Intentional Damage to Submarine Cable Systems by States

Tara Davenport

1. INTRODUCTION

Over the past 170 years, submarine fiber optic cables ("submarine cables") have emerged as one of the most important uses of the oceans. In 2021, 99 percent of the world's telecommunications were transmitted through submarine cables.[1] Approximately 464 submarine cable systems transmit dozens of terabytes of data per second, traversing different jurisdictions until they reach a cable landing station onshore.[2] These submarine cables facilitate a wide variety of services, from phone and internet banking to email and social media, to all manner of cloud services, and more. The United Nations General Assembly lauded them as "critical communications infrastructure" and "vitally important to the global economy and the national security of all States."[3] Submarine cables can serve a diverse range of functions. For example, militaries depend on them for both defense and warfare purposes;[4] oil and gas industries utilize them for platforms connectivity;[5] and the placement of scientific sensors on such cables facilitates oceanographic data collection.[6]

Our extensive reliance on submarine cables has raised concerns that state actors may damage them with the intention of cutting off the communication capabilities of states in order to achieve strategic, military, or political objectives.[7] Historically, cable cutting has been used to destabilize the enemy in times of armed conflict.[8] There are fears that states will do the same during "grey-zone conflicts,"[9] particularly after the 2022 explosions at the NordStream pipelines, linking Russia and Germany, off the coast of Denmark that occurred against the background of the Russia–Ukraine war.[10]

Although there have not been many publicly documented and verified examples of deliberate state-sponsored damage of cables outside of armed conflict,[11] the potential ramifications may be significant given the multitude of services that submarine cables support.[12] This is particularly acute for states that are not connected by multiple routes and are unable to rely on the rerouting of data to other transoceanic cable paths (or satellites).[13] Even for states that have multiple cable routes, restoration of traffic may be slow if a large number of cables are

damaged in a systematic and coordinated attack.[14] A submarine cable can be deliberately damaged with varying degrees of sophistication. This can involve relatively simple methods such as vessels using cutting devices like anchors or dredging equipment. Or it can involve more costly and elaborate underwater methods involving divers, manned or unmanned submersible boats, crafts, maritime autonomous vehicles (MAVs), or submarines.[15] Prevention of such deliberate damage requires specific intelligence as well as intensive surveillance and monitoring of maritime activities using, for example, drones and surface vessels.[16]

With this context in mind, this paper examines the extent to which the international legal framework governs deliberate damage by states to submarine cables on the seabed by physical means during peacetime.[17] The paper focuses on two different legal regimes: the law of the sea and the law on the use of force. It seeks to ascertain the extent to which these legal regimes establish states' primary obligations to refrain from deliberate damage to submarine cables and the consequences if states do indeed deliberately damage cables.[18] This paper argues that these legal regimes are incomplete when applied to the deliberate physical damage to submarine cables by states in peacetime. Although it is possible to apply innovative or creative interpretations to fill these gaps, it is also necessary to consider whether clearer guidelines or norms (if not law) are needed to enhance the protection of submarine cables.

2. LAW OF THE SEA

2.1 PRIMARY OBLIGATIONS

Under the International Law Commission's (ILC) 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts (ASR), states are responsible for damage arising out of acts or omissions attributable to that state under international law that constitutes a breach of an international obligation (i.e., a wrongful act).[19] The responsible state is then under an obligation to make full reparation for the injury caused to another state (including espoused claims) by the internationally wrongful act.[20] A critical step in establishing the responsibility of states is that they have committed a wrongful act that is a breach of an international obligation, also known as a primary obligation.[21] Primary obligations can be found in the traditional sources of international law, including international conventions and customary international law.[22]

Although there are several law-of-the-sea instruments governing submarine cables, the most up-to-date and comprehensive one is the 1982 United Nations Convention on the Law of the Sea (UNCLOS).[23] UNCLOS regulates state activities in the oceans by establishing maritime zones of functional jurisdiction where coastal states and other states have varying rights and obligations depending on the distance from the coast. UNCLOS governs two aspects of activities related to submarine cables: (1) the laying, repair, and maintenance of submarine cables[24] and (2) the protection of submarine cables.[25] UNCLOS has 169 parties, including the European Union. Whether the provisions on submarine cables in Articles 21, 51, 58, 79, 87, and 112–115 reflect customary international law is not straightforward given that "the identification of customary international law is not always susceptible to exact formulations."[26]

A detailed discussion on this goes beyond the scope of this paper. However, it warrants note that the ILC and the International Court of Justice (I.C.J.) have explicitly or implicitly affirmed that the provisions on submarine cables in the Exclusive Economic Zone (EEZ) (Article 58), on the continental shelf (Part VI, Article 79), and on the high seas (Part VII, Articles 87, 112–115) are customary international law, albeit without any detailed analysis on whether the requirements of customary international law have been made.[27]

The following subsections explore the extent to which UNCLOS sets out primary obligations on states to refrain from intentional damage to submarine cables. The applicability of UNCLOS provisions on the prohibition of the use, or threat of use, of force at sea will be addressed in section 3, together with the examination of the laws on the use of force.

2.1.1 UNCLOS Provisions on the Protection of Submarine Cables in Areas beyond Sovereignty

UNCLOS does not explicitly prohibit states from inflicting deliberate damage to submarine cables. In areas outside of coastal state sovereignty, namely the high seas, the EEZ, and continental shelf, Article 113 of UNCLOS stipulates the following:

> Every State shall 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 willfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence. This provision shall apply also to conduct calculated or likely to result in such breaking or injury. However, it shall not apply to any break or injury caused by persons who acted merely with the legitimate object of saving their lives or their ships, after having taken all necessary precautions to avoid such break or injury.[28]

Article 113 is based on Article II of the 1884 Convention for the Protection of Submarine Telegraph Cables (1884 Convention).[29] The utility of this provision in placing a clear obligation on *states* to refrain from intentionally damaging submarine cables is doubtful. Article 113 only places an obligation on a state to criminalize willful or negligent damage by vessels permitted to fly its flag or persons subject to its jurisdiction—it does not explicitly provide that states must refrain from deliberately damaging cables.[30] Moreover, it does not establish state responsibility if states do deliberately damage cables.[31]

2.1.2 UNCLOS Provisions on the Protection of Submarine Cables in Areas under Sovereignty

In areas under coastal state sovereignty, such as internal waters and the territorial sea, there is no equivalent of Article 113 of UNCLOS obliging states to criminalize willful or negligent damage in the territorial sea.[32] Nonetheless, coastal states *may* adopt laws and regulations to protect submarine cables in the territorial sea pursuant to their sovereignty under UNCLOS, and they *may* also adopt laws and regulations relating to innocent passage of vessels in the territorial sea to protect submarine cables.[33]

UNCLOS does contain some provisions that would apply to the deliberate damage of submarine cables in the territorial sea. The applicability of these provisions centers on the question of whether the *damage itself* or the *methods* that are used to damage cables render the passage of foreign vessels in the territorial sea non-innocent, in the sense of being prejudicial to the peace, good order, or security of the coastal state.[34] If foreign vessels were to deliberately damage cables landing in the coastal state while purportedly exercising the right of innocent passage, this would constitute an act "aimed at interfering with any systems of communication or any other facilities or installations of the coastal state" and would render passage non-innocent.[35] It is not clear whether damage to a submarine cable that is merely transiting the territorial sea without making landfall (transit cables) would be considered a system of communication of the coastal state when it is technically not serving the coastal state.[36]

To the extent a *foreign vessel* utilizes a MAV to damage submarine cables, this could render passage non-innocent as the "launching, landing or taking on board of any military device" renders passage non-innocent.[37] If instead a *submarine*, or a *MAV*, is used to damage cables, it could be argued that the submerged passage of a submarine or MAV renders passage non-innocent as UNCLOS requires submarines and underwater vehicles to navigate on the surface.[38] Accordingly, depending on the circumstances, the deliberate damage of submarine cables in the territorial sea could render passage non-innocent.

2.1.3 UNCLOS Marine Environmental Obligations

Deliberate damage to submarine cables may result in damage to the marine environment. For example, the use of underwater explosives could cause damage to the surrounding biodiversity and resources, although the use of anchors or MAVs to simply cut a cable will most likely not result in significant damage to the marine environment.[39] To the extent that the deliberate damage of submarine cables causes damage to the marine environment, the state conducting such activities will be in breach of UNCLOS provisions requiring them to protect and preserve the marine environment, which applies irrespective of the maritime zone where the activity resulting in damage to the marine environment took place.[40] Such states can potentially be held liable for damage to the marine environment. Although assessing and quantifying damage to the marine environment has challenges, international courts and tribunals have awarded damages for damage to resources and the environment that result from a state's activities.[41]

2.1.4 An Interpretation of UNCLOS as Imposing an Obligation to Refrain from the Deliberate Damage to Submarine Cables?

UNCLOS does not set out any explicit prohibition against the deliberate damage of submarine cables by states, either in areas under their sovereignty or beyond their sovereign territory. That said, it is reasonable to argue that such an obligation exists when interpreting UNCLOS "in good faith with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[42] The preamble of UNCLOS recognizes the desirability of establishing "a legal order for the seas and oceans which will facilitate *international communication*, and . . . promote the peaceful uses of the seas and oceans." The freedom to lay submarine cables in areas beyond sovereignty (that is, in the EEZ, continental

shelf, and high seas) has been recognized as customary international law that was codified in UNCLOS.[43] It should follow that states have a corresponding obligation not to deliberately damage submarine cables in these areas.[44]

Article 113 reflects the importance of submarine cables by placing an obligation on states to criminalize willful or negligent damage by flags or persons under their jurisdiction. Even the rules on innocent passage recognize that any interference with systems of communications of the coastal state renders passage non-innocent. It is also relevant that in times of armed conflict, submarine cables are open to attack by belligerents (recognized in the 1884 Convention), and a reasonable a contrario argument can be made that in times of peace, such attacks are prohibited.[45] The General Assembly has also consistently recognized submarine cables as critical communications infrastructure that is vitally important to the global economy and the national security of all states, and it has called upon states to take measures to protect fiber-optic submarine cables.[46] Given the exponential increase in the reliance on submarine cables since the adoption of UNCLOS in 1982, UNCLOS can and should be interpreted as prohibiting intentional damage by states.

2.1.5 Prohibition of Damage to Submarine Cables under Customary International Law?

It has also been argued that the infliction of damage to cables is prohibited as a matter of customary international law, as doing so "would run contrary to the object and purpose of the law governing submarine cables."[47] The experts that drafted the Tallinn Manual 2.0 based this conclusion on the fact that it would be "incongruent to provide States a right to lay such cables without a corresponding obligation on the part of States to protect them" and "the law of the sea does not provide a legal basis for a State to cut another State's submarine fibre optic cable in order to reduce trans-continental Internet traffic in times of tension."[48]

It is debatable whether the Tallinn Manual 2.0 reflects extant customary international law or is simply the view of experts about how international law *should* be applied.[49] The Tallinn Manual 2.0 did not appear to engage in a systematic analysis of whether the prohibition of damage to cables meets the two elements of customary international law (i.e., a general practice and its acceptance as law by states).[50] Such an analysis goes beyond the scope of this paper. For present purposes, it suffices to note that customary international law is relevant to the interpretation of UNCLOS under Article 293, which allows international courts and tribunals tasked with hearing disputes on UNCLOS to apply UNCLOS and "other rules of international law not incompatible with this Convention." International courts and tribunals have acknowledged that even when UNCLOS does not contain express provisions on a particular matter, that general international law can be relied upon in the interpretation of UNCLOS.[51]

2.2 PREVENTION AND RESPONSES AT SEA TO DELIBERATE DAMAGE TO SUBMARINE CABLES

Unless there is specific intelligence that a state is about to deliberately damage a cable system, such actions are difficult to prevent and would require intensive surveillance and

monitoring of maritime activities with, for example, drones and surface vessels.[52] As noted in the introduction, cable operators alerted to a fault or disruption on a viable system will automatically reroute data to working cable systems, though such a reroute can be challenging in the case of multiple faults (for example, in a systematic coordinated attack).[53] It may not be possible to immediately identify the exact cause of the disruption (natural or man-made, accidental or deliberate) or to identify the perpetrator. Cable operators will typically use vessel tracking information to determine which ships were present in the area when damage occurred, but this information may not be immediately available, and vessels can switch off identification systems to evade detection. If submarines or MAVs are used, cable operators may not be able to detect or determine the identity of the perpetrator.

Even if there was a suspicion of a threat or actual deliberate damage, the law of the sea provides limited avenues for immediate responses such as interdiction of vessels. In the high seas, the 1884 Convention contains an article that allows the warship of one state to board vessels suspected of intentionally breaking a cable to require the master of that vessel to provide documentation showing the ship's nationality and to make a report to the flag state.[54] UNCLOS did not incorporate this provision and indeed provides carefully circumscribed grounds in which vessels can either be boarded or arrested in areas beyond sovereignty, none of which include suspicion of cable damage.[55] UNCLOS arguably preserves the 1884 Convention right of warships to board vessels suspected of intentionally breaking a cable and reporting to the flag state, at least for contracting parties to the 1884 Convention.[56]

In any event, even if there is a right to interdict threatened or suspected submarine cable damage, warships or submarines used to deliberately damage cables enjoy sovereign immunity in the high seas and EEZ, which means that they cannot be boarded or arrested by other warships.[57] It is not clear whether an MAV would be entitled to sovereign immunity, and international law, including law of the sea, is still grappling with their classification, which will ultimately determine the applicable legal regime.[58] For example, MAVs may be considered "warships"[59] if they are remotely controlled from a warship or submarine, although questions have been raised as to whether an MAV operating from shore or far from the parent warship/submarine should be entitled to the same sovereign immunity afforded to warships.[60]

Deliberate damage that occurs in the territorial sea, as explained in section 2.1.2, may render passage non-innocent. If the damage is done by commercial vessels, coastal states have a broad discretion to "take necessary steps to prevent passage which is not innocent," which includes the full range of enforcement jurisdiction.[61] However, if damage to submarine cables is done using warships, submarines, or MAVs in ways that breach coastal state laws and regulations relating to passage, the only avenue open to the coastal state is to "require the warship to leave the territorial sea immediately."[62] This is consistent with the general immunities of warships and government ships operated for non-commercial purposes preserved in UNCLOS, subject to the earlier caveat that the position on whether MAVs are entitled to equivalent sovereign immunity has not been conclusively determined.[63]

2.3 ATTRIBUTION TO THE RESPONSIBLE STATE

Even if states have a primary obligation not to intentionally damage submarine cables, several obstacles remain in holding accountable a state found to be responsible for such actions. As noted above, states are responsible for damage arising out of their wrongful acts. Attribution refers to the "process by which international law establishes whether the conduct of a natural person or other such intermediary can be considered an 'act of state' and thus be capable of giving rise to state responsibility."[64] The commentary in the ASR observes, "[W]hat is crucial is that a given event is sufficiently connected to the conduct (whether an act or omission) which is attributable to the State."[65] This entails both factual attribution (i.e., evidence that the state "caused" the act) and legal attribution (i.e., evidence that it was an act by the state or a state organ, or an entity that the state or its organs exercised effective control over).

Factual attribution may be complicated by several factors. First, and as alluded to in section 2.2, cable faults can occur for a variety of reasons; the most common cause is either accidental damage by shipping or fishing activities or natural hazards like earthquakes. Second, there may be difficulties in identifying the identity of the actual perpetrator—automatic identification systems (AIS) and other vessel tracking data may not be effective, especially if they are turned off, and possibilities for detection are even less if submarines or MAVs are used.[66]

Legal attribution is also complex. To the extent that warships, government ships operated for noncommercial purposes, and submarines are used to damage cables, deliberate damage to cables will be deemed an "act of state," and attribution to the flag state should not be difficult.[67] Indeed, Article 31 of UNCLOS provides that the flag state "bears international responsibility for any loss or damage to the coastal State resulting from the non-compliance by a warship or other government ship operated for non-commercial purposes with the laws and regulations of the coastal State concerning passage through the territorial sea or with the provisions of this Convention and other rules of international law."[68] Whether the actions of an MAV will be attributable to the state will depend, again, on whether it can be classified as a "warship."

If a state uses commercial vessels flagged in its own state or another state to damage submarine cables, attribution to the flag state of the vessel is not automatic. The conduct of non-state actors such as vessel owners or operators is only attributable to states in limited circumstances, even if they are state-owned corporate entities.[69] The conduct of a vessel owner/operator will only be attributed to a state if it is empowered by that state's law to exercise elements of "governmental authority"; or if the vessel owner/operator is in fact acting on the "instructions of, or under the direction or control" of that state in carrying out the conduct; or if the state acknowledges and adopts the conduct in question as its own.[70] Both the "governmental authority" and "instructions, direction or control" tests impose high thresholds in attributing the conduct of non-state actors to states.[71] To establish governmental authority, the internal law of the state must specifically authorize the conduct as involving the exercise of public authority.[72] For instructions, direction, or control, it must be demonstrated that the state had effective or factual control over the action during which the wrongful conduct was

committed.[73] Although flag states are required to exercise jurisdiction and control over vessels in a range of matters under UNCLOS, the owners/operators of vessels are not automatically acting under the direct governmental authority or instructions, direction, or control of the flag state. Something more than mere flag state jurisdiction will have to be shown to attribute the conduct of commercial vessels to states.[74]

2.4 INVOCATION OF RESPONSIBILITY

Assuming that there is a breach of a primary obligation attributable to a state, the next question is which state can invoke the responsibility of the wrongdoing state. Under the ASR, the "injured state" entitled to invoke the responsibility of the wrongdoing state is the "state whose individual right has been denied or impaired by the internationally wrongful act or which has otherwise been particularly affected by that act."[75] Article 42 stipulates that a state is entitled "as an injured state" to invoke the responsibility of another state if the obligation breached is owed to

> (a) that State individually; or
> (b) a group of States including that State, or the international community as a whole, and the breach of the obligation:
>> (i) specially affects that State; or
>> (ii) is of such a character as radically to change the position of all the other States to which the obligation is owed with respect to the further performance of the obligation.[76]

The ASR does not define "injured state" but rather specifies that an injury "includes any damages, whether material or moral, caused by the internationally wrongfully act."[77] Material damage refers to "damage to property or other interests of the State and its nationals which is assessable in financial terms."[78]

States that have suffered "damage to property" or "other interests of the State and its nationals," which are assessable in financial terms, because of damage to submarine cables may potentially qualify as an "injured state." The identification of the injured state is complicated by the fact that submarine cables (unlike vessels) are not registered in any state[79] and that submarine cable systems have complex ownership structures, which primarily consist of private entities and state-owned entities either individually or in combination.[80] In December 2020, it was reported that the majority of cable systems have single owners, whereas approximately 33 percent of such systems are owned by an international consortia of companies with different owners incorporated in different jurisdictions.[81] Although rare, states may also directly own a submarine cable system.[82] With this in mind, there are several categories of states that may suffer "material damage" as a result of damage to submarine cables.

First, the landing state (the state to which the damaged cable system provides telecommunications) has suffered material damage to its "interests" because of the losses suffered as a result of deliberate damage to the submarine cable system, subject to the principle of

remoteness of damage.[83] Second, a state that either owns a cable or is part of a consortium that owns the cable can also be considered an injured state in the event of damage, on the basis that it suffered damage to its property.

Third, the state of nationality of a private entity or a state-owned entity that owns a cable may also be considered an "injured state," although this is not clear-cut. If the submarine cable that was damaged is owned by a private entity or a state-owned entity, or a consortium of companies that includes state-owned entities and private entities, a question arises as to whether the state of nationality of the owner of the damaged cable can exercise its right of diplomatic protection and espouse the claim on behalf of companies incorporated there. Under the rules of diplomatic protection, an injury to a national is an injury to the state itself.[84] A decision to espouse a claim of a national is within the discretion of a state.[85] A state can espouse the claim of a corporation that has been incorporated there. But espousal will not be recognized if the corporation is controlled by nationals of another state or states, if it has no substantial business activities in the state of incorporation, and if the seat of management and financial control of the corporation are both located in another state.[86] These are some of the reasons why states might not (or in some cases cannot) espouse claims of the non-state owner of the damaged cables.

Fourth, a coastal state in whose territorial sea, EEZ, or continental shelf the submarine cable transits without making landfall may be able to (subject to the remoteness of damage principle) claim "injured state" status arising from the ancillary consequences of submarine cable damage (for example, damage to natural resources and the marine environment).

2.5 IMPLEMENTATION AND ENFORCEMENT OF STATE RESPONSIBILITY

The ASR provides that the "responsible State is under an obligation to make full reparation for the injury *caused by* the internationally wrongful act."[87] Full reparation for the injury caused by the internationally wrongful act shall take the form of restitution, compensation, and satisfaction.[88] The obligation to compensate for the damage caused (insofar as the damage is not made good by restitution) would "cover any financially assessable damage including loss of profits insofar as it is established."[89] Although it is open to the injured state and the responsible state to come to an agreement on the appropriate reparation, in the event that the responsible state does not agree, the injured state has several options, including countermeasures and dispute settlement proceedings. Space constraints prohibit in-depth exploration of these options, but a few brief points warrant note.

Countermeasures are unilateral measures that would otherwise be contrary to the international obligations of an injured state vis-à-vis the responsible state if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation.[90] An injured state must satisfy substantive and procedural requirements before it can exercise countermeasures. For example, the countermeasure must be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and of the rights in question."[91] Although it is not possible to foresee what type

of countermeasures would be an appropriate response to states' deliberate damage of submarine cables, forcible countermeasures would not be permitted.[92]

On dispute settlement proceedings, UNCLOS is one of the few international treaties that allows one state party to unilaterally bring another state party over a dispute over the interpretation or application of the treaty to contentious proceedings.[93] An UNCLOS state party that is an "injured state" can utilize UNCLOS Part XV dispute settlement mechanisms to bring a claim against another state party who is responsible for deliberate damage to submarine cables if it can frame the dispute as one "over the interpretation or application of UNCLOS."[94]

As mentioned above, UNCLOS does not explicitly address a state's obligations in relation to the deliberate damage to submarine cables, though one might argue that it can be interpreted in such a way or that the matter is governed by customary international law.[95] UNCLOS tribunals have tended to take a broad view of whether a dispute concerns the interpretation or application of UNCLOS. In cases where there is no express provision in UNCLOS governing conduct that is the subject matter of the dispute, courts and tribunals have used Article 293 on applicable law as a "gateway to establish jurisdiction to hear disputes that did not fall squarely under UNCLOS."[96] In sum, UNCLOS courts and tribunals could have jurisdiction to hear claims about deliberate damage to cables by a state, depending on how such a dispute is framed.

3. INTERNATIONAL LAW ON THE USE OF FORCE

This section explores some of the issues that arise in the application of the international law governing states' resort to the use of force to the deliberate damage to submarine cables by states. It does this by examining (1) whether deliberate damage to submarine cables amounts to an "armed attack" against a state so as to warrant the invocation of the individual right of self-defense under Article 51 of the UN Charter; (2) whether the deliberate damage to submarine cables would warrant collective action under the Security Council's mandate under Article 39 of the UN Charter; and (3) whether deliberate damage to submarine cables runs afoul of the prohibition of the use of force in Article 2 (4) of the UN Charter, which Article 301 of UNCLOS incorporates.

3.1 THE RIGHT OF SELF-DEFENSE UNDER ARTICLE 51 OF THE UN CHARTER

Article 2 (4) of the UN Charter provides that member states of the UN "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." Article 51 of the UN Charter states that nothing "shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member State of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security." To rely on Article 51, the state exercising the right to self-defense bears the burden of proof.[97] It must prove (1) that attacks were of such a nature to qualify as "armed attacks"; (2) that it was a victim of the armed attack; and (3) that such

attacks can be attributed to the attacking state.[98] Even if a state establishes the above, it still must demonstrate that any response pursuant to the exercise of the right of self-defense is necessary and proportional and that the target of its response is a legitimate military target.[99] The following sections explore some of the challenges that a state may encounter in seeking to establish that deliberate damage to cables amounts to an "armed attack" under Article 51 of the UN Charter.

3.1.1 Qualified as an Armed Attack

The jurisprudence of the I.C.J. establishes that (1) whether there is a use of force constituting an armed attack is a question of fact; (2) only the gravest forms of the use of force will constitute an "armed attack"; and (3) the "scale and effects" of the attack will be used to distinguish it from a "mere frontier incident."[100] However, the case law has not indicated a specific threshold that must be reached for the use of force to qualify as an armed attack.[101] In *Nicaragua*, the laying of mines in Nicaraguan internal or territorial waters, and certain attacks on Nicaraguan ports, oil installations, and a naval base, constituted an infringement of the prohibition of the use of force, amounting to an armed attack.[102] In the *Oil Platforms* case, the I.C.J. found that a series of attacks allegedly committed by Iran against either US-flagged vessels, US military vessels, or US-owned vessels (if indeed the acts were attributable to Iran) did *not* amount to the most grave use of force amounting to an armed attack, even taken cumulatively, but left open the possibility that a series of smaller-scale incidents, taken cumulatively, may amount to an armed attack.[103] In the *Armed Activities* case, the I.C.J. held that the unlawful military intervention by Uganda was of such a magnitude and duration to breach the prohibition of the use of force and thus amounted to an "armed attack."[104]

Whether the deliberate damage of cables will meet the scale and effects test to amount to an armed attack is context specific. For example, although the use of mines and explosives to damage cables would be an armed attack, it is unclear whether damage to cables caused by vessels dragging an anchor or by an MAV would be an *armed* attack. Moreover, whether the "effects" of deliberate damage to submarine cables meet the requisite gravity test will depend on whether data can be rerouted and on the connectivity of the state being served by that cable. If an attack results in the cutting off of the internet and associated services for a substantial period of time, it could have significant consequences, particularly in less-developed states with minimal connectivity.[105] By contrast, for highly connected states such as the United States and the United Kingdom, deliberate attacks on submarine cables may have minimal impact and would not necessarily meet the gravity required to constitute an armed attack.[106] It also warrants note that purely economic consequences are not (as yet) relevant in ascertaining the gravity of an attack.[107]

3.1.2 "Victim" of an Armed Attack

Another challenge is establishing that the state invoking its right to self-defense is the victim of an armed attack. The state claiming the right to exercise self-defense must establish that the attacks were aimed specifically and deliberately at that state.[108] This raises complex issues about which state is the victim state of an armed attack—issues slightly different than those highlighted in section 2.4 in relation to the identification of the "injured state," which

focused on material damage. Potential states that could be considered victims of a "armed attack" are (1) the landing state (i.e., states that are served by that submarine cable); (2) the state that owns the submarine cable; (3) the state of nationality of the owner of the submarine cable; and (4) the coastal state in whose maritime zones the submarine cable transits without making landfall.

First, the landing state may be a victim state of an "armed attack." To the extent the damage is inflicted on submarine cables in the internal waters or territorial sea of the landing state, that state could be considered a victim of the armed attack by virtue of its sovereignty over these waters and its sovereign authority over this infrastructure.[109] If a segment of a submarine cable is deliberately damaged in the EEZ or continental shelf of the landing state or another state, or in the high seas, the landing state may still be able to argue that it is a victim of an armed attack if its communications were seriously disrupted and it meets the scale and effects test discussed in section 3.1.1.

Second, it is not clear whether a state that has direct ownership of a submarine cable system would be considered a victim of an "armed attack" regardless of where that submarine cable system is deliberately damaged. In the *Oil Platforms* case, the I.C.J. found that an attack against a vessel that was owned by a US company but flagged in Panama "is not in itself to be equated with an attack on that State," acknowledging the possibility that attacking a US-*flagged* commercial vessel could be considered an armed attack if that vessel was intentionally attacked.[110] Analogously, a state that has direct ownership of a submarine cable system that was attacked would not be considered a "victim" by the mere fact of ownership.

Third, and based on the reasoning of the I.C.J. in the *Oil Platforms* case, the state of nationality of either the state-owned entity or the private entity that owns the cable that was subject to deliberate damage is unlikely to be considered a victim of an armed attack. Azaria and Ulfstein note that in the context of the attacks against NordStream, there was "no State practice that would support the proposition that the State of incorporation of the pipeline company would be a victim of 'an armed attack' of a pipeline in the maritime zone within or outside a State's jurisdiction."[111]

Fourth, difficult questions also arise if the attack is against submarine cables owned or operated by militaries for military purposes and whether the state of the military could claim "victim state" status. Militaries use either purely military cables or civilian cables (dual-use cables) for a variety of military purposes.[112] The I.C.J. in the *Oil Platforms* case did not exclude the possibility that the mining of a single military vessel could amount to an armed attack.[113] On this reasoning, it could be argued that an attack against a cable used for purely military purposes and owned by the military of a state meets the criteria for a victim state of an armed attack. But this argument becomes more strained when considering attacks against submarine cables that transmit both civilian and military data.[114]

Fifth, it is conceivable that the coastal state in whose maritime zones submarine cables transit without making landfall is a victim of an armed attack. To the extent the damage is inflicted on

submarine cables transiting in the territorial sea of a coastal state, that coastal state could be considered a victim of the armed attack by virtue of its sovereignty over its waters.[115] However, if it is inflicted on cables that are merely transiting the EEZ or continental shelf of a state, it is less clear that coastal states would be considered a "victim" state. The coastal state only has sovereign rights over the resources in the EEZ or continental shelf under UNCLOS; the EEZ is not the "territory" of the coastal state, and UNCLOS also does not recognize any security interests in these maritime zones.[116]

3.1.3 Attribution to the Attacking State

The case law on whether states have validly exercised the right to self-defense under Article 51 imposes a demanding standard. In the *Oil Platforms* case and the *Armed Activities* case, both the United States and Uganda failed to establish that the acts could be attributed to Iran and the Democratic Republic of Congo, respectively. As highlighted in section 2.3, the attribution of deliberate attacks against cables to particular states is challenging. Moreover, to the extent commercial vessels are used to inflict damage to submarine cables, such acts will only be attributed to the state if it can be established that the state effectively controlled the operation resulting in damage. It is not sufficient that the state financed, trained, supplied, and equipped the vessel owner/operator to enable it to carry out such damage.[117]

3.2 SECURITY COUNCIL COLLECTIVE RESPONSES

The Security Council is the body tasked with determining whether there is an "existence of any threat to the peace, breach of the peace or act of aggression."[118] The Security Council's approach to the existence of a "threat to the peace, breach of the peace or act of aggression" has been inconsistent and inevitably shaped by power politics that characterize discussions in a body dominated by China, Russia, and the United States.[119] Apart from these nonlegal considerations, the Security Council will, at the very least, have to determine that the situation is of sufficient gravity to justify a finding of a threat to peace and security.[120] In this regard, the analysis in section 3.1 would also be relevant. To briefly recap, it will depend on the specific circumstances of the deliberate damage, including the means used to damage such cables; whether a single cable system was attacked or there was a coordinated attack on several systems; the availability of redundancies; and whether the consequences were sufficiently grave.

3.3 PROHIBITION ON THE USE OF FORCE

As mentioned above, Article 2 (4) of the UN Charter sets out the prohibition on the use of force. Article 301 of UNCLOS provides that "States shall refrain from any threat or use of force against the territorial integrity or political independence of any State, or in any manner inconsistent with principles of international law embodied in the Charter of the United Nations."[121] Whether intentional damage to submarine cables by states violates Article 301 will be assessed on the same principles used to determine whether it breaches the prohibition against the use or threat of the use of force in Article 2 (4) of the UN Charter.[122] As discussed in section 3.1, the gravest uses of force constitute an armed attack and entitle a state to exercise its right of self-defense under Article 51.[123] This section focuses on whether deliberate damage to submarine cables can be considered a use of force *not* amounting to an armed attack,

which is still a breach of international law—albeit one which does not entitle the victim state to exercise the right of self-defense under Article 51.[124]

International law has not always been consistent in determining whether a particular state action constitutes a use of force falling short of an armed attack.[125] Moreover, the judicial case law in this area may not be useful for states in an operational context.[126] The traditional conception construes a use of "force" narrowly to mean armed or military force, which focuses on the means of the use of force.[127] On this view, a state deployment of warships, submarines, or MAVs to place underwater explosives to damage submarine cables would constitute a use of force. However, the use of anchors or dredging equipment to cut cables may not fall within conventional understandings of "armed force."

In the context of ongoing discussions on when cyber operations amount to a use of force, commentators have placed more emphasis on the "effect" of states' actions and have begun to conclude that cyber operations capable of causing significant malfunctions to critical national infrastructure would be considered a use of force.[128] If this interpretation of "use of force" gains traction, it should also apply to physical damage to submarine cables, which is critical infrastructure.

If deliberate damage to submarine cables is considered a use of force not amounting to an armed attack, questions arise as to the consequences of such a characterization. In principle, the rules on state responsibility would come into play, and the analysis highlighted in sections 2.3–2.5 would apply, with similar challenges relating to attribution, invocation of responsibility, implementation, and enforcement. One interesting question that arises is which state is entitled to invoke responsibility for a breach of Article 2 (4) of the UN Charter and Article 301 of UNCLOS. In principle, the "injured state" analysis in section 2.4 will be relevant, although a question might be raised as to whether the rules applicable in determining when a state is a "victim of an armed attack," outlined in section 3.1.2, are more appropriate.

4. CONCLUSION

This paper has shown that although the law of the sea and the law on the use of force apply to the deliberate damage of submarine cables by states, many important questions remain unresolved. Questions that need to be interrogated further include the following:

- Whether there is a primary obligation on states to refrain from deliberate damage to submarine cables either under the law of the sea or under the law on the use of force (or any other law)

- Available responses at sea to deliberate damage of cables

- Attribution issues, especially in terms of evidence collection as well as challenges in attribution when states use commercial vessels to damage submarine cables

- Identification of which state is the "injured state" under the rules of state responsibility and/or the "victim state" of an armed attacked under the law on the use of force—a topic that is challenging due to the complex ownership structures of submarine cables and the transnational nature of their operation

- Whether, and in what circumstances, countermeasures and dispute settlement proceedings can and should be used to resolve these disputes

- Whether deliberate damage to submarine cables will meet the gravity necessary to constitute a use of force under Article 2 (4) of the UN Charter or an armed attack under Article 51 of the Charter.

Clarity on this last question is most urgent given the current geopolitical landscape, particularly because broad interpretations of "armed attack" to include deliberate damage to cables could have significant repercussions on international peace and security.

This paper aimed to explore gaps and questions in specific international legal regimes, without examining in any detail the law as it may or should develop. Others (including this author) have previously suggested the adoption of an international treaty that protects submarine cables from all acts of intentional damage from both state and non-state actors.[129] However, negotiations of international treaties require political will and will also take a substantial amount of time. It is therefore unclear whether this solution will gain traction. The International Law Association's Committee on Submarine Cables and Pipelines may also consider these issues, and the outcome of their efforts may provide some guidance to states, industry, and policymakers alike.[130]

A developing avenue for further research and discussion is the extent to which intentional physical damage to submarine cables should come within the mandate of the United Nations groups that are currently studying this issue from the perspective of responsible behavior in cyberspace. While cyberspace has traditionally been understood as a virtual domain, cyberspace actually has at least three layers: "a physical layer which consists of computers, integrated circuits, cables, communications infrastructure and the like; a second layer which consists of the software logic; and finally, a third layer which consists of data packets and electronics."[131] Cyberspace is a "man-made environment that 'requires a physical architecture' to exist, including fibre-optic cables, copper wires, microwave relay towers, satellite transponders, Internet routers etc."[132]

Ongoing discussions at the United Nations on information and communications technologies (ICT) have developed certain norms that can apply to the physical infrastructure underpinning cyberspace—a point made by Kavanagh in a recent report by the UN Institute for Disarmament Research.[133] The Group of Governmental Experts (GGE) On Advancing Responsible Behavior in Cyberspace has suggested as a norm that "[s]tates should not conduct or knowingly support ICT activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide

services to the public."[134] The GGE also suggested that states "should co-operate . . . to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security"; "should take appropriate measures to protect their critical infrastructure from ICT threats"; and "should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts."[135] The extent to which the Open-ended Working Group on Security of and in the Use of ICTs is a useful forum for further collaboration on this issue warrants further study and discussion because the security of submarine cables involves not only cybersecurity but also maritime and law of the sea issues.

ACKNOWLEDGMENTS

The author would like to thank Professor Jack Goldsmith and Camino Kavanagh for their helpful comments on this paper. The views expressed in this paper and all mistakes are the author's own.

NOTES

1. Douglas Main, *Undersea Cables Transport 99% of International Data*, Newsweek (Apr. 2, 2015), https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072 [https://perma.cc/BD29-47AY]. Submarine cables can also be used to transmit electricity, but submarine power cables are not the focus of this paper.

2. Douglas R. Burnett, *Submarine Cable Security and International Law*, 97 Int'l L. Stud. 1659, 1668 (2021).

3. G.A. Res. 65/37, ¶ 121 (Dec. 7, 2010).

4. Gov't Accountability Off., GAO-04-858, The Global Information Grid and Challenges Facing its Implementation 4–5 (2004) [hereinafter Global Information Grid].

5. Wayne F. Nielsen & Tara Davenport, *Submarine Cables and Offshore Energy in Submarine Cables*, *in* Submarine Cables: Handbook on Law and Policy 351 (Douglas Burnett et al. eds., 2014).

6. Lionel Carter & Alfred H. A. Soons, *Marine Scientific Research Cables*, *in* Submarine Cables: Handbook on Law and Policy 323 (Douglas Burnett et al. eds., 2014).

7. *See, e.g.*, Rishi Sunak, Undersea Cables 23 (2017); Christian Bueger et al., Security Threats to Undersea Communications Cables and Infrastructure–Consequences for the E.U.: In-Depth Analysis for the European Parliament 21–34 (2022); Camino Kavanagh, Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour 20–21 (2023). There is also concern that they will be deliberately damaged by non-state actors such as terrorists, but that is not the focus of this paper.

8. For a history of cable-cutting during armed conflict, see Douglas Guilfoyle, Tamsin Phillipa Paige & Rob McLaughlin, *The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables*, 71 Int'l & Comp. L.Q. 657, 680–82 (2022).

9. Grey zone conflicts have been described as "malicious activity below the threshold of armed conflict." Bueger et al., *supra* note 7, at 31.

10. Edward Stringer, *Putin Knows That Undersea Cables Are the West's Achilles Heel*, Fin. Times (Nov. 5, 2022). States such as Russia, China, North Korea, Iran, and Turkey are said to have the capabilities to sabotage cables as part of grey-zone/hybrid warfare tactics: *See* Franz-Stefan Gady, *Undersea Cables: How Russia Targets the West's Soft Underbelly*, The Diplomat, Oct. 27, 2015; Bueger et al. *supra* note 7, at 30–31. However, also note that "the scenarios underpinning the threat discourse seems to be built not on prior incidents but on overall assessments of the geopolitical landscape," and this could imply that "the threat scenarios could be exaggerated, and a substantial risk of threat inflation and fearmongering." Christian Bueger & Tobias Liebetrau, *Protecting Hidden*

Infrastructure: The Security Politics of the Global Submarine Data Cable Network 42 Contemporary Security Policy 391, 398 (2021).

11. Justin Sherman, Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security 6 (2021). There have been instances where deliberate damage by state-sponsored actors was suspected but these reports have not been verified. *See, e.g.*, Stringer, *supra* note 10. *But see* Severin Carrell, *Shetland Loses Telephone and Internet Services After Subsea Cable Cut*, The Guardian (Oct. 20, 2022) (claiming UK registered trawler was responsible); Lisbeth Kirk, *Mysterious Atlantic Cable Cuts Linked to Russian Fishing Vessels*, EU Observer, Oct. 26, 2022, https://euobserver.com/nordics/156342 [https://perma.cc/R6ZK-7RAF].

12. *See* Guilfoyle et al., *supra* note 8, at 692.

13. Burnett, *supra* note 2, at 1664; Blair Shepard, *Cutting Submarine Cables: The Legality of the Use of Force in Self-Defense*, 31 Duke J. Comp. & Int'l L. 199, 210–14 (2020). The International Cable Protection Committee (ICPC) notes that clustering of cables magnifies risk that a single incident will damage multiple cables and impair connectivity. *See* ICPC, Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables (2022).

14. Burnett, *supra* note 2, at 1664–65; *see also* Guilfoyle et al., *supra* note 8, at 682.

15. Bueger et al., *supra* note 7, at 29. This paper adopts the terminology of "maritime autonomous vehicles" as a catch-all category to describe the various types of maritime vehicles in operation including unmanned vehicles, underwater autonomous vehicles, unmanned surface vehicles, and remotely operated vehicles. *See* Natalie Klein, *Maritime Autonomous Vehicles within the International Law Framework to Enhance Maritime Security*, 95 Int'l L. Stud. 244, 248–50 (2019).

16. Bueger et al., *supra* note 7, at 31; Jonathan E. Hillman, CSIS Reconnecting Asia Project, Securing the Subsea Network: A Primer for Policymakers 10–11 (2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ [https://perma.cc/U7VH-MP8U].

17. The paper does not focus on cable damage during armed conflict. For a comprehensive discussion on the applicability of the laws of armed conflict to damage to submarine cables, see Guilfoyle et al., *supra* note 8.

18. Other international legal regimes may apply, but law of the sea and the law on the use of force are the most immediately applicable and therefore serve as a good starting point.

19. Int'l L. Comm'n Rep. on the Work of Its Sixty-Fourth Session, U.N. Doc. A/56/10, at 26 (2001).

20. *Id*. at 92.

21. *Id*. at 91–95.

22. *See* Statute of the International Court of Justice (I.C.J.) art. 38.

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

24. *See* UNCLOS, *supra* note 23, at arts. 51, 58, 79, 87, and 112.

25. *See* UNCLOS, *supra* note 23, at arts. 21, 113, 114, and 115.

26. Int'l L. Comm'n, Draft Conclusions on identification of customary international law, with commentaries, Rep. on the Work of Its Seventieth Session, U.N. Doc. A/73/10, at 123 (2018). Determining the existence and content of customary international law is not a straightforward exercise, and the way that international courts and tribunals have done so has been critiqued. *See generally* The Theory, Practice and Interpretation of Customary International Law (Panos Merkouris et al. eds., 2022).

27. Articles 113–115 in Part VI (high seas) of UNCLOS, which address the breaking or injury of a submarine cables, are based on three provisions in the 1884 Convention on the Protection of Submarine Telegraph Cables. *See* Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989 [hereinafter 1884 Convention]. These three provisions were included in the ILC's 1956 Draft Articles on the Law of the Sea, incorporated in the provisions of the 1958 Geneva Convention on the High Seas because they were considered by the ILC as essential principles

of international law. *See Summary Records of the Seventh Session*, [1955] 1 Y.B. Int'l L. Comm'n 20–21, U.N. Doc. A/CN.4/Ser.A/1955. The preamble to the 1958 High Seas Convention notes that the provisions (including the predecessors to arts. 113–115) are generally declaratory of established principles of international law, and this has been affirmed by the I.C.J. *See* N. Sea Continental Shelf (Ger. v. Den.), Judgment, 1969 I.C.J. 3, ¶ 65 (Feb. 20). Similarly, the right to lay cables in the high seas (under UNCLOS's art. 87) and continental shelf (under UNCLOS's art. 79) was based on Article 2 of the 1958 High Seas Convention, which was said to be declaratory of established principles of international law by the I.C.J. *Id.*; *see also* Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicar. v. Col.), Judgment, 2022 I.C.J. 266, ¶ 57 (Apr. 21). The US Commander's handbook on the law of naval operations notes that "although the United States is not a party to UNCLOS, it considers the provisions concerning traditional uses of the ocean, such as freedom of navigation and overflight, as generally reflective of customary international law binding on all States," and this includes the freedom to lay submarine cables in the high seas, continental shelf, and EEZ: *See* Dep't of the Navy, The Commander's Handbook on the Law of Naval Operations ¶¶ 1.2, 1.62, 1.7, 2.63 (2022).

28. Article 113 of UNCLOS applies in the EEZ by virtue of Article 58(2) of the same. *See* UNCLOS, *supra* note 23, at art. 58(2).

29. 1884 Convention, *supra* note 27, at art. II.

30. Notably, during the negotiations of the 1884 Convention, the United States had proposed that crimes against cables should be equated to crimes of piracy and that all states should have universal jurisdiction to arrest and prosecute perpetrators. This was rejected by most states, and a more limited form of jurisdiction was established (flag state and state of nationality of the offender). *See* Minutes of the International Conference Gathered in Paris from Oct. 16 to Nov. 2, 1882, and from Oct. 16 to Oct. 26, 1883, to Solve the Issue of Submarine Cables, *in* 11 Deuxième Série du Nouveau Recueil Général de Traités et Autres Actes Relatifs aux Rapports de Droit International [Second Series of the New General Collection of Treaties and Other Acts Relating to Relations of International Law] 104, 122. Article VIII of the 1884 Convention provides that (i) the tribunals that are competent to take cognizance of violations of the 1884 Convention are those of the flag state of the vessel that committed the offence, and (ii) if the courts of the flag state do not take any action, parties "so far as the subjects and citizens of those States respectively are concerned" are to exercise jurisdiction in accordance with the "general rules of criminal jurisdiction" when the state of registration of the offending vessel cannot prosecute the offence. 1884 Convention, *supra* note 27, at art. VIII.

31. Guilfoyle et al., *supra* note 8, at 666.

32. See Part II of UNCLOS for the provisions on internal waters and territorial sea. Although archipelagic waters are also areas under sovereignty, this paper does not discuss submarine cables in archipelagic waters due to space constraints. *See* UNCLOS, *supra* note 23, at Part II.

33. *See* UNCLOS, *supra* note 23, at arts. 2, 21(c).

34. UNCLOS, *supra* note 23, at art. 19.

35. UNCLOS, *supra* note 23, at art. 19(2)(c).

36. Note that the group of experts for the Tallinn Manual 2.0 has said that states enjoy sovereign authority over cyber infrastructure physically located within its territory (including its territorial sea) regardless of whether that infrastructure belongs to or is operated by government institutions, private companies, or private individuals and includes computer networks and systems supported by that cyber infrastructure, which would include submarine communication cables. However, the Tallinn Manual 2.0 does not specify whether this sovereign authority is confined to submarine cables that land in the relevant state (and hence serve that state) or extends to submarine cables that are transiting the territorial sea. North Atlantic Treaty Organization [NATO] Cooperative Cyber Defense Center of Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 14 (Michael N. Schmitt ed., 2017) [hereinafter Tallinn Manual 2.0].

37. UNCLOS, *supra* note 23, art. 19(2)(f). Although "military device" is not defined in UNCLOS and another term, "underwater vehicles," is used in Article 20 of UNCLOS, it has been suggested that "military device" should be interpreted purposively to include "drones and unmanned submersibles."

Richard Barnes, *Article 19: Meaning of Innocent Passage*, *in* United Nations Convention on the Law of the Sea: A Commentary 187, 194–95 (Alexander Proelss ed., 2017).

38. UNCLOS, *supra* note 23, art. 20. But see contrary arguments that submarines and underwater vehicles traveling submerged does not necessarily render passage non-innocent, *e.g.*, Barnes, *supra* note 37, at 196, 198–99.

39. This is in contrast to the damage of submarine pipelines, which is more likely to result in damage to the marine environment. *See* Danae Azaria & Geir Ulfstein, *Are Sabotage of Submarine Pipelines an "Armed Attack" Triggering a Right to Self-Defence*, EJIL:Talk! (Oct. 18, 2022), https://www.ejiltalk.org/are-sabotage-of-submarine-pipelines-an-armed-attack-triggering-a-right-to-self-defence/ [https://perma.cc/4Z33-2HUF].

40. UNCLOS, *supra* note 23, arts. 192, 194, 235; The S. China Sea Arbitration (Phil. v. China), Award, 2013–19 PCA Case Repository 1, ¶ 927 (Perm. Ct. Arb. 2016).

41. Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.), Judgment, 2018 I.C.J. 15 (Feb. 2); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2022 I.C.J. 13 (Feb. 9) [hereinafter *Armed Activities*].

42. Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, art. 31(1).

43. *See supra* text accompanying note 27.

44. A point acknowledged by the Tallinn Manual 2.0, discussed below. *See* Tallinn Manual 2.0, *supra* note 36, at 256.

45. 1884 Convention, *supra* note 27, at art. XV. The principle that submarine cables are open to attack by belligerent states is being increasingly challenged by experts and scholars on various grounds, highlighting the importance of submarine cables and reinforcing that they should be protected even though damaging them can confer a significant military advantage: Guilfoyle et al., *supra* note 8; Yoram Dinstein & Arne Willy Dahl, Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary 63 (2020).

46. *See, e.g.*, G.A. Res. 77/248, at 1, 32 (Dec. 30, 2022).

47. Tallinn Manual 2.0, *supra* note 36, at 256.

48. *Id*.

49. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 Am. J. Int'l L. 583, 589 (2018).

50. N. Sea Continental Shelf, *supra* note 27, ¶ 77.

51. *See, e.g.*, *M/V SAIGA* (No. 2) (St. Vincent v. Guinea), Case No. 2, Judgment, 2 ITLOS Rep. 10, ¶ 155 (July 1); Guyana v. Suriname 30 R.I.A.A. 6, ¶ 406 (Perm. Ct. Arb. 2007).

52. Bueger et al., *supra* note 7, at 31. Hillman, *supra* note 16, at 10–11. A number of states do conduct surveillance on high-risk or suspicious activities in the vicinity of cables in territorial waters and EEZs as part of their overall maritime domain awareness programs or fishery control activities: Bueger et al., *supra* note 7, at 53.

53. Burnett, *supra* note 2, at 1664–65.

54. 1884 Convention, *supra* note 27, at art. X.

55. UNCLOS, *supra* note 23, at arts. 110, 111.

56. UNCLOS art. 110 states, "except where acts of interference derive from powers conferred by treaty," which would apply to the 1884 Convention. UNCLOS, *supra* note 23, at art. 110. In 1959, the United States invoked Article 10 of the 1884 Convention to board and investigate a Soviet trawler, *Novorossiisk*, for damaging five transatlantic cables, and the US warship inspected the vessel and determined that there was a "strong presumption" that the *Novorrosiisk* violated Article 2 of the 1884 Convention. *See* U.S. Dept. of State, *U.S. and U.S.S.R. Exchange Notes on Damage to Submarine Cables*, 40 Dep't of State Bull. No. 1034, at 555 (Apr. 20, 1959).

57. As reflected in Article X of the 1884 Convention and Article 95 of UNCLOS (applicable to the EEZ by virtue of Article 58 (2) of UNCLOS). For the argument that MAVs fit within the definition of "warships" in Article 29 of UNCLOS, see Klein, *supra* note 15, at 252–53.

58. *Id*. at 252.

59. UNCLOS defines "warships" as a ship belonging to the armed forces of a state bearing the external marks distinguishing such ships of its nationality, under the command of an officer duly commissioned by the government of the state and whose name appears in the appropriate service list or its equivalent, and manned by a crew which is under regular armed forces discipline. UNCLOS, *supra* note 23, at art. 29.

60. Natalie Klein et al., *Maritime Autonomous Vehicles: New Frontiers in the Law of the Sea*, 69 Int'l & Comp. L.Q. 719, 726 (2020). Note that the United States takes the position that underwater unmanned systems and underwater unmanned vehicles are entitled to sovereign immunity as an extension of the sovereign immunity of the vessels from which they are launched or as naval auxiliaries. *See, e.g.*, James Kraska & Raul Pete Pedrozo, *China's Capture of U.S. Underwater Drone Violates Law of the Sea*, Lawfare (Dec. 16, 2016, 7:03 PM), https://www.lawfareblog.com/chinas-capture-us-underwater-drone-violates-law-sea [https://perma.cc/5S7S-63QV].

61. UNCLOS, *supra* note 23, at art. 25.

62. UNCLOS, *supra* note 23, at art. 30.

63. UNCLOS, *supra* note 23, at art. 32.

64. James Crawford, State Responsibility: The General Part 113 (2013).

65. Int'l L. Comm'n Rep. on the Work of Its Sixty-Fourth Session, *supra* note 19, at 35.

66. A case in point are the difficulties in identifying the perpetrators of the attacks against NordStream I and II. *See* Adam Entous, Julian E. Barnes & Adam Goldman, *Clues Emerge in Bid to Solve Pipeline Attack*, N.Y. Times, Mar. 7, 2023, at A1.

67. *See* Richard Barnes, *Article 31: Responsibility of the Flag State for Damage Caused by a Warship or Other Government Ship Operated for Non-Commercial Purposes*, *in* United Nations Convention on the Law of the Sea: A Commentary 248–49 (Alexander Proelss ed., 2017) (citing *Theodor Garcia and M. A. Garza* (Mex. v. U.S.), 4 R.I.A.A. 119, 132 (Mex./U.S. Gen. Cl. Comm'n 1926)).

68. This is said to be an exception to the general immunity of warships as described in Article 32 of UNCLOS. Barnes, *supra* note 67, at 248.

69. The ASR considers state-owned corporations or enterprises as separate from the state, except where the "corporate veil" is a mere device or a vehicle for fraud or evasion. Int'l L. Comm'n Rep. on the Work of Its Sixty-Fourth Session, *supra* note 19, at 47–48.

70. *Id*. at 26.

71. Vladyslav Lanovoy, *The Use of Force by Non-State Actors and the Limits of Attribution of Conduct*, 28 Eur. J. Int'l L. 563, 574 (2017).

72. Int'l L. Comm'n Rep. on the Work of Its Sixty-Fourth Session, *supra* note 19, at 43.

73. *See* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 412 (Feb. 26); *see also* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 190 (June 27).

74. UNCLOS, *supra* note 23, at arts. 92, 94. Flag states have a due diligence obligation to take all necessary measures to prevent harm from occurring, but this is different from attribution of the conduct by private actors to states. It would be possible to hold flag states responsible for the failure to exercise due diligence to prevent vessels flagged under their jurisdiction from being used as a means to damage submarine cables. *See* Guilfoyle et al., *supra* note 8, at 665–70.

75. Int'l L. Comm'n Rep. on the Work of Its Sixty-Fourth Session, *supra* note 19, at 116.

76. *Id*. at 117.

77. *Id*. at 91.

78. *Id*. at 91–92.

79. UNCLOS, *supra* note 23, at arts. 58, 79, 87.

80. Mick Green, *The Submarine Cable Industry: How Does it Work?*, *in* Submarine Cables: Handbook on Law and Policy 41 (Douglas Burnett et al. eds., 2014).

81. Sherman, *supra* note 11, at 6.

82. For example, the Government of Tonga is reported to be one of the owners of the Tonga Cable linking Fiji and Tonga. *See Tonga Cable*, Submarine Cable Map (Sept. 5, 2023), https://www.submarinecablemap.com/submarine-cable/tonga-cable [https://perma.cc/LWK5-59Y3].

83. Int'l L. Comm'n Rep. on the Work of Its Sixty-Fourth Session, *supra* note 19, at 92–93.

84. *Draft Articles on Diplomatic Protection*, [2006] 2 Y.B. Int'l L. Comm'n 26–55, U.N. Doc. A/61/10.

85. That said, the Draft Articles provide that states "should . . . give due consideration to the possibility of exercising diplomatic protection, especially when a significant injury has occurred." *Id*. at 53.

86. *Id*. at 37.

87. Int'l L. Comm'n Rep. on the Work of Its Sixty-Fourth Session, *supra* note 19, at 91.

88. *Id*. at 95.

89. *Id*. at 98.

90. *Id*. at 71–75.

91. *Id*. at 30.

92. *Id*. at 132.

93. Under article 287 of UNCLOS, parties can choose between (i) the International Tribunal for Law of the Sea (ITLOS); (ii) the I.C.J.; (iii) an arbitral tribunal constituted under Annex VII of UNCLOS; and (iv) an arbitral tribunal constituted under Annex VIII for special categories of disputes relating to fisheries, protection, and preservation of the marine environment, marine scientific research, and navigation. Annex VII arbitration is the default procedure if parties have not accepted the same procedure or if parties have not made a declaration. UNCLOS, *supra* note 23, at art. 287(3)–(4).

94. UNCLOS, *supra* note 23, at art. 286.

95. *See supra* section 2.1.

96. Lan Ngoc Nguyen, *Jurisdiction and Applicable Law in the Settlement of Marine Environmental Disputes under UNCLOS*, 9 Korean J. Int'l & Comp. L. 337, 348 (2021).

97. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 51.

98. *Id*.

99. *Id*.

100. *Military and Paramilitary Activities in and Against Nicaragua*, *supra* note 73, ¶¶ 195, 231.

101. Karl Zemanek, *Armed Attack*, *in* Max Planck Encyclopedias of Public International Law, ¶ 8 (2013).

102. *Military and Paramilitary Activities in and Against Nicaragua*, *supra* note 73, ¶ 227.

103. *Oil Platforms*, *supra* note 97, ¶ 64.

104. *Armed Activities*, *supra* note 41, ¶¶ 148–65.

105. Shepard, *supra* note 13, at 211–15; Guilfoyle et al., *supra* note 8, at 659–60. Shepard, for example, notes that large states such as the United Sates may not be as affected; they would still have access to the internet if their cables were cut, as they have plenty of redundancy and their servers are located domestically. Shepard, *supra* note 13, at 213.

106. Shepard, *supra* note 13, at 211–13.

107. This view may shift as states continue to discuss the issue in the context of cyber operations. Azaria & Ulfstein, *supra* note 39; Tallinn Manual 2.0, *supra* note 36, at 342; Claus Kress, *On the*

Principle of Non-Use of Force in Current International Law, JUST SEC. (Sept. 30, 2019), https://www.justsecurity.org/66372/on-the-principle-of-non-use-of-force-in-current-international-law/ [https://perma.cc/6BXB-Q4J9].

108. In this regard, the I.C.J. in the *Oil Platforms* case noted that none of the alleged attacks seemed to have been aimed specifically and deliberately at the United States, which imposes a requirement of an intentional attack on the target state rather than a merely indiscriminate attack. *Oil Platforms*, *supra* note 97, ¶¶ 191–92.

109. *See* Azaria & Ulfstein, *supra* note 39.

110. *Oil Platforms*, *supra* note 97, ¶ 64.

111. Azaria & Ulfstein, *supra* note 39.

112. *See* Ashley Roach, *Military Cables*, *in* SUBMARINE CABLES: HANDBOOK ON LAW AND POLICY 323 (Douglas Burnett et al. eds., 2014); Guilfoyle et al., *supra* note 8, at 690.

113. *Oil Platforms*, supra note 97, ¶ 195.

114. *See also* Azaria & Ulfstein, *supra* note 39.

115. *Id*.

116. *See also* Azaria & Ulfstein, *supra* note 39 (discussing attacks against commercial pipelines found in the EEZ and continental shelf of a coastal state).

117. *Military and Paramilitary Activities in and Against Nicaragua*, *supra* note 73, ¶ 115.

118. U.N. Charter art. 39.

119. For a discussion of this, see Guilfoyle et al., *supra* note 8, at 677.

120. *Id*.

121. UNCLOS, *supra* note 23, at art. 301; *see also id*., at arts. 88, 141.

122. Although Article 301 of UNCLOS incorporates Article 2 (4) of the UN Charter, determining whether there has been an unlawful use of force at sea may not always entail using Article 2 (4) as a benchmark. ITLOS has developed principles on the use of force in maritime interdiction operations that do not fall within the ambit of the general prohibition under Article 2(4) of the UN Charter. *See* Efthymios D. Papastavridis, *The Use of Force at Sea in the 21st Century: Some Reflections on the Proper Legal Framework(s)*, 2 J. TERRITORIAL & MAR. STUDS. 119, 131 (2015).

123. *Military and Paramilitary Activities in and Against Nicaragua*, *supra* note 73, ¶ 191.

124. Some states claim that an unlawful use of force qualifies as an armed attack triggering the right of self-defense without any gravity threshold to distinguish uses of force from armed attacks. *See, e.g*., OFFICE OF THE GEN. COUNS. OF THE DEP'T OF DEF., LAW OF WAR MANUAL ¶ 16.3.3.1 (2023).

125. Kress, *supra* note 107.

126. Zemanek, *supra* note 101, ¶ 7.

127. Killian O'Brien, *Article 301: Peaceful Uses of the Sea*, *in* UNITED NATIONS CONVENTION ON THE LAW OF THE SEA: A COMMENTARY 187, 194–95 (Alexander Proelss ed., 2017).

128. Kress, *supra* note 107; TALLINN MANUAL 2.0, *supra* note 36, at 330–37.

129. *See* Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 CATH. U. J.L. & TECH. 57, 89–92 (2015); Robert Beckman, *Protecting Submarine Cables from Intentional Damage—the Security Gap*, *in* SUBMARINE CABLES: HANDBOOK ON LAW AND POLICY 281 (Douglas Burnett et al. eds., 2014).

130. See the ILA website for more information on the ILA Committee on Submarine Cables and Pipelines, *Submarine Cables and Pipelines under International Law*, ILA (Nov. 17, 2018), https://www.ila-hq.org/en_GB/committees/submarine-cables-and-pipelines-under-international-law [https://perma.cc/K49M-J46F].

131. Nicholas Tsagourias, *The Legal Status of Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 13, 15 (Nicholas Tsagourias & Russell Buchan eds., 2021).

132. Russell Buchan, Cyber Espionage and International Law 4–8 (2019) (citing Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?* 64 Air Force L. Rev. 1, 33 (2009)).

133. Kavanagh, *supra* note 7, 32–33.

134. UN Secretary General, Report of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 13(f), U.N. Doc. A/70/174 (July 22, 2015).

135. *Id*. ¶¶ 13(a), (g), (h).

29 28 27 26 25 24 23 7 6 5 4 3 2 1

The preferred citation for this publication is Tara Davenport, *Intentional Damage to Submarine Cable Systems by States*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2305 (October 26, 2023), available at https://www.lawfaremedia.org/article/intentional-damage-to-submarine-cable-systems-by-states.

ABOUT THE AUTHOR

TARA DAVENPORT

Dr. Tara Davenport is an assistant professor on the Faculty of Law, National University of Singapore, where she coheads the Ocean Law and Policy Team at the Centre for International Law. She is also deputy director of the Asia-Pacific Centre for Environmental Law and co-rapporteur of the International Law Association's Committee on Submarine Cables and Pipelines.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution working group, visit us online at hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION