LAWFARE

INTERNATIONAL LAW

Cutting the Cord: The Legal Regime Protecting Undersea Cables

By **Garrett Hinck**
Tuesday, November 21, 2017, 7:00 AM

DayZero: Cybersecurity Law and Policy

One of the U.S. economy's most critical resources is the massive network of undersea cables that transverse the globe, carrying the overwhelming majority of all internet traffic. Over 400 fiber optic cables carry 99% of transoceanic data, providing the physical links that bind our digital world together. This global infrastructure rests almost entirely in the hands of private companies.

In the modern geopolitical environment, the vulnerability of undersea communications cables stands out as an acute cyber security concern. Relatively little attention, however, has focused on the legal frameworks that govern the networks of glass and steel that form the literal backbone of our internet. This post lays out the threats to communications cables and the existing international laws protecting cables from intentional damage.

Landing of the Italy-U.S. submarine cable, 1925. (Source: German Federal Archive)

Threats to Undersea Cables

Physical Attack

Physical damage is the most direct threat to undersea cables. Such damage is usually accidental—often the cause is fishing ship nets and anchors. But history is rife with examples of navies intentionally attacking cables. At the outbreak of World War I, Britain severed all but one of Germany's undersea telegraph lines. The British tapped the remaining cable, which allowed them to intercept communications (including those with important geopolitical consequences, such as the Zimmerman telegram that helped push the U.S. into the war). The Germans, lacking a fleet of cable ships of their own, attacked British telegraph cable landing sites in the Pacific Ocean. This case illustrates three cable vulnerabilities that still exist today: direct cutting, tapping and targeting landing sites.

States have long recognized that cables are vital to secure communication. In 1959, a Soviet trawler cut five cables off the coast of Newfoundland, prompting the U.S. to send a radar ship to board the trawler under the provisions of the 1884 Submarine Cable Convention. (The 1884 treaty prohibits intentional damage to cables and allows navies to board vessels to investigate reports of damage.) The incident was followed by a diplomatic exchange of notes in which the United States said: "The protection of submarine telecommunications cables on the high seas constitutes an international obligation."

More recently, Bangladeshi authorities determined that an intentional cable outage in 2007 cost Bangladesh's telecommunication company over $1 million. In 2013, Egyptian authorities discovered three scuba divers attempting to cut a cable off the port of Alexandria. The cable industry estimates that over 150 faults in cable connectivity occur every year, but because the vast majority are isolated incidents, network redundancy limits their effects. It is far more problematic to lose *all* cables in a specific area: An 2006 earthquake off the coast of Taiwan struck a concentration of cables in the nearby ocean and disrupted internet traffic across Asia, causing months of slow connectivity.

Recognizing the grave possible consequences, the United States takes threats to cables seriously. In 2015, Russian ships and submarines near cable routes around the world caused concern within the U.S. intelligence community that Russia was attempting to tap or cut critical internet communications lines. A Cold War-style drama played out between the Russian subs following cable lines and the American ships, subs and spy satellites tracking them. These incidents highlighted the danger of cutting cables in deep water, where repairing them could take weeks or months.

Network Attack

Today, in addition to physical threats, submarine cable systems face significant virtual vulnerabilities. The consortiums of companies that operate submarine cables (which are worth hundreds of millions of dollars) use network-management software to control the wavelengths that transmit gigabits of data at high speed along the ocean floor. These systems allow operators to monitor data traffic, see cable faults, and add or drop wavelengths transmitting data (resembling other Supervisory Control and Data Acquisition (SCADA) systems). They enable remote control of entire cables and are vulnerable to a wide array of attacks because they use common operating systems like Linux and Windows.

Furthermore, network management systems often are connected to remote operating centers through networked connections and even linked to the internet. Michael Sechrist wrote about the systems' risks:

> What is the nightmare scenario? A hacker penetrates a cable management system, gains administrative rights, and hacks into the presentation server … Hackers could then attain unprecedented top-level views of multiple cable networks and data flows, discover physical cable vulnerabilities, and disrupt and divert data traffic. With that access, hackers/attackers can gain a potential "kill click" – with a click of a mouse they can delete wavelengths and, potentially, significantly disrupt or alter global Internet traffic routes.

Many network management systems are not up-to-date, including older Siemens systems. The Stuxnet worm hit Siemens SCADA systems worldwide and ultimately targeted Iran's nuclear centrifuges—highlighting how malware can attack critical infrastructure vulnerabilities. One Stuxnet lesson of relevance to undersea cables is how the virus masked its presence by feeding false information to monitoring centers. If a piece of malware similarly hides its effects on cable traffic, the time it would take to identify the faults with the system could prolong global disruptions.

International Law on Damage to Submarine Cables

Understanding the international laws governing cables is essential to protecting them.

First, international law differentiates between attacks on cables and espionage. Spying operations on cables consist of passively tapping the information coming through the pipes at landing sites. (For more on the jurisdictional issues involving the legality of cable tapping, see section 4 of Tara Davenport's article on the subject.)

The earliest international law agreement on the topic is the Convention on the Protection of Submarine Cables, signed in Paris in 1884. The treaty applies to all cables outside the territorial waters of states and requires all states to incorporate its protections into their domestic law. (The relevant U.S. provision is 47 U.S.C. § 21-39.) Article 2 mandates that "the breaking or injury of a submarine cables, done willfully or through culpable negligence...shall be a punishable offense." In Article 12, the parties agree to implement national legislation to impose the penalties for violating the treaty. Notably, Article 15 says its provisions "shall in no wise [sic] affect the liberty of action of belligerents." Thus, in wartime, the protections do not apply.

Maritime law is also important to undersea cable governance. The 1958 Geneva Conference on the Law of the Sea addressed submarine cables in two treaties, the Convention on the High Seas and the Convention on the Continental Shelf. The High Seas Convention included the submarine cable protections of the 1884 Convention but in the context of the "freedom to lay submarine cables," a fundamental freedoms of the high seas "recognized by the general principles of international law." Article 27 addresses damage to cables, but it does not explicitly prohibit the intentional damage to them. Instead, it mandates that states party to the treaty "take the necessary legislative measures" to make breaking a cable a "punishable offense."

The 1982 U.N. Convention on the Law of the Sea (UNCLOS) superseded the 1958 Geneva Conventions. This landmark agreement addressed submarine cables in multiple chapters. Articles 113-115 replicate the language from the 1958 convention requiring states to enact domestic legislation penalizing damage to cables by ships or persons subject to their jurisdiction. UNCLOS establishes exclusive economic zones (EEZs), waters 200 nautical miles beyond states' territorial waters in which they enjoyed sovereign rights to undertake economic activities. Among those activities, UNCLOS recognizes the freedom of all states to lay cables within the EEZ and extended its protections to cables within the EEZ. In Article 79, UNCLOS recognizes the freedom of all states to lay cables on the continental shelf.

The United States has not ratified UNCLOS. However, President Reagan's 1983 United States Ocean Policy Statement said the U.S. will follow the provisions of UNCLOS relating to "balance of interests relating to the traditional uses of the oceans." As James Kraska discussed on *Lawfare* in January, the U.S. follows UNCLOS so long as other states respect U.S. claims. Numerous scholars have debated whether the submarine cable convention have become part of customary international law (See, for example, Eric Wagner and Tara Davenport's contributions on the subject).

International Law on Cyber Attacks

No existing treaty addresses cyber warfare operations. The U.N.'s Governmental Group of Experts (GGE) concluded in its 2013 report that international law—and specifically the U.N. Charter—is applicable to cyberspace. While the GGE has since stalled, other groups of influential experts have weighed in on the legality of operations in cyberspace.

The highly-influential Tallinn Manual addresses the issue of submarine cables. It extends international law protections that apply to submarine cable to submarine communications cables. In its analysis following Rule 54, the manual says states enjoy sovereignty over submarine cables in their territorial sea: "[T]hey generally are treated in the same fashion as cyber infrastructure located on land territory." The manual concludes that customary international law prohibits intentional damage to cables, reasoning that since states have a right to lay cables, it would be "incongruent" to not require states to respect that right.

However, the manual also caveats its decision, saying it is "without prejudice to the rules applicable during armed conflict." Michael Schmitt, the Tallinn Manual project lead, additionally wrote in 2017 that a submarine communications cable carrying both military and civilian traffic would be a legitimate target under the law of armed conflict.

Scholars have discussed how this aspect of international law could allow attacks on civilian cyber infrastructure, including underseas cables. Rule 39 of the Tallinn Manual's first edition (rule 101 in Tallinn 2.0) says that objects used for military and civilian purposes (a category which includes cyber infrastructure) are legitimate military objectives. Another group of scholars led by Oona Hathaway recommended an international treaty to limit attacks on civilian infrastructure. Earlier this year, Microsoft's CEO, Brad Smith, called for the creation of such a treaty—a "Digital Geneva Convention."

In this debate, states, corporations and scholars would be wise to consider submarine cables. While existing treaties do offer some legal protections for cables, a camp of international lawyers contends that cables become legitimate objects of attack in war time. In practice, the lack of legal disputes involving attacks on cables leaves their legality uncertain.

Topics:

- Cybersecurity,
- International Law

Garrett Hinck is a research intern at the Brookings Institution. A senior at Georgetown University's School of Foreign Service, he is particularly interested in cyber security and Internet law. He has held previous internships at the policy team of an internet domain company and at the National Consortium for the Study of Terrorism and Responses to Terrorism (START).

- **@garretthinck**

Published by the Lawfare Institute in Cooperation With
BROOKINGS

Related Articles

- ### Document: Vulnerabilities Equities Process Charter

  Vanessa Sauter Wed, Nov 15, 2017, 10:48 AM

- ### The Lawfare Podcast: Susan Landau is Listening in on You

  Vanessa Sauter Tue, Nov 7, 2017, 5:10 PM

- ### ABA Cybersecurity for Lawyers Handbook

  Paul Rosenzweig Tue, Nov 7, 2017, 6:07 AM

- ### New ‘Hack Back’ Legislation Makes Improvements and Raises New Questions

  David Forscey Fri, Nov 3, 2017, 11:00 AM

- ### Melissa Hathaway on The Future of Cybersecurity

  Paul Rosenzweig Sun, Oct 29, 2017, 12:47 PM