The Law of Maritime Neutrality and Submarine Cables

ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/

By James Kraska

July 29, 2020

In an era of great power competition in which states seek to avoid "taking sides," the international law of neutrality deserves greater attention. Information technology is the contemporary currency of power and the global network of over 420 submarine cables spanning some 700,000 miles is the information superhighway used for sharing 97 percent of international communications. During armed conflict, belligerents could degrade, damage, or sever submarine cables, or use them to launch cyberattacks against their enemy. These activities invariably will affect the economic and military communications of neutral states. To what extent may belligerent states damage, destroy, or use submarine cables owned or operated by neutral states to prosecute the war effort? This question lies at the intersection of three areas of law: the peacetime law of the sea, the law governing submarine cables, and the law of naval warfare, including the law of maritime neutrality. There are few restrictions on using or destroying neutral submarine cables in the law of naval warfare, which is *lex specialis*, and prevails as against the other two bodies of law during armed conflict. Belligerents may lawfully use the entire global network of submarine cables as a domain of virtual warfare without any material restraint from the law of neutrality. We may expect that belligerents will use, and even intentionally damage or cut neutral submarine cables.

This article first explores the peacetime law governing submarine cables. All states have the right to lay submarine cables on the high seas, as well as in the exclusive economic zone (EEZ) and continental shelves of coastal states. Next, the article focuses on the traditional maritime law of neutrality. This body of law applies during armed conflict and protects the rights of neutral states not party to the conflict, including the inviolability of submarine cables in their waters from physical attack by belligerents. This right, however, neither protects neutral cables lying outside neutral territorial waters from destruction by belligerents, nor prevents belligerents from using neutral cable infrastructure for cyberattacks against another belligerent. The automatic routing of cable traffic in today's global submarine cable systems means that belligerents are unable to avoid neutral cables. At the same time, neutral states are absolved of their traditional obligation under the law of neutrality to ensure that their cables are not (mis)used by a belligerent. This article concludes that the technology of the global cable system, and customary law reflected in state practice, suggest that belligerent states would use or even destroy neutral submarine cables during armed conflict.

Law Governing Submarine Cables

Submarine cables wind through the seabed of the oceans and connect to landing stations on the beach. In peacetime, this infrastructure is protected from accidental or purposeful damage or destruction by the 1884 Convention for the Protection of Submarine Cables. The treaty states in article 15, however, that it does not limit belligerent rights during armed conflict. The operation of submarine cables in peacetime is also regulated by the 1982 United Nations Convention on the Law of the Sea (UNCLOS). States may lay cables in the EEZ and on the continental shelves of coastal states in accordance with articles 58(1) and 79, subject to the duty to exercise "due regard" for the resource rights of the host coastal states, as set forth in article 56. In these areas coastal states may adopt "reasonable measures" concerning foreign cables to protect its right to develop seabed mineral resources or to protect the marine environment, under article 79(2). States also may lay cables on the deep seabed beyond national jurisdiction under articles 87(1)(c) and 112. During armed conflict, however, the *lex specialis* regime of the law of naval warfare suspends UNCLOS among the belligerents and it modifies the relationship between belligerent states and neutral states.

The Law of Maritime Neutrality

Neutral states are those that have elected not to take part in an armed conflict and instead seek to maintain friendly, impartial relations with all states. The law of neutrality regulates the relationship between states that are party to a conflict and those that are not engaged in armed conflict. Neutral states strive to balance two conflicting interests: the right of belligerents to prosecute the war effort by isolating the enemy and destroying opposing armed forces, and the right of neutral states to be free from the adverse effects of armed conflicts to which they are not a party. As President Thomas Jefferson decreed in 1793 as French warships sought refuge in American ports during the war between revolutionary France and the first coalition, "the law of nations and the rules of neutrality forbid" taking sides.

The law of neutrality largely has focused on the right of neutral states on the high seas to engage in trade with one another, and separately, with belligerent states (except for contraband), as set out in the British Declaration on Neutrals and Letters of Marque of 28 March 1854 and the 1856 Paris Declaration Respecting Maritime Law. These provisions were further codified in article 6 of the U.S.-U.K. 1871 Washington Treaty. Neutral states have the right to engage in commerce, protected from the worst effects of armed conflict to which they are not a party.

Neutral territory is inviolable by belligerents under article 1 of the 1907 Hague Convention V. At sea, neutral space extends to the waters under the sovereignty of coastal states, including ports, internal waters, and the territorial sea of a state in accordance with articles 2 and 5 of Hague Convention XIII. Similarly, article 3 of the 1928 Convention on Maritime Neutrality requires that belligerents shall "refrain from acts of war" in neutral waters. This rule extends logically to archipelagic waters under Part IV of UNCLOS, as recognised in Part II, rules 23 to 30, of the San Remo Manual on

International Law Applicable to Armed Conflict at Sea and para. 1.1 of the Helsinki Principles on the Law of Maritime Neutrality. Belligerent warships and auxiliaries may enter neutral territorial seas for mere transit but may not conduct operations in excess of simple innocent passage, archipelagic sea lanes passage, or transit passage through straits, as appropriate.

Belligerent states are forbidden from using neutral waters as a base of naval operations against the enemy. This proscription includes using neutral waters to refuel, resupply, repair, or rearm warships (beyond what is minimally required to get underway) in accordance with article 6 of Hague XIII, and belligerent warships may not remain in neutral waters longer than twenty-four hours under article 12, as well as article 5 of the 1928 Inter-American Convention on Maritime Neutrality.

Article 5 of Hague XIII prohibits belligerents from erecting on neutral territory "wireless telegraphy stations or any apparatus" used in military communications with "belligerent forces on land or sea." This rule is amplified in article 4 of the Inter-American Convention: belligerents may not install in neutral waters "radio-telegraph stations or any other apparatus" to communicate with military forces, or to "make use" of such installations established before the war and "which have not been opened to the public." These rules on the neutral inviolability of the physical domain of waters under coastal state sovereignty also apply to submarine cables physically present in those areas. The law of neutrality has always been complex – even unsettled – and submarine cables makes analysis even more challenging.

"Necessities of War"

Submarine cables that lie on the continental shelf in the internal waters, archipelagic waters, or territorial sea of a coastal state are under the sovereignty of the coastal state and are physically inviolable during armed conflict. During the Spanish-American war, the United States set the precedent for the belligerent right to cut neutral cables serving the enemy that lie outside neutral waters. On 1 May 1898, Commodore Dewey entered Manila Bay and destroyed or captured the Spanish fleet. The following day, he cut the Manila-Hong Kong cable owned by a British company and laid down under Spanish concession. Afterward, First Lord of the Treasury Balfour remarked in parliament that article 15 of the 1884 Treaty recognised the right of belligerents to cut cables used by the enemy. The United States also severed cables in Cuba and Puerto Rico, which were also owned by a British company.

In 1902, a table-top exercise published in volume 2 of International Law Studies at the U.S. Naval War College concluded that belligerent states acting on the high seas could interrupt or cut submarine cables between belligerents and neutrals "if the necessities of war require," although cables connecting neutral states only were inviolable. Similarly, in article 54 of the 1907 Hague IV Regulations, cables connecting an occupied territory with a neutral territory are protected from seizure or damage "except in the case of absolute necessity." The exception seems to swallow the rule. The U.S. actions during the Spanish-American war resulted in a U.S.-U.K. arbitration tribunal in 1923, the

"Eastern Extension Case," that considered compensation for British companies that owned the cables. The tribunal denied compensation, ruling that cutting the cables was consistent with the law of naval warfare and "fully justified." After World War II, in commenting on attacks against submarine cables during time of war, C. John Colombos declared in § 471 of his 1951 classic treatise, "there do not appear to be any [rules] which are clearly discernible." The more complicated operation and administration of submarine cables in the cyber era magnifies uncertainty in applying the neutrality law.

Not everyone would agree today with the holding in the Eastern Extension Case, which permitted a belligerent to cut a cable outside neutral territory. Rule 150 of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, for example, asserts that the exercise of belligerent rights by cyber means "directed against" neutral submarine infrastructure, such as submarine cables, is prohibited. This proscription applies to cables inside the territorial waters of the coastal state, as well as those owned by companies of the neutral state that span the globe. Furthermore rule 151 of the Tallinn Manual 2.0 states that "the exercise of belligerent rights by cyber means" are prohibited in neutral territory. This approach incorrectly analogises cyber data as akin to physically transporting munitions or supplies of war through a neutral power, which is a violation of article 2 of Hague V.

Information packets, however, like radio or sound waves, merely propagate energy and therefore cannot not be analogised to physically violating neutral territory. The law of neutrality was developed based on actions in the physical domain – the sanctity of neutral waters, for example. Submarine cables, while consisting of a physical infrastructure, serve as a medium of transmission and operate much like the airspace, within which radio waves propagate at will. Travel by ship through neutral waters implicates the law of neutrality, so too does flight in national airspace. But broadcasting radio waves through neutral national airspace does not by itself affect state sovereignty in the same way, since it is not a tangible physical activity. Likewise, submarine cables located in neutral states are themselves physically inviolable, but their usage as information conduits are not protected during armed conflict. Under this view, belligerents may utilise submarine cables as part of their cyberattack against an enemy. Indeed, the nature of submarine cables today means there is no alternative to this view because submarine cables are no longer bi-polar, in which data serves only the two states physically connected. Implementation of the Tallinn Manual 2.0 rules appears to presume a level of control required by belligerents to avoid cables lying in neutral waters or neutral cables on the deep seabed that almost certainly is unrealistic.

The Russian government's apparent loss of control over Notpetya, the most devastating cyberattack in history, is a case in point. It suggests that it is difficult to create a discriminate cyber weapon. Once unleashed, it appears that because of the nature of the submarine cable network that it will be impossible to keep a cyber weapon out of neutral territory or off neutral cables. The reasons why relate to the way submarine

cables operate today. One hundred years ago submarine cables were bipolar, connecting country X to country Y. It was simple to conduct an analysis of whether a neutral state was affected by cutting a cable.

The Global Submarine Cable System

Today, however, submarine cables generally are owned and operated by multinational consortia consisting of from four to as many as forty stakeholders, each with a percentage ownership stake in the cable. Google, for example, has partial stakes in more than a dozen submarine cables. These ownership consortia are responsible for construction and maintenance of the cable based on a divided percent of the capacity. The entities that own the cables typically are based in tax havens, such as Bermuda, even if the actual ownership is by a company in the United States or Germany. There is no global registry of ownership for submarine cables, so it is difficult, perhaps impossible, to identify the actual owners. The cable obtains a landing license in each state that it physically touches, and the landing state likely would obtain information on all the owners. But, here it gets even more complicated because the owners often sublease part or all their stake to another company located in another state, and this subdivision, called an indefeasible right of use, is usually not reported subsequently to landing states. Thus, states with an interest in the cable would not be known to either landing states or belligerent states that propose to use the cable during hostilities.

To make matters even more complex, it is likely impossible for a belligerent state targeting a submarine cable to be certain of the impact on any neutral state, or neutral states generally, because submarine cable traffic is automatically re-routed in a fraction of a second in the event of a cable casualty or disruption. This split-second re-routing is negotiated in advance under mutual restoration agreements with multiple cable operators. All neutral states connected to the cable network must be factored into the belligerent state's targeting analysis.

Ninety-eight percent of cables are commercial, non-government lines. Military information packets sent by a belligerent state are indistinguishable from ordinary Internet traffic and the specific pathways of information through submarine cables is unpredictable and uncontrollable. Attempts to establish a legal rule that precludes every belligerent use of neutral commercial submarine cables would be nugatory. While the 1902 Naval War College study and the Eastern Extension Case concluded that belligerents could damage or cut neutral submarine cables "if the necessities of war require," the Tallinn Manual is more restrictive, stating that such attacks are prohibited if the belligerent has knowledge such action would generate foreseeable spillover effects on the neutral state. The 1923 arbitration sets the standard. Belligerents acting pursuant to military necessity may entirely disrupt or even cut the cable despite its effect on neutral states. Between the more restrictive Tallinn Manual 2.0 commentary and the permissive 1923 arbitration, the arbitration is the more realistic and compelling standard. In the exigencies of war, belligerents will utilise cables and conduct cyberattacks through them, particularly when the law is less than certain. The 1923 arbitration and the practicalities driven by cable operations today suggest that

belligerents may resort to using – or even cutting – submarine cables as a method of naval warfare. In effect, the virtual cyberspace within submarine cables, like the airwaves, constitutes a global electromagnetic domain that is open to belligerents. Neither the black letter law nor the actual technology supports more aspirational protections of neutral states. What about the ability of neutral states to fulfil their obligations of impartiality?

Duties of Neutral States on the Use of their Cables

The rights of neutral states concerning submarine cables have been diminished in law, aided by the impracticality of discerning among users and cables and the ubiquity of the global Internet. At the same time, these factors also have absolved neutral states of their traditional duties of neutrality in armed conflict when it comes to submarine cables.

Rule 152 of the Tallinn Manual 2.0 suggests that neutral states have a due diligence requirement to ensure their submarine cables are not utilised for belligerent purposes. Yet the amorphous nature of the electromagnetic data traveling through submarine cables, while exposing neutral states to belligerent activity, also mitigates their duty to ensure belligerents do not use their cables. Neutral states have an obligation to ensure that belligerents do not use their territory or waters under their sovereignty to prosecute the war effort. The British Wireless Telegraphy (Foreign Ships) Regulations of 1908, for example, authorised the postmaster general and the Admiralty to "control transmissions of messages by wireless telegraphy" by foreign ships in the territorial waters. The United States had the same policy, which rankled the Germany and Austria during World War I, since there was no restriction on submarine cable messages. The U.S. rationale to distinguish censoring radio transmissions in the territorial sea, but not submarine cable messages, was that radio waves broadcast in the open cannot be interrupted and may be received and utilised by anyone – including belligerent warships on the high seas, making the neutral territory or territorial sea from where they were broadcast a base of naval operations, an unneutral act. At that time, submarine cables in a neutral state, on the other hand, could not be used as a means of direct communication with belligerent warships on the high seas. Furthermore, undersea cables may be cut by belligerents, as the German cruiser SMS *Nürnberg* did in its 1914 attack on the cable relay station at Fanning Island in the central Pacific Ocean.

Article 8 of Hague V states that neutral powers need not "forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals." Utilising submarine cables, like telephone and wireless transmissions, do not involve physical entry into the neutral state. That provision indicates that neutral states are not under an obligation to ferret out and stop the (mis)use of their submarine cables by belligerent states, and by not doing so, they do not jeopardise their neutral status. Regardless of either approach, however, if a neutral state restricts or prohibits belligerents from using its submarine cables it must do so in a manner that is impartial to all parties to a conflict.

Belligerents Likely will Use Neutral Cables

In conclusion, the traditional law of neutrality uneasily covers the case of submarine cables. While it is clear that belligerent states are not permitted *in situ* to use submarine cables located in the territory or territorial sea, straits, or archipelagic waters of a coastal state, this infrastructure may be used virtually, despite the electromagnetic data traversing neutral cables on the high seas, or indeed in the territory of the neutral coastal state. This rule, consistent with the 1923 US-UK arbitration, is more permissive than the majority view of the Tallinn Manual 2.0 commentary. It is also more realistic since states engaged in armed conflict may determine they have a compelling military need to use (or to cut) submarine cables. These legal findings have great implications for neutral states and submarine cables during armed conflict. Not only may neutral states have very little or no expectation that belligerents will refrain from using their submarine cables, it is also largely impractical to expect neutral states to attempt to prevent such use.