belligerent acts that would render enemy merchant vessels military objectives, one of which is cutting undersea cables. *Id.* at 640.

while Part IV examines the current threat to submarine cables. Part V evaluates the *lex lata* (the law as it exists)[23] of targeting submarine cables in naval warfare and introduces the precedent of targeting them during naval operations in past conflicts. Given that targeting submarine cables achieves military effects across domains, Part VI presents the issue of targeting submarine cables in the cyber warfare context. Finally, Part VII provides recommendations on how to ensure the protection of submarine cables. Before examining the relevant legal regimes and LOAC principles, a brief recitation of the history of submarine cables helps to illuminate the issues.

II. Development and Use of Submarine Cables

"The United Nations, in 2010, described submarine cables as 'critical communications infrastructure' and 'vitally important to the global economy and the national security of all States.'"[24] Having a basic understanding of the development of this technology is critical to understanding its unique importance to the global economic and social order and the impact on the civilian population.

Halfway between the United States and the United Kingdom, in the middle of the Atlantic Ocean, U.S. and U.K. warships made history on 29 July 1858 when they spliced together two ends of copper cable and dropped it to the seafloor.[25] Eighteen days later, Queen Victoria and President James Buchannan would exchange telegrams.[26] What would have likely taken weeks or months to transmit by ship took only 17 hours and 40 minutes via cable.[27] While the cable would last only a few days, it "marked the first step in a communications revolution that would lead, ultimately, to the creation of the internet."[28] After Alexander Graham Bell's invention of the telephone in 1875 and the discovery of polyethylene[29] in 1933, a suitably protected submarine cable could carry more than one voice channel.[30] In

---

[23] *Lex Lata*, BLACK'S LAW DICTIONARY (11th ed. 2019).
[24] Davenport, *supra* note 14, at 62.
[25] SUNAK, *supra* note 1, at 12.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] Polyethylene is a light, synthetic resin that forms the most widely used plastic in the world and can be modified to take on the properties of rubber. *Polyethylene*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/science/polyethylene (last visited Aug. 6, 2021).
[30] LIONEL CARTER ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECT THE WORLD 14 (2009).

1956, two newly laid submarine cables between the United Kingdom and Newfoundland transmitted 707 calls between London and North America on their first day in use.[31]

With the advent of satellite communications technology in the 1970s and the 1980s, the transmission of a majority of international telecommunications was through space rather than through the century-old copper submarine cables then in existence.[32] However, the development of fiber optic technology would change the balance, and, in 1988, the first trans-oceanic fiber optic cable was put in service.[33] Since their employment, submarine cables have "outperform[ed] satellites in terms of the volume, speed, and economics of data and voice communications."[34]

There are now close to 448 submarine cables[35] grouped into more than 200 independent cable systems owned by a number of international consortiums, each consisting of anywhere between 4 and 30 private companies.[36] A single submarine cable consists of six to twenty-four hair-like, glass fiber optic wires.[37] Each wire can transmit 400 gigabytes of data per second via wavelengths of light that travel about 180,000 miles per second.[38] About the diameter of a garden hose,[39] submarine cables transmit approximately 97 percent of international communication.[40] The "backbone of the global economy,"[41] submarine cables provide the means to exchange more than 10 trillion U.S. dollars in daily transactions,[42] and they transmit millions of financial messages to over 8,300 banks and securities institutions

---

[31] *Id.*
[32] *Id.* at 15.
[33] *Id.* at 16.
[34] *Id.* at 15–16.
[35] Carl Schreck, *Explainer: How Vulnerable Are Undersea Cables That U.S. Says Russia Is Tracking?*, RADIO FREE EUR. (June 12, 2018, 4:44 PM), https://www.rferl.org/a/explainer-undersea-cables-u-s-says-russia-vulnerable-internet/29287432.html.
[36] INT'L SEABED AUTH., TECH. STUDY NO. 14, SUBMARINE CABLES AND DEEP SEABED MINING 17 (2015).
[37] Davenport, *supra* note 14.
[38] SUNAK, *supra* note 1, at 14.
[39] See *infra* app. A, for a photograph that depicts the size of modern cables; see *infra* app. B, for a map of active and planned cable networks with their associated cable landing stations.
[40] BURNETT ET AL., *supra* note 13.
[41] INT'L SEABED AUTH., *supra* note 36.
[42] Davenport, *supra* note 14, at 6 (quoting MICHAEL SECHRIST, NEW THREATS, OLD TECHNOLOGY 9 (2012).

in more than 200 countries.[43] Given the heavy reliance on submarine cables in the global marketplace, "[t]hese international connections over fiber-optic cables mean that cable disruptions can potentially affect multiple countries and lead to cascading issues internationally . . . ."[44]

From a U.S. defense perspective, submarine cables are a vital link to U.S. forces, as well as U.S. allies and partners, overseas. In fact, the U.S. Department of Defense (DoD) relies on commercially owned submarine cables to transmit 95 percent of its international communications.[45] For example, the DoD has used submarine cables to stream live video data captured by unmanned aerial vehicles above the battlefields of Iraq and Afghanistan to command centers at home.[46] The DoD also uses submarine cables to control the battlespace by transmitting data that is then collected, processed, stored, disseminated, and managed via the Global Information Grid.[47] Given the DoD's reliance on commercial submarine cables, protection of this undersea network during armed conflict is critical because, "without ensured cable connectivity, the future of modern warfare is in jeopardy."[48]

III. Status of Submarine Cables Under International Law

The oldest international convention currently in force and dedicated to the protection of submarine cables is the 1884 Convention for the Protection of Submarine Telegraph Cables (1884 Convention).[49] "The 1884 Cable Convention is a stand-alone convention dealing solely with the *protection* of submarine telegraph cables."[50] Its primary purpose is to require signatory States to adopt domestic legislation that criminalizes the destruction of

---

[43] JAMES DEAN ET AL., THREATS TO UNDERSEA CABLE COMMUNICATIONS 11 (2017).
[44] *Id.*
[45] Hinck, *supra* note 5.
[46] Brian Mockenhaupt, *We've Seen the Future, and It's Unmanned*, ESQUIRE (Oct. 14, 2009), https://www.esquire.com/news-politics/a6379/unmanned-aircraft-1109.
[47] *Global Information Grid*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/global_information_grid (last visited Aug. 6, 2021) (defining the Global Information Grid as "[t]he globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.").
[48] MICHAEL SECHRIST, CYBERSPACE IN DEEP WATER 5 (2010).
[49] Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989 [hereinafter 1884 Convention].
[50] Davenport, *supra* note 14, at 67.

submarine cables.[51] Forty States are a party to the 1884 Convention, including the United States and Russia.[52] Although Article X permits warships to visit and board other ships suspected of tampering with submarine cables, the 1884 Convention does not apply in armed conflict, and it expressly prohibits the boarding of warships of other States.[53]

Moreover, while the 1884 Convention is the only treaty solely dedicated to the protection of submarine communications cables, other legal conventions also include provisions that relate to submarine cables. First, in the 1958 Geneva Conventions on the High Seas and the Conventional Shelf, the international community "secured the legal principle that [S]tates could not obstruct the construction of undersea cables in international waters."[54] In 1982, the Third United Nations Convention on the Law of the Sea (UNCLOS), which superseded the 1958 Geneva Convention for signatory States, expanded submarine cable protections as part of a comprehensive and monumental effort to develop the "constitution for the oceans."[55] Of the 320 articles and 9 annexes, 6 articles address submarine cables. Article 113 essentially restates Article II of the 1884 Convention, requiring States to "adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence . . . shall be a punishable offence."[56] Unlike the 1884 Convention, however, UNCLOS "stops short of giving warships the right to board a vessel suspected of intentionally trying to damage undersea cables in international waters, making it difficult for naval powers to effectively deter hostile vessels."[57] In addition to criminalizing injury to submarine

[51] 1884 Convention, *supra* note 49, 24 Stat. at 993 ("The breaking or injury of a submarine cable, done willfully or through culpable negligence, and resulting in the total or partial interruption or embarrassment of telegraphic communication, shall be a punishable offense, but the punishment inflicted shall be no bar to a civil action for damages.").
[52] Davenport, *supra* note 14, at 67 (citing BURNETT ET AL., *supra* note 13, at 64).
[53] 1884 Convention, *supra* note 49, 24 Stat. at 997 ("It is understood that the stipulations of this Convention shall in no wise affect the liberty of action of belligerents.").
[54] SUNAK, *supra* note 1, at 16.
[55] Davenport, *supra* note 14, at 67.
[56] United Nations Convention on the Law of the Sea art. 113, Dec. 10, 1982, 1833 U.N.T.S. 397.
[57] SUNAK, *supra* note 1, at 17.

cables, UNCLOS protects States' "*freedom to lay, repair and maintain*" submarine cables while balancing the rights of coastal States.[58]

IV. The Threat to Submarine Cables

"Cables are inherently vulnerable as: their location is generally publicly available [so as to mitigate accidental damage by fishermen, etc.], they tend to be highly concentrated geographically both at sea and on land, and it requires limited technical expertise and resources to damage them."[59] While anchors and dredging equipment can accidently sever submarine cables, some of the Russian Navy's submarines can exploit these vulnerabilities while operating on the high seas and outside State jurisdiction.[60] In addition to deep-sea nuclear submarines like the *Losharik*, Russia also deploys a *Yantar*-class intelligence vessel that has the capability to carry two smaller submarines, which some commentators believe are designed to cut or hack submarine cables.[61] In 2015, the *Yantar* was discovered probing a cable route during its voyage to Cuba, resulting in reports that the Russians were targeting highly classified DoD-owned submarine cables connecting the naval base at Guantanamo Bay with Miami.[62] The suspicion that Russia is actively exercising the ability to target submarine cables has provoked strong responses from U.S. national security leaders. In 2017, Admiral Michelle Howard, who at the time was serving as the commander of U.S. Naval Forces Europe, stated that "[w]e're seeing activity [by Russia] that we didn't even see when it was the Soviet Union. . . . [T]he activity in this theatre has substantially moved up in the last couple of years."[63] Furthermore, Admiral James Stavridis, who retired in 2013 as the Supreme Allied Commander Europe, has opined that Russia's relative weakness, when matched with conventional forces of the North Atlantic Treaty Organization, "raises the appeal of asymmetric targets like fibre-optic cables."[64]

---

[58] Davenport, *supra* note 14, at 68.
[59] SUNAK, *supra* note 1, at 19.
[60] *See* Ma & Pickrell, *supra* note 2.
[61] SUNAK, *supra* note 1, at 30.
[62] Hinck, *supra* note 5.
[63] Andrea Shalal, *Russian Naval Activity in Europe Exceeds Cold War Levels—U.S. Admiral*, REUTERS (Apr. 9, 2017, 10:54 AM), https://www.reuters.com/article/usa-russia-military-idINKBN17B0OA.
[64] Stavridis, *supra* note 1, at 10.

In addition to voicing concerns, other departments in the U.S. Government have taken substantive action. In 2018, for example, the U.S. Treasury Department sanctioned five Russian firms and three Russian nationals alleged to have provided support to Russia's primary security agency, the Federal Security Service, in tracking underwater fiber-optic cables.[65] In support of the Treasury Department's sanctions, Congressman Jim Langevein, who serves as a member of both the House Armed Services and House Homeland Security Committees, stated that, "[w]ere those [cables] ever to be cut, there would be significant damage to our economy and to our everyday lives."[66] In addition to having the capability, Russia has also shown a willingness to destroy access to data in armed conflict. During the annexation of Crimea in 2014, one of Russia's first acts was to disrupt internet connectivity to the Crimean peninsula and isolate it from the rest of Europe.[67]

Given that Russia has the technological capability in its deep-sea submersibles and intelligence ships to attack submarine cables, as well as the willingness to do so, as shown during its invasion of Crimea, the threat to submarine cables is real. If coordinated attacks against multiple submarine cables were to occur at the outbreak of armed conflict, there would likely be a catastrophic impact on not only the targeted belligerent, but also the global economic and social order as a whole. The question then becomes whether submarine cables are lawful targets under the current LOAC rules and interpretations.

V. The Law of Naval Warfare and Submarine Cables

The issue of whether submarine cables are legitimate targets during armed conflict is a historical one.

> The issue was raised regularly in the nineteenth century—from an 1864 draft treaty among France, Brazil, and others,

---

[65] Morgan Chalfant & Olivia Beavers, *Spotlight Falls on Russian Threat to Undersea Cables*, THE HILL (June 17, 2018, 8:14 PM), https://thehill.com/policy/cybersecurity/392577-spotlight-falls-on-russian-threat-to-undersea-cables.

[66] *Id.*

[67] Damien Sharkov, *Russian Ships Could Cause 'Catastrophe' for West by Cutting Transatlantic Internet Cables*, NEWSWEEK (Dec. 15, 2017, 5:08 AM), https://www.newsweek.com/russian-forces-could-cause-catastrophe-west-cutting-internet-cables-749047.

> to the 1874 Brussels conference on the laws of war, to the 1879 meeting of the Institut de Droit International (IDI) and the 1882 Conference for the Protection of Submarine Cables. But cable neutralization was not achieved.[68]

Despite the recognition of their importance to the global economic and social order and the multiple legal regimes in force to protect them in peacetime, efforts to examine their status in armed conflict is almost non-existent. In fact, the primary legal handbook on submarine cables "notes the potential risk of terrorist attacks, but says surprisingly little about the threat of war."[69]

The status of submarine cables in armed conflict may receive such little attention because State action and a traditional application of LOAC suggest that the matter is settled. After all, as historical precedent has shown, belligerents have targeted submarine cables since the technology's inception. However, if advances in technology have perpetuated the evolution of all-domain warfare and changed the character of war, it begs the question of whether the status of this undersea technology as a legitimate target should also change. "In our world so dependent on internet interconnectivity, States have still not agreed to protect submarine cables from the putative rights of belligerents."[70]

This part will explore the relevant *lex lata* of targeting submarine cables. Despite explicit language that destruction of submarine cables in armed conflict is to be prohibited or avoided, historical precedent has clearly exploited the caveats and exceptions included in the restatements discussed below, rendering the current rules weak in their ability to protect such a vital component of the global economic and social order.[71]

---

[68] Douglas Howland, *The Limits of International Agreement: Belligerent Rights vs. Submarine Cable Security in the Nineteenth Century*, 2 JUS GENTIUM: J. INT'L LEGAL HIST. 67, 71 (2017).
[69] *Id.* at 92.
[70] *Id.*
[71] *See* James Kraska, *Submarine Cables in the Law of Naval Warfare*, LAWFARE (July 10, 2020, 8:01 AM), https://www.lawfareblog.com/submarine-cables-law-naval-warfare.

A. *Lex Lata* of Submarine Cables in the Law of Naval Warfare

Before reviewing the history of targeting submarine cables in wartime, it is informative to review the *lex lata* related to the protection of submarine cables. The only LOAC legal instrument that relates specifically to submarine cables is Article 54 of the 1907 Hague Regulations.[72] Article 54, however, only applies to submarine cables connecting occupied territory with neutral territory. Therefore, to obtain some clarity regarding the legal status of submarine cables in wartime, one must look to the various restatements. This section provides a brief review of the three primary, non-binding legal treatises related to submarine cables and the laws of naval warfare.

1. Oxford Manual of the Laws of Naval Warfare *(1913)*

Under Article 54, the *Oxford Manual of the Laws of Naval Warfare* suggests that the rules governing the destruction of submarine cables during wartime fall under a binary analytical framework: (1) status of the States connected by cables and (2) jurisdiction pertaining to the maritime zone where the cables are targeted.[73] The special committee reinforced the consensus that cables connecting belligerents or two points within a belligerent State are lawful targets. Additionally, with regard to cables connecting belligerents with neutral States, the special committee wrote that these cables may also be destroyed, but it is unlawful to destroy a cable in the waters of the neutral State. "On the high seas," however, Article 54 C states, "this cable may not be seized or destroyed unless there exists an effective blockade and within the limits of that blockade, on consideration of the restoration of the cable in the shortest time possible."[74] Finally, the special committee stated that "[s]eizure or destruction may never take place except in case of absolute necessity."[75]

---

[72] 1907 Hague Regulations, *supra* note 11.
[73] INST. OF INT'L LAW, THE LAWS OF NAVAL WARFARE GOVERNING THE RELATIONS BETWEEN BELLIGERENTS art. 54 (1913), *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 857 (Dietrich Schindler & Jiří Toman eds., 1988).
[74] *Id.*
[75] *Id.*

2. San Remo Manual on International Law Applicable to Armed Conflicts at Sea *(1994)*

Prepared by a group of "legal and naval experts . . . . [t]he purpose of the [*San Remo*] *Manual* is to provide a contemporary restatement of international law applicable to armed conflicts at sea."[76] Within the *San Remo Manual*, the only rule that explicitly relates to submarine cables is paragraph 37, which states: "Belligerents shall take care to avoid damage to cables and pipelines laid on the sea-bed which do not exclusively serve the belligerent."[77] While recognizing the "concern for protection of cables," the explanation to paragraph 37 acknowledges "that cables or pipelines exclusively serving one or more of the belligerents might be legitimate military objectives."[78]

3. Oslo Manual on Select Topics of the Law of Armed Conflict *(2020)*

Funded by the Norwegian Ministry of Defense, a group of experts convened in Oslo in 2015 to address the gaps created by advancements in technology and military concepts since the 2009 Program on Humanitarian Policy and Conflict Research's *Manual on International Law Applicable to Air and Missile Warfare*.[79] The group of experts restated the rule that "[s]x."[80] The caveat "unless they qualify as lawful targets" creates sufficient ambiguity to render the rule essentially worthless. Additionally, the commentary to Rule 69 notes that, although

> Article 54 of the 1907 Hague Regulations and the provisions of the *San Remo Manual* seem to reflect correctly the *lex lata* insofar as submarine pipelines and submarine high voltage cables are concerned. . . . [i]t is, however, doubtful whether the 1907 Hague Regulations and the *San Remo* provisions also apply to submarine communications cables.[81]

---

[76] INT'L INST. OF HUMANITARIAN L., SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA 5 (Lousie Doswald-Beck ed., 1994).
[77] *Id.* at 111.
[78] *Id.*
[79] OSLO MANUAL ON SELECT TOPICS OF THE LAW OF ARMED CONFLICT: RULES AND COMMENTARY, at v–vi (Yoram Dinstein & Arne Willy Dahl eds., 2020).
[80] *Id.* at 63.
[81] *Id.*

The international legal experts in Oslo recognized how technological advances have changed the character of the effects related to targeting submarine cables. They stated that "other than telegraphic cables, modern submarine communications cables are the backbone of global data traffic. . . . Accordingly, it is important to distinguish between submarine communications cables and other submarine cables."[82] That distinction, however, is neither required under any sort of legal framework nor apparent in the history of naval warfare and the activities of modern navies.

B. Historical Precedent

Given the utility of telegraph cables for military operations in wartime, the status of submarine cables in armed conflict has been a topic of discussion since their inception.

> [A]s the submarine cable network developed, the question of its destruction in warfare was present from the start. The conferences and discussions about cable security between 1864 and 1907 demonstrate that the great powers, leading statesmen, and international lawyers were arguably committed to making the world an environment safer for war.[83]

The first and only expressed prohibition of targeting submarine cables in wartime was included in the 1864 draft treaty between France, Brazil, Haiti, Italy, and Portugal.[84] The treaty, however, was suspended in 1872 because the cable was never laid.[85] Additionally, just prior to the Franco-Prussian War, the United States intended to host an international convention in Washington to resolve the issue of submarine cables during wartime.[86] Because the conflict raging in Europe at the time consumed the U.S. Government and other States, the convention never occurred. Historians suggest that had the convention taken place in Washington, it likely would have concluded that targeting cables during wartime amounted to an act of

---

[82] *Id.*
[83] Howland, *supra* note 68, at 70.
[84] BURNETT ET AL., *supra* note 13, at 66.
[85] Howland, *supra* note 68, at 78.
[86] R. J. R. Goffin, *Submarine Cables in Time of War*, 15 L.Q. REV. 145, 146 (1899).

piracy, and it may have developed a legal instrument to prohibit the targeting of international telecommunications in war and in peace.[87]

More than a century before the tragic deaths of the Russian sailors in July 2019, the U.S. Navy was targeting submarine cables in their maritime operations. On 24 May 1898, readers of the *New York Times* awoke to the headline "*Right to Cut Cables in War; Admiral Dewey Created a New Precedent Under the Law of Nations in Manila Bay*."[88] At the time, U.S naval forces were engaged in fleet operations against the Spanish Armada in the Philippines during the Spanish-American War. In order to degrade the command and control of the Spanish fleet, Admiral Dewey ordered the submarine telecommunications cables linking the Philippines with Hong Kong (and thus the rest of the world) be cut. As the *New York Times* declared, Admiral Dewey established international legal precedent on that day in Manila Bay. Even though submarine cables were legitimate targets at the time, many believed that "a belligerent was obliged to recompense the damage when peace was restored."[89] When the U.S. Government refused to indemnify the British owner of the cable, diplomats and international legal experts grew concerned.[90] As a result, during the fourth Hague Peace Convention in 1907, drafters included a section that required compensation to the cable owner and permitted the seizure or destruction of submarine cables in neutral waters only under the condition of absolute necessity.[91]

Both World Wars also supported the case that submarine cables were lawful targets. At the outbreak of World War I, Britain targeted Germany's submarine cables, and Germany retaliated by targeting Britain's cables in the Pacific and Indian Oceans in an attempt to isolate London from its colonies outside Europe.[92] The same activity also occurred during World War II. For example, during Operation Sabre, an Australian Navy midget

---

[87] *Id.*

[88] *Right to Cut Cables in War: Admiral Dewey Created a New Precedent Under the Law of Nations in Manila Bay*, N.Y TIMES, May 24, 1898, at 2; *see* Jonathan Reed Winkler, *Silencing the Enemy: Cable-Cutting in the Spanish-American War*, WAR ON THE ROCKS (Nov. 6, 2015), https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war.

[89] Howland, *supra* note 68, at 72.

[90] *Id.*

[91] *Id.*

[92] Davenport, *supra* note 14, at 80; *see also* Mark Stout, *Trans-Atlantic Bandwidth: Then and Now*, WAR ON THE ROCKS (Oct. 30, 2015). https://warontherocks.com/2015/10/trans-atlantic-bandwidth-then-and-now.

submarine cut the undersea cable linking Singapore with Saigon, forcing the Japanese to send messages via encrypted radio signal that the Allies had decoded earlier in the war.[93]

More recently, when Russia invaded Ukraine's Crimean Peninsula, one of its first acts at the outbreak of the conflict was to target Crimea's internet. "According a 2016 Chatham House report, during the 2014 invasion of Crimea, Russian forces seized the peninsula's main internet traffic exchange point, isolating Crimea's internet from the rest of the world at a key moment in the conflict."[94]

Although the history shows multiple attempts to protect submarine cables, State practice has consistently been to target the cables in wartime and exploit the "liberty of action of belligerents"[95] exception in the 1884 Convention. If navies were to apply current LOAC rules and interpretations today, despite the change in technology and their impact to the civilian population, the analysis suggests that submarine cables would remain lawful targets.

VI. The Law of Cyber Warfare and Submarine Cables

Despite the fact that the binding rules found in the 1907 Hague Regulations and the non-binding restatements of the *Oxford, San Remo*, and *Oslo Manuals* suggest that submarine cables are protected during armed conflict, an analysis under an Industrial Age, single-domain application of LOAC rules suggests otherwise. To reconcile this inconsistency, the development of legally binding protections must be considered. Before exploring possible ways to ensure that submarine cables are protected during armed conflict, it is worth exploring the matter through the context of international law as applied to cyber warfare.

Two fundamental issues arise when discussing whether a single-domain approach to applying LOAC principles or Industrial Age LOAC treaties sufficiently apply in the cyber age: (1) which objects should be protected if

---

[93] *Operation Sabre Helps End War in the Pacific*, AUSTL. GOV'T: DEP'T OF VETERANS' AFFS., https://anzacportal.dva.gov.au/stories-service/australians-war-stories/operation-sabre-helps-end-war-pacific (June 3, 2019).
[94] Hinck, *supra* note 5.
[95] 1884 Convention, *supra* note 49, 24 Stat. at 997 ("It is understood that the stipulations of this Convention shall in no wise affect the liberty of action of belligerents.").

the LOAC principles of distinction and proportionality are meant to mitigate harm to the civilian population, and (2) whether the law that currently exists can adequately protect those objects. The view of a majority of experts that produced the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, a comprehensive treatise discussed further below, is that LOAC protects tangible objects but not intangible ones (e.g., data).[96] In the cyber age, this interpretation fails to fulfill the legal obligation to mitigate harm to the civilian population. Just as it is impossible to separate the ship from the sea, it is illogical to distinguish the intangible data from the tangible networks it traverses when applying LOAC to cyber operations. The physical layers of cyberspace are insignificant without the invisible data that flows through it. As evidenced in the scholarship related to LOAC in cyber warfare, the primary issue to settle is how to mitigate harm to the civilian population from the non-kinetic, intangible effects that modern military capabilities are able to achieve. Moreover, the issue of protecting submarine cables is similar in that the same non-kinetic, intangible effects are achieved through a method of warfare as old as the late nineteenth century's Spanish-American War.

It is the impact on the non-kinetic, intangible objects (e.g., data, economy, society) that make the destruction of submarine cables so costly—the so called "knock-on" effects.[97] The reason that their destruction has such economic and social impact is not because of what they are, but because of what they transmit. Under current LOAC rules and interpretations, the targeting of a bridge or railway, even if used by civilians, is permissive so long as there is a clear military advantage, such as the prevention of the transportation of weapons or troops.[98] The bridge or railway would have likely been targeted, despite the fact that it also carried civilians to jobs or goods to markets, upon both of which the civilian population depends. Under a traditional proportionality analysis, although the potential of death

---

[96] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 437 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL].

[97] Commander Peter Pascucci, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, 26 MINNESOTA J. INT'L L. 419, 449–51 (2017).

[98] *Cf.* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 56, June 8, 1977, 1125 U.N.T.S. 3 (prohibiting attacks on dams, dykes, and nuclear electrical generating stations because they contain dangerous forces and not because of their utility to the civilian population). Although 168 States have ratified Additional Protocol I, the United States has not. *See* LAW OF WAR MANUAL, *supra* note 6, § 5.13.1.

or injury to those civilians (and possibly the nature of the goods, such as medicine for sick noncombatants) is considered, international law currently ignores the intangible forces associated with the movement of the people and goods on that same bridge or road. For example, these intangible forces could include the skill of the civilian worker and his income or the impact the goods have on the health and welfare of the local village. Because these forces are impossible to calculate accurately and thus impractical to consider in a proportionality analysis, it traditionally has been prudent to focus only on quantitative factors, such as the civilian casualty count or the economic cost to the enemy's war effort when destroying or damaging a civilian object. Additionally, these forces usually only have a local or isolated effect, thus permitting their destruction to have minimal value in the context of an armed conflict.

In the cyber age, it has become more difficult to ignore the effects that the intangible forces, specifically data and its disruption, have on the civilian population as a whole. Where the global economic and social order of the Industrial Age depended on tangible networks (such as roads, bridges, railways, and ships) to carry tangible goods, people in the cyber age depend on the intangible as well. Unlike any time in history, the global economic and social order now relies on the expedient and uninterrupted transfer of data. Therefore, the issue raised in this new cyber age is whether an application of LOAC should recognize and protect the intangible as it has the tangible.

The international group of experts addressed this issue briefly in the *Tallinn Manual*. A majority maintained the view that, under existing law, "data is intangible and therefore neither falls within the 'ordinary meaning' of the term object . . . [t]herefore an attack on data *per se* does not qualify as an attack."[99] A minority of the experts, however, believed that certain civilian datasets should be protected from targeting, such as "social security data, tax records, and bank accounts," deletion of which "run[s] counter to the principle (reflected in Article 48 of Additional Protocol I) that the civilian population enjoys general protection from the effects of hostilities."[100] Whereas the classification of "data" under LOAC

[99] TALLINN MANUAL, *supra* note 96.

[100] *Id.* While the United States has not ratified Additional Protocol I, its position is that article 48 reflects customary international law. *See* COLONEL THEODORE T. RICHARD, UNOFFICIAL UNITED STATES GUIDE TO THE FIRST ADDITIONAL PROTOCOL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 83 (2019).

may be debatable, there is a consensus of how critical data is to the civilian population in the cyber age.

A. Applying *Jus in Bello* Principles to Targeting Submarine Cables in the Cyber Age

According to the *Tallinn Manual*, there are two "cardinal" principles of LOAC: the prohibition of unnecessary suffering and distinction.[101] From the principle of *distinction*, LOAC requires that if there is likely to be civilian collateral damage when targeting a military objective, the impact to the civilian person or object must be *proportional*.

1. Distinction

Rule 93 of the *Tallinn Manual* states that "the principle of distinction applies to cyber-attacks," requiring belligerents at all times to distinguish between civilian objects and military objectives.[102] The 1868 Saint Petersburg Declaration first articulated this rule, which was later adopted in Article 52(1) of Additional Protocol I,[103] stating in part that "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy."[104] The *Tallinn Manual* applies this rule to the cyber domain and states, "[c]ivilian objects shall not be made the object of cyber-attacks. Cyber infrastructure may only be made the object of attack if it qualifies as a military objective."[105]

As described above, both civilians and militaries use commercially owned submarine cables to transfer data between continents. "As a matter of law, status as a civilian object and military objective cannot coexist; an object is either one or the other. This principle confirms that all dual-use

---

[101] *Compare* RICHARD, *supra* note 100, at 420, *with* LAW OF WAR MANUAL, *supra* note 6, § 2.1. "Three interdependent principles—*military necessity*, *humanity*, and *honor*—provide the foundation for other law of war principles, such as *proportionality* and *distinction*, and most of the treaty and customary rules of the law of war." LAW OF WAR MANUAL, *supra* note 6, § 2.1.

[102] TALLINN MANUAL, *supra* note 96, at 420.

[103] While the United States has not ratified Additional Protocol I, its position is that article 52(1) reflects, in part, customary international law. The United States does, however, object to the rule holding that civilian objects shall not be the object of reprisals. *See* RICHARD, *supra* note 100, at 98 n.107.

[104] TALLINN MANUAL, *supra* note 96, at 434.

[105] *Id.*

objects and facilities are military objectives, without qualification."[106] The *Tallinn Manual*'s experts used the analogy of a road network to illustrate how the dual-use principle applies in the cyber domain. If belligerents use a bridge to transport materiel to the front line while the local civilian population also uses it for going about their everyday lives, it is a valid military objective because of its military use. The principle supports the conclusion that "so long as it is reasonably likely that a road in the network may be used, the network is a military objective subject to attack. There is no reason to treat computer networks differently."[107]

Therefore, under a traditional application of the dual-use principle, where civilians and militaries use submarine cables simultaneously, they are military objectives. Even though an object that is otherwise used primarily by civilians is a lawful target because its nature, location, purpose, or use makes an effective contribution to military action,[108] "it will be appropriate to consider in applying the principle of proportionality the harm to the civilian population that is expected to result from the attack on such a military objective."[109]

Another key issue raised by the principle of distinction is the positive obligation of States to keep their military objectives separate from civilians and civilian objects. "*Distinction* also creates obligations for parties to a conflict to take feasible measures to separate physically their own military objectives from the civilian population and other protected persons and objects."[110] Therefore, under current LOAC rules and interpretations, it may be necessary for militaries to refrain from utilizing submarine cables to transfer military related data during armed conflict in order to avoid harm to the civilian population. As stated above, the DoD currently uses commercial submarine cables to transmit 95 percent of its international communications.[111] By applying the traditional LOAC principle of distinction, without specific legal agreements to protect submarine cables in wartime, the DoD's ability to communicate with its forces overseas would collapse. Additionally, given that most States do not have the capacity or capability to lay government-owned cables for the exclusive use of their

---

[106] *Id.* at 446; *see* LAW OF WAR MANUAL, *supra* note 6, § 5.6.1.2.
[107] TALLINN MANUAL, *supra* note 96, at 446.
[108] *See* LAW OF WAR MANUAL, *supra* note 6, § 5.6.6.
[109] *Id.* § 5.6.1.2.
[110] *Id.* § 2.5.3.2.
[111] Hinck, *supra* note 5.

military, the part of the distinction principle obligating States to separate their military objectives from civilian objects is not a practical option at this time.

2. Proportionality

If the targeting of military objectives would result in injury to civilians or damage to civilian objects, a proportionality analysis is required. As Rule 113 of the *Tallinn Manual* states, "[a] cyber-attack that 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 is prohibited."[112] First, it is critical to understand that "[i]n war, incidental damage to the civilian population and civilian objects is unfortunate and tragic, but inevitable."[113] Therefore, the targeting of military objectives need not have zero impact to the civilian populations or its objects to be lawful.

Take, for example, a scenario in which Russia's navy, in support of a Middle East ally, targets five of the six cables located in the Mediterranean Sea that connect Egypt with Europe. A repaired *Losharik* would likely either sever the cables in real time or place remote-controlled explosives on the cables prior to the outbreak of the conflict. While the destruction of the cables themselves would cost the cable owner only a few hundred thousand dollars to repair, the incidental impacts would be much more costly. Egyptian internet capacity would degrade by 70 percent.[114] Further, because India heavily relies on the same five cables for 50 to 60 percent of its internet connectivity to Europe, the cutting would significantly affect their major economic outsourcing sector.[115] Despite the harm to Egypt's and India's civilian populations, both of which are neutral in the conflict, the primary purpose of targeting the cables would be degradation of the command and control capabilities of Russia's overseas enemy. By targeting the five submarine cables, their adversary's communications traffic to the region collapses and video streaming capacity degrades to a level that would require enemy commanders to decrease exponentially daily unmanned aerial vehicle flights that provide critical surveillance and kinetic strike

---

[112] TALLINN MANUAL, *supra* note 96, at 470.
[113] LAW OF WAR MANUAL, *supra* note 6, § 2.4.1.2.
[114] SUNAK, *supra* note 1, at 37 (recounting the 2008 destruction of five undersea cables that adversely affected Egypt's westbound internet connectivity).
[115] *Id.*

capabilities.[116] Regardless of the relatively low repair cost associated with the tangible damage to the cables, it would be unlikely, or at the very least extremely challenging, that a cable repair ship would be able to gain access and repair the cables within an area of active hostilities.

The incidental effects described above are not theoretical. In 2008, two merchant ships accidentally severed five submarine cables off the coast of Egypt, and the result was just as portrayed above.[117] Despite the far-reaching impact on the civilian population, whether Russia's targeting of the cables is lawful turns on whether the cutting is *excessive* when weighed against its military advantage. While there is no doubt that degrading a belligerent's ability to communicate with its forces overseas is advantageous, determining whether the collateral damage is *excessive* does not necessarily require the commander to calculate these difficult-to-measure incidental effects.

Although the term "excessive" is not defined in international law, the *Tallinn Manual*'s majority "took the position that extensive collateral damage may be legal if the anticipated concrete and direct military advantage is sufficiently great. Conversely, even slight damage may be unlawful if the military advantage expected is negligible."[118] The DoD offers additional guidance when attempting to determine whether damage would be excessive:

> Determining whether the expected incidental harm is excessive does not necessarily lend itself to quantitative analysis because the comparison is often between unlike quantities and values. The evaluation of expected incidental harm in relation to expected military advantage intrinsically involves both professional military judgments as well as moral and ethical judgments evaluating the risks to human life (e.g., civilians at risk from the attack, friendly forces or civilians at risk if the attack is not taken).[119]

---

[116] *Id.* at 21.
[117] *See id.* at 37 (providing several such examples).
[118] TALLINN MANUAL, *supra* note 96, at 473.
[119] LAW OF WAR MANUAL, *supra* note 6, § 5.12.3.

B. Submarine Cables in the *Tallinn Manual*

The status of submarine cable protections under the laws of cyber warfare has already been considered. Within its chapter on the law of the sea, the *Tallinn Manual* restates the freedoms of States regarding submarine cables established in UNCLOS.[120] It acknowledges that the "infliction of damage to cables by a State is prohibited as a matter of customary international law," but notes that the general rule is "without prejudice to the rules applicable during armed conflict."[121] Part IV of the *Tallinn Manual* covers how LOAC applies in the cyber domain, and it mentions submarine cables twice. Both times, the experts restate Article 54 of the 1907 Hague Regulations, which "provides that submarine cables connecting an occupied territory with neutral territory may be seized or destroyed 'in case of absolute necessity,' subject to the restoration and compensation after the end of war."[122]

Despite the direct economic and social harm to neutral States, the targeting of five garden-sized, fiber optic cables that cost a few hundred thousand dollars to repair[123] is minimal when compared to the degradation in the belligerent's command and control network. Thus, even if applying the *Tallinn* majority's interpretation of LOAC principles, the targeting of submarine cables remains lawful.

As shown above, applying a single-domain LOAC framework—using interpretations of LOAC principles and treaties developed in the Industrial Age—fails to satisfactorily protect necessary and critical civilian infrastructure during all-domain operations. A traditional interpretation of the LOAC principles (i.e., distinction and proportionality), treaty law developed in the Industrial Age, and State practice all suggest that targeting submarine cables remains lawful, despite the likely calamitous second and third order effects to the civilian population. However, if States (and their military lawyers) abandon the single-domain approach and instead view LOAC through an all-domain lens, gaps in legal protections, such as the targetability of submarine cables, may begin to be adequately addressed.

---

[120] TALLINN MANUAL, *supra* note 96, at 252.
[121] *Id.* at 256.
[122] *Id.* at 510, 551–52 (citing 1907 Hague Regulations, *supra* note 11).
[123] *See supra* Section VI.A.2.

VII. Protecting Submarine Cables in Modern Warfare

"The debate regarding whether [LOAC] applies to cyberspace is largely settled."[124] However, as the issue of targeting submarine cables illustrates, there are significant "deficiencies in the application of the principles of distinction and proportionality to cyberwar . . . ."[125] The lawfulness of naval operations are often viewed through a single-domain lens using LOAC principles that are "premised on a paradigm in which most of the deleterious consequences that [they seek] to temper are physically destructive or injurious."[126] However, when the operation seeks to achieve a cyber effect (e.g., targeting submarine cables), the result is that current LOAC rules and interpretations fall short of protecting the civilian population during all-domain operations. One solution is to develop a comprehensive LOAC regime for the cyber age, such as Additional Protocol IV.[127] This approach, however, comes with significant risks and is well outside the scope of this article. However, the overarching themes in such a discussion inform whether there should be a change to the law of naval warfare in order to place submarine cables under special protection during armed conflict.

Despite the historical precedent of targeting submarine cables in wartime, applying LOAC during all-domain operations should reflect how the evolution of technology has changed the ways in which civilian populations can be harmed or injured.[128] A severed telegraph cable may have had some local impact in Admiral Dewey's era, but it did not come close to the harm that the destruction of a submarine cable causes today. Therefore, to ensure that LOAC principles and rules in the cyber age provide adequate protections during all-domain operations, States must be obligated to protect submarine cables in wartime either through custom or treaty.

---

[124] Pascucci, *supra* note 97, at 451.
[125] *Id.*
[126] Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 289 (2014).
[127] *See generally* Pascucci, *supra* note 97.
[128] In the cyber age, disinformation can arguably be just as harmful to the civilian population as inaccessibility of data. While not the focus of this paper, perhaps the current LOAC principles and rules related to disinformation need to be re-examined given the potential modern effect.

A. 1884 Convention

The simplest remedy is to amend the 1884 Convention, which would require the consent of the thirty signatories. Although the amended 1884 Convention would not obligate non-signatory States, those States that have the technological and military capabilities to target cables in the high seas—mainly Russia and the United States—are signatories. If such a consensus could be reached, removing the language from Article XV ("shall in no wise affect the liberty of action of belligerents")[129] and explicitly declaring submarine cables unlawful targets in wartime would be sufficient to afford submarine cables special protection during armed conflict.

One State that did not sign the 1884 Convention and would thus be exempt from the amended treaty's prohibition of targeting submarine cables during armed conflict is the People's Republic of China. This is significant, given that State's growing blue-water naval capabilities. Moreover, because of China's exclusion under this approach, it would be far more effective to either develop a new treaty or articulate and defend a State practice that obligates all States that have the means, opportunity, and possible motive to target submarine cables in armed conflict.

B. New Convention on the Protection of Submarine Cables in Armed Conflict

Another approach is to initiate a stand-alone agreement that declares the importance of submarine cables to civilization and places them under special protection during wartime. While this approach requires the right geopolitical conditions just as much as it requires an acknowledgement of a legal necessity, the international community has made similar concessions before during periods of great power competition. The most analogous legal instrument designed to protect an object because of intangible effects is the 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict, which placed "cultural property" under "special protection" in the event of armed conflict.[130]

Within the cornucopia of LOAC treaties and conventions that followed the Geneva Conventions, the convention to protect cultural property is

[129] 1884 Convention, *supra* note 49, 24 Stat. at 997.
[130] *See* Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, S. TREATY DOC. NO. 106-1, 249 U.N.T.S. at 240.

unique. Most post-Geneva treaties, such as the "Convention on Prohibitions or Restriction on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects" (and its progeny)[131] and the "Chemical Weapons Convention," were designed to prevent unnecessary suffering—one of the cardinal principles of LOAC.[132] In the case of cultural property, however, destroying an ancient building or important statue neither violates the principle of unnecessary suffering nor constitutes a *prima facia* violation of the principle of distinction. However, due to broad agreement regarding how important cultural property is to the civilian population, and the intangible effects such as its intrinsic value or the loss of enjoyment by future generations, the international community developed a consensus to place these objects under special protection. Specifically, the Convention for the Protection of Cultural Property acknowledges that "the preservation of the cultural heritage is of great importance for all peoples of the world and that it is important that this heritage should receive international protection . . . ."[133]

Additionally, the support for such a unique LOAC restriction derived from the fact that there was some historical precedent recognizing the importance of cultural property to the civilian population. The Convention for the Protection of Cultural Property notes that it was "[g]uided by the principles concerning the protection of cultural property during armed conflict, as established by the Conventions of The Hague of 1899 and of 1907 and in the Washington Pact of 15 April, 1935."[134]

In the case of submarine cables, such a treaty would require States to recognize that the free flow of data between continents and the preservation of the global economic and social order is more crucial than the military advantage of degrading a belligerent's command and control capability during armed conflict. Mainly, mitigating harm to civilians during all-domain operations requires a new approach to taking feasible precautions that avoid non-kinetic, intangible injury to the civilian population. As shown above, there have been various historical attempts to prohibit the targeting of submarine cables in wartime. Each attempt failed not because

---

[131] Protocols prohibiting or regulating such weapons, as well as non-detectable fragments, mines, booby-traps, incendiary weapons, lasers, and remnants of war, were later adopted.
[132] *See* TALLINN MANUAL, *supra* note 96, at 420.
[133] *See generally* Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, *supra* note 130, S. TREATY DOC. NO. 106-1, at 16, 249 U.N.T.S. at 240.
[134] *Id.* (citations omitted).

of significant differences in principle, but for other reasons specific to the time and place. However, just as the international community went beyond the cardinal principles of LOAC to recognize the necessity to mitigate the "knock-on" effects of targeting cultural property, so too can it create a legal instrument designed to protect submarine cables.

C. State Practice and Customary International Law

Recent scholarship has included a thorough analysis of a customary international law [135] approach to protecting submarine cables in peacetime.[136] The difficulties with developing customary international law for peacetime protection—mainly creating a consensus in today's political environment—are all the more difficult and lead to greater dangers in armed conflict.

Difficult does not mean impossible, however, as it has been done before. The Truman Proclamation is one example of how State practice created customary international law and paved the way for the development of treaty law.[137] In 1945, President Harry Truman declared "the natural resources of the subsoil and sea bed of the continental shelf beneath the high seas but contiguous to the coasts of the United States as appertaining to the United States, subject to its jurisdiction and control."[138] This proclamation, which at the time was a "radical departure" from the law of the sea, eventually led to the 1958 Geneva Conference on the Law of the Sea.[139] It could be argued that the 1958 Geneva Conference, and from there UNCLOS, served as affirmation of unilateral State action that is taken in support of molding customary international law to reflect reality and technological advances.

---

[135] *See* LAW OF WAR MANUAL, *supra* note 6, § 1.8 ("*Customary international law* results from a general and consistent practice of States that is followed by them from a sense of legal obligation (*opinio juris*). Customary international law is an unwritten form of law in the sense that it is not created through a written agreement by States. Customary international law is generally binding on all States, but States that have been persistent objectors to a customary international law rule during its development are not bound by that rule. Assessing whether State practice and *opinio juris* have resulted in a rule of customary international law may be a difficult inquiry." (citations omitted)).

[136] *See, e.g.*, Lieutenant Commander 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 (2020).

[137] *Id.* at 43.

[138] Proclamation No. 2667, 10 Fed. Reg. 12303 (Oct. 2, 1945).

[139] O'Connor, *supra* note 136, at 44.

With regard to submarine cables, a proclamation declaring that (1) targeting submarine cables that connect the United States to another State constitutes an armed attack that would justify the use of force in self-defense and (2) targeting submarine cables in armed conflict is a violation of the principles of LOAC would not be a "radical departure" from today's international law. On the contrary, experts behind law of war publications such as the *Oxford, San Remo, Tallinn,* and *Oslo Manuals* already recognize the importance of submarine cables and have declared, with some relatively significant exceptions and caveats, that submarine cables deserve protection. Such a proclamation would be similar to adopting a "no first use" policy[140] declaring that, unlike in all the past conflicts discussed above, commencement of hostilities will not include the targeting of submarine cables. Given "the justifications for protecting underwater fiber optic cables are universal,"[141] this approach may begin to build diplomatic and political consensus toward future treaty efforts to legally prohibit the targeting of submarine cables. At the very least, it may effect customary international law in the practice of naval warfare.

VIII. Conclusion

While the changing character of war requires commanders and their legal advisers to develop an understanding of emerging issues related to all-domain threats, targeting submarine cables is an illustrative example of how it should also drive them to think of old issues in new ways. Since Admiral Dewey's actions in Manila Bay, navies have often legally targeted submarine cables on the basis that they are a valid military objective. However, given that technological advancements have made today's global economic and social order dependent on submarine cables, their destruction would have a significant and harmful impact on the civilian population.

One of the purposes of international law as it relates to the regulation of armed conflict is to enforce the principle that "the civilian population enjoys general protection from the effects of hostilities."[142] Although LOAC prevents the targeting of civilian objects, which most submarine cables inherently are, they are considered military objectives, and thus lawful targets, under the dual-use principle. Additionally, despite the likelihood

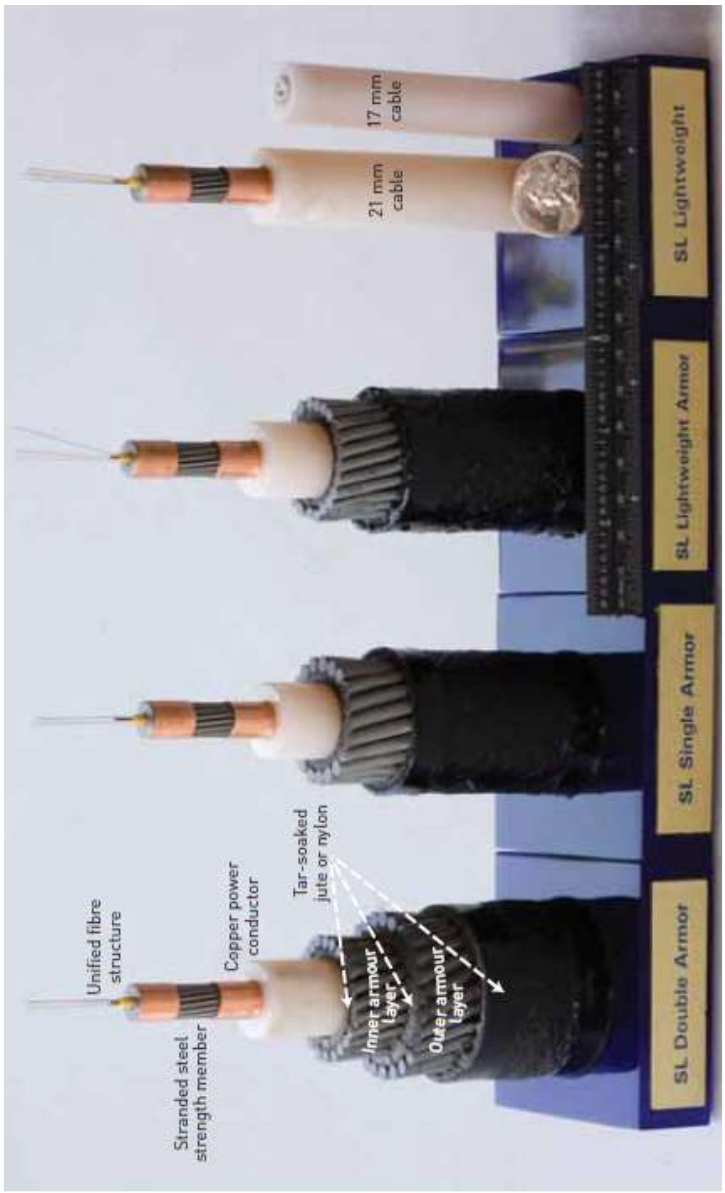
---

[140] AMY F. WOOLF, CONG. RSCH. SERV., IN10553, U.S. NUCLEAR WEAPONS POLICY: CONSIDERING "NO FIRST USE" (2021).
[141] O'Connor, *supra* note 136, at 49.
[142] TALLINN MANUAL, *supra* note 96.

that the destruction of a few submarine cables could have a harmful impact on the civilian population, they remain lawful targets because, under the traditional application of determining what is "excessive," the destruction of the cable itself would not outweigh the military advantage.[143] However, as the character of war has changed and civilian reliance on submarine cables has increased, LOAC must not only reflect the protective status of the tangible cable, but also seek to protect the intangible data it transmits and avoid the devastating "knock-on" effects that would result from its targeting. Therefore, modern warfare requires new approaches to LOAC, such as the development of international law that prohibits the targeting of submarine cables.

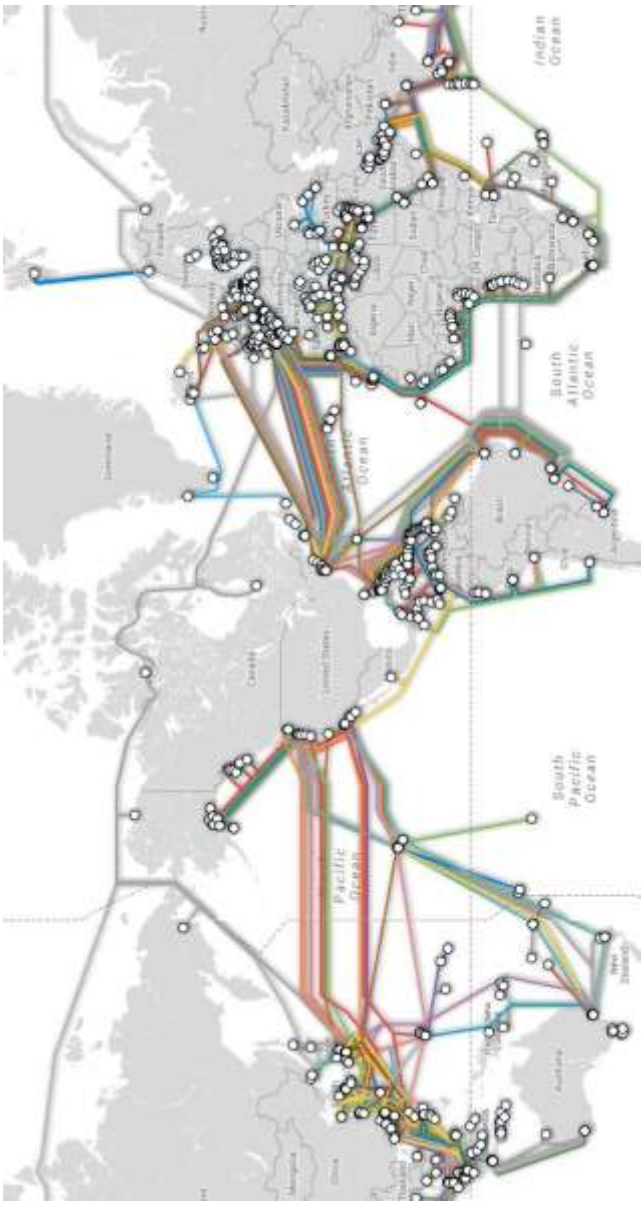
[143] LAW OF WAR MANUAL, *supra* note 6, § 5.12.3.

Appendix A. Photograph of fiber optic submarine cable.[*]



[*] CARTER ET AL., *supra* note 30, at 18.

Appendix B. Map of majority of submarine cable systems.*



* *Cable Data*, INT'L CABLE PROT. COMM., https://www.iscpc.org/information/cable-data (last updated Sept. 29, 2014).