THE FINAL FRONTIER OF CYBERSPACE: THE SEABED BEYOND NATIONAL JURISDICTION AND THE PROTECTION OF SUBMARINE CABLES

DOUGLAS GUILFOYLE, TAMSIN PHILLIPA PAIGE* AND ROB MCLAUGHLIN

Abstract Cyberspace is now acknowledged not only as the newest domain of warfare, but also as a space vital to economic, educational and cultural development for all States. This thin consensus ignores the fundamental fact that the backbone of cyber infrastructure—submarine telecommunication cables—is not (for the large part) located within sovereign territorial jurisdiction. The radically increased reliance of States upon submarine data cables emphasises their vulnerability to damage by malicious acts, accidents, or natural phenomena. Faced with these problems, legal analysis has tended to identify gaps or deficiencies in the law, and propose the creation of new legal instruments. The contribution of this article is twofold. First, it expands the frame of analysis to include deliberate damage to cables not only in peacetime but under the law of armed conflict. Second, rather than treating the legal framework as inherently deficient, it considers the extent to which existing rules and principles can be progressively developed, interpreted, or creatively applied to close perceived gaps. This article surveys the existing law specific to the protection of submarine cables and assesses how general principles of the law of the sea, State responsibility, the law on the use of force, and the law of armed conflict apply to this problem. It thus considers in turn the applicable ‘law of peace’, the jus ad bellum and the jus in bello.

Keywords: public international law, law of the sea, submarine cables, law of naval warfare, maritime security.

I. INTRODUCTION

Liberal Western States are calling for an Internet which is fundamentally free, open, and secure while authoritarian States prioritise ‘cyber sovereignty’ and an Internet which is free from criminality, secessionism and terrorism.

* Professor, University of New South Wales (Canberra), douglas.guilfoyle@unsw.edu; Senior Lecturer, Deakin Law School, t.paige@deakin.edu.au; Professor, Australian National Centre for Ocean Resources and Security, rmclaugh@uow.edu.au. The authors would like to acknowledge the helpful comments of Fleur Johns, participants in the Australian and New Zealand Society of International Law Oceans and International Environmental Law Interest Group, and the anonymous reviewers, which greatly assisted in the finalisation of this article.

Nevertheless, there is now widespread agreement that existing public international law applies to cyberspace and, in particular, certain principles derived from sovereignty, including the right of States to exercise jurisdiction over those aspects of the material infrastructure underpinning cyberspace which are located within their territory (albeit that the concept of ‘sovereignty’ in cyberspace is still debated in some quarters).

This thin consensus, however, ignores the fundamental fact that the backbone of cyber infrastructure—submarine telecommunication cables—is not (for the large part) located within sovereign territorial jurisdiction. This means that the increasing utility of these cables beyond data transfer—for example, as a source of environmental data—will create further tensions between States; as the ITU has noted, such use of submarine data cables in the EEZ has raised questions as to the applicability or otherwise of the UNCLOS marine scientific research regime to these cables.

This increased utility, and the radically increased reliance of States upon submarine data cables for data transfer, serves to emphasise the potential consequences of their vulnerability to damage by malicious acts, accidents, or natural phenomena. These vulnerabilities extend beyond international

---

1 Noting, however, that the UN Group of Governmental Experts in 2017 did not achieve consensus on its report; this represented (to some extent) an attempt by some States to wind back previously agreed positions in relation to ‘recommendations on the implementation of norms, rules and principles for the responsible behaviour of States’, and ‘application of international law to the use of information and communications technologies’: ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General’ UN Doc A/72/327 (14 August 2017) <https://undocs.org/A/72/327>. The renewed dual track Open Ended Working Group (OEWG) – Group of Government Experts (GGE) process (2019–2021) has attempted to revive this process. See <https://www.un.org/disarmament/ict-security/>.


3 Through use of SMART (Science Monitoring And Reliable Telecommunications) cables which integrate environmental sensors directly into cable design to capture ocean bottom temperature, pressure, and seismic data: BM Howe et al., ‘SMART Subsea Cables for Observing the Earth and Ocean, Mitigating Environmental Hazards, and Supporting the Blue Economy’ (Frontiers in Earth Sciences, 7 February 2022) <https://www.frontiersin.org/articles/10.3389/feart.2021.775544/full>.


5 Non-criminal damage to two cables in the Mediterranean in 2008 reduced Internet capacity in Egypt 80 per cent and disrupted 75 per cent of communications between the Middle East/Asia and the rest of the world, with significant economic and social consequences; the rerouting required then caused further slowdowns and disruptions to Internet services globally: see inter alia, B Johnson, 2009.
communications to financial, data storage and service provision, and to the military sectors. It is, for example, a commonplace that US$10 trillion of transactions take place via the undersea data cable network daily; beyond this, a majority of Europe’s data is stored in US data centres and relies on cable connectivity for access. Increasingly, major cloud-based corporations such as Google, Amazon and Meta are investing in submarine cables or rolling out their own proprietary cables. They are doing this in part to facilitate access to their cloud-based services for overseas customers. One goal of Google’s new ‘Firmina’ cable was to connect customers in Argentina, Brazil and Uruguay with Google services. Universities and commercial organisations increasingly rely on cloud-based providers for their data storage and email provision. This rise of ‘software as a service’ means that the applications used on our desktop or laptop computers may actually be based in another country. Thus ‘as individuals and businesses increasingly rely on the cloud to perform basic functions, reliable access to that cloud is not merely important – it is critical’, and that access for many States relies upon submarine cables. Governments too are vulnerable, as ‘[d]iplomatic cables and military orders largely pass through … privately owned cables’.

The political, social and economic consequences of interference with these cables therefore cannot be underestimated. This is exponentially so for some States—such as Kiribati, Tonga, and the Marshall Islands—which are currently serviced by a single data cable. Recently, a volcanic eruption off Tonga severed the country’s sole cable between 15 January and 22 February
2022 largely cutting the country off from communication with the rest of the world.\textsuperscript{14}

Presently, more than 98 per cent of all data traffic is carried by just over 400 undersea data cables globally.\textsuperscript{15} Critical ‘bottlenecks’ link numerous cables in Egypt, Guam and Hawaii—the latter being both exposed to volcanic damage and accounting for up to 70 per cent of Australia’s international connectivity.\textsuperscript{16} Terrestrial cable networks offer a partial, but potentially limited and vulnerable, alternative. The US, Canada and Mexico can perhaps be treated as one integrated North American bloc linked through terrestrial cables. The same is not necessarily true of other continents. The overland cable networks connecting Europe and Southeast Asia, for example, all run through Russia and China,\textsuperscript{17} putting those two governments in a position to monitor or interrupt communications.

While it may be the case that ‘it has long been held that submarine cables are legitimate wartime targets’,\textsuperscript{18} increased dependence on them now means that the consequences of severing of a submarine telecommunications cable as part of an armed conflict, whether by a State or non-State actor, would be severe and could be felt in every corner of the globe. Alarmingly, a characteristic of the race to weaponise and securitise cyberspace has been the lack of restraint shown by many actors.\textsuperscript{19}

Faced with these problems, the tendency of legal analysis has been to identify gaps or deficiencies in the law,\textsuperscript{20} and propose the need either for the creation of


\textsuperscript{19} G Austin, ‘Restraint and Governance in Cyberspace’ in A Burke and R Parker (eds), \textit{Global Insecurity: Futures of Global Chaos and Governance} (Palgrave Macmillan 2017) 216–34.

new legal instruments or the urgent conclusion of a multilateral treaty making intentional damage to cables an international crime. Nonetheless, such projects have had to acknowledge the unlikelihood of major legal reform and in particular of concluding new treaties. The contribution of this article to the literature is twofold. First, it expands the frame of analysis to include deliberate damage to cables not only in peacetime, but under the law of armed conflict. Second, rather than treating the legal framework as inherently deficient, it considers the extent to which existing rules and principles can be progressively developed, interpreted, or creatively applied to close some of the perceived gaps.

This article will thus survey the existing law specific to the protection of submarine cables as well as assess how general principles of the law of the sea, State responsibility, the law on the use of force, and the law of armed conflict apply to this problem. It thus considers in turn the applicable ‘law of peace’, the *jus ad bellum* and *the jus in bello*. For reasons of space, it is beyond the scope of this article to consider the potential role of submarine cables as a vector for foreign espionage or interference operations against a target State.

II. PEACETIME PROTECTION OF SUBMARINE CABLES

A. Introduction

This section first reviews the international law of the sea applicable to the protection of submarine cables beyond territorial jurisdiction. To date, this body of law has largely focussed on the liability of private actors for damage to submarine cables. Second, it discusses the potential application of the law of State responsibility to incidents of accidental cable damage beyond territorial jurisdiction. It is argued that there is, at least where a failure of due diligence on the part of flag States can be shown, a potential application of the transboundary harm principle in such cases. Finally, it discusses the

eg HE Matley ‘Closing the Gaps in the Regulation of Submarine Cables: Lessons from the Australian Experience’ (2019) 11(3) Australian Journal of Maritime & Ocean Affairs 165–84; Burnett (n 18); Liao (n 18); and Shepherd (n 16). There is presently an International Law Committee examining the regime of submarine cables: ‘Proposal for Establishment of a New ILA Committee on Submarine Cables and Pipelines under International Law’, paras 5–10; ‘International Law Association: Submarine Cables and Pipelines under International Law—Interim Report 2020’ both available at <www.ila-hq.org/index.php/committees>. Its work does not yet cover the law of armed conflict, though it may examine that question in the future.


23 Bueger and Liebetrau (n 20) 398; Davenport (n 22) 221.

24 See Davenport (n 16).
application of the international law of piracy and national terrorism laws to cable protection.

B. The Law of the Sea on Submarine Cables

It has been acknowledged that ‘the legal basis for coastal States to protect submarine cables lying in areas outside of their sovereignty is open to question’.25 Within the territorial sea, a coastal State’s title to regulate and protect submarine cables lies in its sovereignty (territorial jurisdiction).26 The UN Convention on the Law of the Sea (UNCLOS) provides that a ‘coastal State may adopt laws and regulations … relating to innocent passage through the territorial sea, in respect of … the protection of cables and pipelines’ and that it may further ‘establish conditions for cables or pipelines entering its territory or territorial sea’.27

The rights and responsibilities of a coastal State in the exercise of its jurisdiction are less than entirely clear. UNCLOS contains permissive jurisdictional provisions which, for example, do not impose duties to protect cables in the territorial sea. Nonetheless, and despite the likelihood such cables will be privately owned by foreign entities, coastal States have a clear national interest in exercising this jurisdiction to protect cables. However, in the absence of a positive duty to protect, it will be difficult to attribute responsibility for damage to the coastal State. Territorial jurisdiction, only extends as far as the 12 nm limit. To take but a few examples, the vast majority of the 12,700 km Australia–Japan Cable or the 21,000 km Pacific-Crossing 1 telecommunications cable linking Japan and the US, or of any of the 7000 km cables between the US and UK, plainly falls beyond national jurisdiction.

Beyond the territorial sea, ‘[r]egulatory efforts have focused on the attribution of responsibility for damage to cables, with that centring on the flag state of the offending vessel, rather than vesting jurisdiction in a coastal state or cable user’.28 This position has not substantially changed with the historic extension of coastal State rights over the continental shelf after 1945 and through the Exclusive Economic Zone from the 1970s onward. These developments are discussed below. The first relevant international instrument was the earlier 1884 Paris Convention for the Protection of Submarine Telegraph Cables (Paris Convention). Article 2 provides that:

It is a punishable offence to break or injure a submarine cable, wilfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic

25 Liao (n 18) 457.
communication, either wholly or partially, such punishment being without prejudice to any civil action for damages.

The Convention provides for flag-State jurisdiction over such offences, and in the alternative for prosecution by the State of nationality of an offender. The Convention excluded from the scope of this offence cases where damage to a cable resulted from persons acting with the ‘lawful object of saving their lives or their ship’, and acts carried out in accordance with—when applicable—the law of war. Article 10 provided a rare power of high seas visit by foreign warships to gather evidence under the Convention:

When the officers commanding … ships of war, [or other commissioned vessels] … have reason to believe that an infraction of … the present Convention has been committed by a vessel other than a vessel of war, they may demand from the captain or master the production of the official documents proving the nationality of the said vessel. … Further, formal statements of the facts may be prepared by the said officers, whatever may be the nationality of the vessel incriminated.

At least one such inspection occurred when in 1959 a US warship investigating a break in an Atlantic cable off Newfoundland ‘boarded the Soviet trawler Novorossiisk and minuted its papers’. The Paris Convention, however, provided only for ‘visitation on the high seas, not for arrest or even for search.’ Its practical utility is further hampered by its low level of ratification having only 36 parties.

Certain of its provisions were, however, transposed into the Geneva High Seas Convention 1958 (63 parties) and UNCLOS (168 parties). The High Seas Convention Article 27 and UNCLOS Article 113 provide:

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 wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications … shall be a punishable offence.

Article 113, however, provides for prescriptive jurisdiction only. Action against a national under such a law would have to await their return to their own jurisdiction; and while enforcement action could be taken by a law-enforcement vessel against a merchant vessel flying the same flag on the high seas which was suspected of such an offence, such a case is highly improbable.

30 ibid, art XV: ‘It is understood that the stipulations of the present Convention do not in any way restrict the freedom of action of belligerents.’ O’Connell (n 26) 821.
(relying as it does on the random proximity of the two co-national vessels). There is no equivalent to the Paris Convention’s provision of visitation powers in UNCLOS. The provision for the exercise of flag State jurisdiction and jurisdiction over the conduct of nationals over acts occurring on the high seas applies equally within the Exclusive Economic Zone of third States by virtue of Article 58(2) UNCLOS.

The legal framework established under Article 113 has two notable consequences. First, ‘[t]here is no equivalent obligation for coastal States to adopt such national legislation in areas subject to their territorial sovereignty or sovereign rights’.34 Secondly, there is no obvious power in coastal States to exert prescriptive or enforcement jurisdiction within the EEZ or upon the surface of their continental shelves (outside the territorial sea) over telecommunication cables.35 Indeed, as the laying of such cables in the EEZ is treated not as a right of the coastal State but as a freedom of the high seas belonging to third States, a potentially ‘competitive relationship’36 is established by Article 79(2) which provides that:

subject to its right to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources and the prevention, reduction and control of pollution from pipelines, the coastal State may not impede the laying or maintenance of such cables or pipelines (emphasis added).

Nonetheless, the literature has noted the increasing propensity of States to prescribe ‘cable protection zones’ within their EEZs where certain activities are prohibited. A proposal for such protective zones around submarine pipelines was considered by the International Law Commission in its work on the law of the sea in 1956 and was rejected by the Special Rapporteur JPA François as it ‘would constitute a further encroachment on the freedom of navigation and fishing … that it is consequently unjustified’.37 François further noted that ‘[i]t would prove very difficult, in practice, to mark the limits of such a zone’ (a concern one might consider to have diminished with improvements in navigational technology).38

While it has thus been asserted that ‘the legal basis’ for such zones ‘in areas outside the territorial sea is questionable’,39 much depends on the precise scope of such zones and the powers asserted within them by coastal States. For example, within the EEZ a coastal State has a general power to impose ‘terms and conditions’ regarding fishing in the EEZ with which foreign nationals ‘shall comply’ including but not limited to licensing conditions, gear restrictions and enforcement measures.40 Thus, within the EEZ, ‘the restriction of various types of fishing activities’ which could damage cables

---

34 Liao (n 18) 461. 35 Kaye (n 28) 190. 36 Liao (n 18) 462. 37 (1956) 2 Yearbook of the International Law Commission 12. 38 ibid. 39 Liao (n 18) 465. 40 UNCLOS art 62(4) (setting out regulatory powers in a lengthy but non-exhaustive list).
would be a valid exercise of a coastal State’s jurisdiction over fisheries. Such measures could include gear restrictions or closure of certain areas to fishing activities.

New Zealand has a tailored statutory regime under which numerous cable protection zones have been declared, but which may only be enforced against New Zealand flagged vessels, New Zealand nationals (even when operating on a foreign vessel) or within the territorial sea. For its part, the Australian regime of cable protection zones established under the Telecommunications Act 1997 may prohibit or restrict a range of fishing and other economic activities within such zones (all of which fall within the authority of a coastal State over its EEZ).43

A range of further offences under Australian law deal with negligently or deliberately damaging a submarine cable within a declared protection zone. The fact that these latter offences are prima facie enforceable against foreign nationals and vessels has been described as ‘questionable’ as a matter of international law. Nonetheless, it is notable that the Telecommunications Act 1997 appears to contemplate enforcement only by restraining injunction or civil penalty, and such proceedings against foreign nationals and vessels further require the consent of the Commonwealth Attorney General. No question of at-sea enforcement beyond the territorial sea thus arises, mitigating the extent to which the Telecommunications Act could be considered to assert exorbitant enforcement jurisdiction. The regime also appears designed to ensure that if Australia takes action under its legislation that may give rise to State responsibility, then that decision is one which must be taken deliberately by the Attorney General.

C. State Responsibility for Accidental Cable Damage

As discussed above, international law has long focussed on individual responsibility for deliberate or negligent damage to cables. This leads to the question whether there are any conditions under which a flag State may be responsible for such damage. State responsibility obviously relies on there being an act or omission, attributable to a State, which constitutes a breach of that State’s international obligations. It is contended that it is possible to conclude that there may be such a duty. This is not because a vessel is an organ of its flag State, the acts of which are attributable to the flag State. The point is rather that even where there is no strict liability duty to prevent an outcome, there may still be duties of due diligence to take steps to prevent such an outcome. A failure of due diligence may be a basis for State responsibility.

41 Kaye (n 28) 192.
42 See Kaye (n 28) 200; Submarine Cables and Pipelines Protection Act 1996 (New Zealand) sections 4, 12–13.
43 Telecommunications Act 1997 (Australia), Schedule 3A, cl. 10–11.
44 ibid, cl. 36–39.
45 ibid, cl. 36–39.
46 ibid, Schedule 3A, cl. 83A.
The first question is to identify where such duties might be found in UNCLOS. Article 113 clearly places an obligation on States to criminalise wilful or negligent damage by vessels permitted to fly its flag; it does not, however, address the issue of financial liability or State responsibility for such damage. It is suggested that cases of damage caused to submarine data cables that do not meet the threshold of criminal behaviour (for private actors), or armed attack (for State actors) may nonetheless give rise to State responsibility (and financial liability). The caveat to this responsibility is that where it can be shown that all care was taken, or the damage to the data cable was not reasonably foreseeable, then the State cannot be held liable.

The basis of this argument for State responsibility for the harm caused follows from the principle in the *Trail Smelter* arbitration or the due diligence principle enunciated by the International Tribunal for the Law of the Sea (ITLOS) in two of its advisory opinions.48

The *Trail Smelter* arbitration concerned whether Canada was liable for environmental harm occurring in the territory of the United States caused by pollution from the smelter which it had permitted to operate in Trail, British Columbia. The question at the core of the case was: is a State liable for harm that originates within its jurisdiction but that is realised in another jurisdiction. The arbitration enunciated the principle that:

> no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the cases of serious consequence and the injuries established by clear and convincing evidence.49

The arbitration has since been treated as establishing a norm of international law regarding State responsibility for transboundary harm generally. Sometimes called the principle of prevention, the duty extends not only to activities in a State’s territory which might cause significant harm to other States but to ‘any area under its jurisdiction’.50 It is argued that where cable damage is attributable to a State under this principle, because of its responsibility for the conduct of the vessel in question, it may be responsible not only for the value of the repair to the cable, but all losses stemming from the cable damage. For the most part the question of attribution is a simple one under the law of the sea because of the nature of flag ship jurisdiction set out in Articles 92 and 94 of UNCLOS.51 That is, vessels are subject to the ‘exclusive jurisdiction’ of their

---

48 Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission (SRFC) (No. 21), Case No. 21, Advisory Opinion of 2 April 2015, ITLOS <https://www.itlos.org/fileadmin/itlos/documents/cases/caseno.21/advisory-opinion/C21-AdvOp-02.04.pdf>; Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (No. 17), Case No. 17, Advisory Opinion of 1 February 2011, 10 ITLOS REP 7, 10.
51 UNCLOS, arts 92 and 94.
flag State in areas beyond the territorial sea; and each State has a positive duty to ‘effectively exercise its jurisdiction and control in administrative, technical and social matters over ships flying its flag’.

The duties regarding cable protection, it is suggested, are one aspect of that broader duty to ‘effectively exercise jurisdiction’. Thus, while a vessel on the high seas is not considered floating territory, it certainly constitutes an area under State jurisdiction. It is therefore perfectly possible to apply the transboundary harm principle to events originating aboard a ship and having harmful consequences felt elsewhere. The standard is obviously not one of strict liability; rather, in the ILC’s formulation of the Corfu Channel principle, liability for a transboundary harm follows where a harm arises within a State’s ‘territory or control’ and it has ‘knowledge of the harm, or means of knowledge, and opportunity to act’. Further, the ‘standard of care or vigilance required of a State rises in proportion to the degree of danger known to be associated with the conduct of a particular activity’. We would now call this the due diligence principle.

The application of the due diligence principle in the context of the law of the sea has been explored in two ITLOS advisory opinions: Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (‘Obligations in the Area’) and Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission (‘SRFC’). It is argued that the due diligence principle developed in both of these cases could also be extended to a responsibility for flag States to take measures to prevent damage to submarine cables by vessels enjoying their nationality. This requires a brief review of the approach taken in both opinions.

The first arose in the context of Nauru and Tonga putting forward proposals for seabed mining activities through sponsored commercial entities, Nauru Ocean Resources Inc and Tonga Offshore Mining Ltd, which would operate within the international seabed ‘Area’ administered under UNCLOS by the International Seabed Authority. However, both States were concerned as to the extent of their potential liability for any adverse environmental consequences caused by the activities of the entities they sponsored. In this regard Article 139(1) of UNCLOS provides (emphasis added):

States Parties shall have the responsibility to ensure that activities in the Area, whether carried out by States Parties, or state enterprises or natural or juridical persons which possess the nationality of States Parties or are effectively controlled by them or their nationals, shall be carried out in conformity with this Part.

52 ibid
53 S.S. Lotus (Fr v Turk), 1927 PCIJ (ser. A) No. 10 (Sept 7), 23.
54 Pulp Mills (n 50) para 101.
56 ibid 148.
Article 4(4) of Annex III restates this obligation and adds:

A sponsoring State shall not, however, be liable for damage caused by any failure of a contractor sponsored by it to comply with its obligations if that State Party has adopted laws and regulations and taken administrative measures which are, within the framework of its legal system, reasonably appropriate for securing compliance by persons under its jurisdiction.

As small-island developing States, Nauru and Tonga were obviously concerned about the extent of their vicarious liability under such provisions. Nauru thus asked the Secretary General of the International Seabed Authority to seek an advisory opinion on the question from the Seabeds Dispute Chamber of ITLOS. In sum, ITLOS held that Article 139 imposes obligations of conduct, not result. While there was no strict liability for damage caused, there was nonetheless an obligation of due diligence, which may impose more stringent requirements for higher-risk activities. In support of this conclusion the Chamber endorsed Principle 15 of the Rio Declaration, and noted that cases such as *Pulp Mills on the River Uruguay* support a trend towards due diligence becoming part of customary international law.

In the context of Article 139 the obligation includes: application of the precautionary approach; the obligation to take action where there are plausible indications of potential risk but scientific evidence is insufficient; the adoption of best environmental practices; a requirement that the sponsored entity must give technical and financial guarantees (including financial recourse for any damage caused); and undertaking an environmental impact assessment. This system of supervision must be carried out through laws, regulations, and administrative measures in the sponsoring State and not merely contractual measures.

The SRFC advisory opinion was sought by member States of a West African regional fisheries management organisation concerned at the prevalence of illegal, unreported or unregulated (IUU) fishing in their jointly managed waters. The question at issue was the extent of flag State responsibility for such activities. The ITLOS found that ‘the primary responsibility for taking the necessary measures to prevent, deter and eliminate IUU fishing rests with the coastal State[s]’.

Nonetheless, ITLOS found that in light of other provisions in the Convention, including the general duty to protect and preserve the marine environment under Article 192, that ‘flag States also have the responsibility to ensure that vessels flying their flag do not conduct IUU fishing activities within the exclusive economic zones of the SRFC Member States’. In giving content to this duty ITLOS referred both to

---

58 *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, paras 141–150.

59 *Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission*, para 106.

60 ibid, para 124.
Obligations in the Area and once again quoted Pulp Mills on the River Uruguay for the proposition that this required:

not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement and the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party.61

The argument could be made that Article 113 on the measures to be adopted to protect submarine cables by States parties are less detailed than UNCLOS’ provisions on seabed mining, and that seabed mining arises in the context of a permitted activity. Nonetheless, the provisions of Article 113 are considerably more precise than the Article 119 duty to protect and preserve the marine environment. That duty was examined in the SRFC advisory opinion regarding illegal fishing and environmental harm. It would therefore seem reasonable to apply a duty of due diligence to flag States to take appropriate measures in respect of vessels flying their flags to prevent damage to submarine cables in line with both the Obligations in the Area and SRFC advisory opinions. The only basis on which to resist this conclusion would be to suggest that Article 113 imposes an exhaustive obligation of result: to implement necessary ‘laws and regulations’.

Such a conclusion should be resisted for two reasons. The first is the principle of effectiveness. Nothing in Article 113 requires the laws be effectively enforced. The provision cannot mean State responsibility ends with merely enacting laws. The lack is supplied by the principle of due diligence. Second, this conclusion is bolstered by the Article 94 duty upon each flag State to ‘effectively exercise its jurisdiction and control’ which must extend to the matters contemplated in Article 113 (emphasis added). Of course, following Pulp Mills, it was held in both Opinions that responsibility is contingent on regulatory failure; for liability to arise it must be shown that the State ‘had failed to act diligently and thus take all appropriate measures to enforce its relevant regulations’.62 The result is thus not strict liability but liability for the failure to regulate effectively.

This application by analogy of Trail Smelter or the principle of due diligence to unintentional peacetime damage to submarine cables is consistent with the United States’ influential Restatement of International Law documents, and with the ILC draft articles related to International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law.63 The most distinct interpretation of the weight of Trail Smelter on issues of transboundary harm in international law occurred in Restatement Two where the US stated: ‘The relation of cause to effect underlies the parallel principle

61 Pulp Mills 79, para 197.
62 ibid.
that a state may be held responsible under international law for damage which it causes in the territory of another state.\(^{64}\) While Restatement Three is somewhat more opaque in how it puts this proposition,\(^{65}\) the positions taken in later Restatements appear generally consistent with the Restatement Two position. This notion of liability under international law for damage caused within the territory of another State can, and should, be limited to situations in which the responsible State did not take all reasonable steps and exercise due diligence to prevent said damage.\(^{66}\)

**D. Is Intentional Damage to Submarine Cables a Form of Piracy?**

Absent a more effective international regime of protection, the question has occasionally been raised, since at least 1869, as to whether intentional damage to submarine cables on the high seas may be a form of piracy.\(^{67}\) This point has recently and stridently been put by, *inter alia*, Lawrence Wrathall:

… there is temporal ripeness to treat undersea pirates as *hostes humani generis*. Critical infrastructure below the waterline is often beyond national jurisdiction and remote from the state of affiliation. Therefore, it should be unambiguously incorporated into the LOSC definition of piracy along with ocean platforms. The *two-vessel* requirement and the *private ends* limitation should be eliminated to deter signatory states and their inhabitants from looting and possibly inciting economic and environmental shock at the margins of antiquated definitions.\(^{68}\)

An advantage of this approach is that it would bring such offences within universal jurisdiction (or, perhaps more accurately, concurrent municipal jurisdiction)\(^{69}\) to prosecute and provide powers of visit, board, search, and arrest for government vessels encountering suspect ships outside the territorial sea. Such a result might now follow insofar as piracy covers, under both the 1958 Geneva Convention on the High Seas Article 15 and UNCLOS Article 101(a), not only acts of violence on the high seas committed from one vessel against another (as highlighted by Wrathall) but also:

\(^{64}\) *Restatement (Second), Foreign Relations Law of the United States* (American Law Institute 1965), 55.


any illegal acts of violence … or any act of depredation, committed for private
ends by the crew or the passengers of a private ship … and directed: … (ii)
against a ship, aircraft, persons or property in a place outside the jurisdiction of
any State[.]) (Emphasis added.)

The important point to note here is that for a certain category of property
offences, those occurring ‘outside the jurisdiction of any State’, the two-
vessel requirement was removed from the definition of piracy no later than
1958. Thus, on its face, deliberately damaging a section of submarine cable
outside the territorial sea would be an act of violence or depredation against
property in a place beyond any State’s jurisdiction and would thus constitute
piracy within the meaning of Article 101(a)(ii). Notably, however, piracy
may not be committed by a government vessel or warship unless its crew
mutinies. Thus deliberate governmental acts of interference with submarine
cables (such as tapping them for intelligence gathering purposes) will not
qualify as piracy.

As is common (if not inevitable) in matters regarding the definition of piracy,
however, the correct construction of the words emphasised above has been the
subject of some controversy. Liao contends that the wording found in Article
101(a)(ii) ‘should be understood as [only] including internal seizures of a
ship as piracy’. While this view has some support, it is ultimately
unsustainable. The disjunctive reference (using ‘or’) to ‘property … outside
the jurisdiction of any State’ could not be plainer. Further the principle of
flag State jurisdiction makes it dubious whether incidents such as the ‘mutiny
of the crew against the master of a vessel’ can be described as acts of violence
occurring outside the jurisdiction of any State.

The International Law Commission (ILC) first included this phrasing in order
to cover acts ‘committed by a ship … [against persons or property] on an island
constituting terra nullius or on the shores of an unoccupied territory’. It is thus
not incompatible with this intention to apply it to another terra nullius (or
perhaps res communis), the seafloor area beyond national jurisdiction. Indeed,
the ILC went on to observe that ‘it wished to prevent such acts
committed on ownerless territories from escaping all penal jurisdiction’. It
thus appears that the ILC intended these broad words to be construed broadly.

70 DR Burnett and MP Green, ‘Security of International Submarine Cable Infrastructure: Time
to Rethink?’ in MH Nordquist, R Long and R Wolfrum (eds), Legal Challenges in Maritime Security
71 UNCLOS, art 102; D Guilfoyle, ‘Article 102’ in A Proelss (ed), United Nations Convention
72 Liao (n 18) 472.
74 ILC, Report of the International Law Commission: Commentaries to the Articles Concerning
the Law of the Sea, UN Doc A/3159 (1956), GAOR 11th Sess. Suppl. 9, 12, 28 (art 39).
75 ibid.
The essence of the provision is that piracy cannot occur in spaces where sovereignty is present; and the Area is a space where sovereign claims are excluded. Insofar as the status of the Area is a legal development occurring after the initial codification of piracy, the phrase ‘beyond the jurisdiction of any State’ is, as Alan Boyle has put it, an ‘ambulatory’ phrase using legal words to incorporate meanings found in general international law as it exists from time to time. They are words designed to permit a (limited) evolutionary interpretation.

An alternative objection has been raised in the case of terrorist damage to submarine cables, the argument being that intentional terrorist damage to cables could not be piracy because it would be, by definition, politically motivated and thus not an act ‘for private ends’. The words ‘for private ends’ appear both in the High Seas Convention and UNCLOS definitions of piracy, having been taken up from codification efforts in the period 1926–1932. This phrase, however, has no origins in case law and appears to be traceable to the work of a criminal law textbook author of the 1890s.

The question which has arisen is whether the relevant distinction is between private ends and political motives (private/political), or between private ends and public authorisation (private/public). It is submitted that the relevant distinction is private/public: that is, the essence of piracy is unauthorised violence at sea. This is so for several reasons. First, UNCLOS Article 102 itself makes it plain that warships may not commit piracy unless they mutiny, in which case their acts may be ‘assimilated to acts committed by a private ship’. This strongly suggests the relevant distinction is private/public. Thus, it was said by a League of Nations expert committee in 1927:

According to international law, piracy consists in sailing the seas for private ends without authorization from the Government of any State with the object of committing depredations upon property or acts of violence against persons.

Secondly, the concrete historical problem codifiers sought to address with these words was generally agreed to be a narrow question of the law of armed conflict: the status of belligerent insurgencies which took to the sea and attacked foreign shipping. There was general agreement that such actors (in what we would now call non-international armed conflicts) should enjoy a limited immunity from the law of piracy. In this sense, the exemption was a question of

---

76 UNCLOS art 137(1).
79 Guilfoyle (n 73) 740–1.
80 ibid 740.
81 Quoted in JW Bingham, ‘Codification of International Law: Part IV: Piracy’ (1932) 26 AJIL Suppl. 739, 775, 808.
objective status, not subjective motivation.\textsuperscript{83} Thirdly, it has not been adequately explained as a matter of policy why those perpetrating otherwise criminal violence at sea should have a complete defence if they claim they had a political motive.\textsuperscript{84} Indeed, in no decided case has a court confronted with such a claimed ‘defence’ accepted it.\textsuperscript{85} Consequently, depredations against submarine cables in the high seas by non-State actors may constitute piracy, and concurrent municipal jurisdiction over such offences is available.\textsuperscript{86} (However, as noted, where such actions are carried out by \textit{de facto} or \textit{de jure} State agents, they cannot be piracy other than in cases of mutiny.)

It might be set against this conclusion that UNCLOS Article 97 establishes the exclusive penal jurisdiction of the flag State or the defendant’s State of nationality in respect of any ‘incident of navigation concerning a ship on the high seas’ involving the responsibility ‘of the master or of any other person in the service of the ship’.\textsuperscript{87} In this context, the International Law Commission thought that damage to submarine telegraph cables could be considered an incident of navigation.\textsuperscript{88} Does this exclude any claim to universal jurisdiction over offences against submarine cables? No, it does not. Article 97 was intended to cover such matters as collisions, strandings, and other ‘maritime casualties’ resulting from the manoeuvring of a vessel.\textsuperscript{89} The expression ‘incident of navigation’ may thus cover accidental or even negligent damage to a cable (and as such it may be used to render private actors liable for the cost of damages arising from State liability discussed above) but does not carry connotations wide enough to encompass deliberate acts,\textsuperscript{90} let alone malicious ones.

Ultimately, of course, the ability to prosecute malicious cable cutters as pirates will only be as good as national laws enabling such prosecutions. However, if this interpretation of the law of piracy is correct any national law directly incorporating the terms of UNCLOS or the Geneva Convention will be sufficient. Unfortunately, national laws sometimes depart from UNCLOS.

\begin{itemize}
\item \textsuperscript{83} D Guilfoyle, \textit{Shipping Interdiction and the Law of the Sea} (CUP 2009) 42; see also \textit{United States v Hutchings}, 26 F.Cas. 440 (1817).
\item \textsuperscript{86} Guilfoyle (n 83) 49.
\item \textsuperscript{87} UNCLOS art 97 and Geneva Convention art 11 were the result of a campaign by seafarers to overturn the rule in \textit{Lotus} that both flag States involved in a negligent collision could assert criminal jurisdiction: D Guilfoyle, ‘Article 97’ in A Proelss (ed), \textit{United Nations Convention on the Law of the Sea: A Commentary} (Beck/Hart/Nomos, 2017) 721, 722–3.
\item \textsuperscript{88} ILC, Report of the International Law Commission: Commentaries to the Articles Concerning the Law of the Sea, UN Doc A/3159 (1956), GAOR 11th Sess. Suppl. 9, 12, 27 (art 35).
\item \textsuperscript{89} Guilfoyle (n 87) 723.
\item \textsuperscript{90} Contra this argument: \textit{The ‘Enrica Lexie’ Incident (Italy v. India)}, Provisional Measures, International Tribunal for the Law of the Sea, Case No. 24, Written Submissions of Italy (July 21, 2015), para 35(b). The argument was, however, rejected: \textit{The ‘Enrica Lexie’ Incident (Italy v. India)}, Permanent Court of Arbitration case 2015-28, Award, 21 May 2020, paras 642–650.
\end{itemize}
in significant ways and do not necessarily incorporate the ‘outside the jurisdiction’ of any State principle.\textsuperscript{91} Where possible, this should be remedied by national legislatures.

\textit{E. National Terrorism Laws}

Other offences might incidentally grant jurisdiction over non-State actor attacks on submarine cables, in particular terrorist offences. For example, the Australian definition of terrorist offences under the Commonwealth Criminal Code largely reflects the growing international consensus that such offences include acts (or threatened actions) causing serious harm to a person or serious damage to property when (1) ‘made with the intention of advancing a political, religious or ideological cause’ and (2) done with the further intention of either:

(a) ‘coercing, or influencing by intimidation’ a government (be it Australian or foreign); or
(b) ‘intimidating the public or a section of the public’.\textsuperscript{92}

In addition, however, the Australian legislation (following to some extent the UK model)\textsuperscript{93} also covers any act which ‘seriously interferes with, seriously disrupts, or destroys, an electronic system including’ \textit{inter alia}: an ‘information system’; ‘a telecommunications system’; ‘a financial system’; ‘a system used for, or by, an essential public utility’.\textsuperscript{94} Plainly, a submarine telecommunications cable falls within at least the second of these definitions, but may in addition plausibly fall within some or all of the others. Moreover, for constitutional reasons the Australian offence expressly covers acts that disrupt trade or commerce ‘between Australia and places outside Australia’, including banking and insurance services.\textsuperscript{95}

Such an Australian nexus is not strictly required, however, as a sweeping definition of extraterritorial jurisdiction applies to such offences irrespective of whether either the relevant conduct or result ‘constituting the alleged offence occurs in Australia’.\textsuperscript{96} Thus, Australia effectively asserts universal jurisdiction over terrorist offences.\textsuperscript{97} As a consequence, if done with the


\textsuperscript{92} Criminal Code Act 1995, Australia, section 100.1(1).

\textsuperscript{93} Terrorism Act 2000 (c. 11), United Kingdom, section 1(2)(e).


\textsuperscript{95} ibid, section 100.4(5)(j) and (k).

\textsuperscript{96} ibid, section 101.1(2) referring to section 15.4 (‘extended geographic jurisdiction’).

\textsuperscript{97} Albeit that prosecution of a de facto universal jurisdiction offence requires the approval of the Attorney General: ibid, section 16.1.
requisite motive, intentional damage to a submarine cable anywhere in the world could fall within the Australian definition of terrorism.

To the extent that the concern is with preventing malicious damage to submarine cables such efforts may, ironically, be undermined by efforts to prevent their inadvertently being damaged through the creation of protection zones. As Heintschel von Heinegg has noted, while cable protection zones may be successful in terms of integrated ocean management, and may even ‘ease the burden of attributing mal intent’ in cases where vessels deliberately loiter in such zones, nonetheless cable protection zones and their location must be made public to international shipping, thus giving potential attackers almost perfectly exact information on their target. Hence, such zones will only contribute to an enhancement of submarine cable protection against the usual threats posed by merchant and fishing vessels.98

Similarly, the Australian Commonwealth offence of sabotage makes it an offence (subject to an assertion of extraterritorial protective jurisdiction) to ‘seriously disrupt’ an electronic system which constitutes ‘public infrastructure’ when the act is done on behalf of or in collaboration with a ‘foreign principal’ (including a foreign government or terrorist organisation).99 This includes not only electronic systems belonging to the Australian government but also extends to electronic systems located in Australia, which provide services to the public, and which are operated by corporation or which are used in trade and commerce (section 82.2(1)(e)).100 Again, the cutting of a telecommunications cable outside Australian territory (whether within or beyond the EEZ) could ‘seriously disrupt’ Internet service provision within Australia in a manner falling within the defining of sabotage. Jurisdiction over such an offence is unobjectionable as ‘the crime is completed via [its] effects on [a] communications system within’ territorial jurisdiction.101

III. STATE OR STATE-SPONSORED DAMAGE TO SUBMARINE CABLES

A. Introduction

When examining intentional damage to cables carried out by States (either directly, or through conduct that can be attributed to the State) and whether such measures could justify the use of force in individual or collective self-defence, two separate questions need to be addressed. The first is how the Security Council will be likely to respond to such an incident; and the second

99 Criminal Code Act 1995, Australia, sections 82.1 and 82.3.
100 ibid 82.2(1)(e).
101 Liao (n 18) 467.
is would such cable damage give rise to self-defence measures under Article 51 of the Charter.

When considering the potential response of the Security Council to State or State-sponsored cable cutting, the focus of this analysis centres around possible Chapter VII action. This is because it is under Chapter VII that the Security Council has the ability to make binding resolutions addressing a cable-cutting incident, resolutions which would justify action against the responsible actors. This could include the authorisation of a sanctions regime, collective military action, interruption of diplomatic relations with the State in question, or any other action short of the use of armed force that it deems appropriate (such as a commission of enquiry).

This analysis of the likely Security Council response to a major cable-cutting incident focusses upon whether Security Council is predisposed to a finding of ‘threat to the peace’. This is because it is the most elastic of the options available under Article 39 of the Charter allowing the Security Council to take Chapter VII action. The line of enquiry explored in relation to Article 51 will focus on whether intentional damage to a submarine cable is of sufficient gravity to give rise to characterisation as an armed attack. The question of if and when a cyber-attack could be classified as an armed attack giving rise to a right of self-defence has been extensively debated in recent years; the question addressed here concerns an attack on the underlying infrastructure, an attack with consequences which are unlikely to be localised to a single State. Given those consequences, discussed further below, cable cutting could not usually be justified as a proportionate countermeasure or belligerent reprisal (nor as a legal measure of retorsion). The analysis will therefore view it as a question of the law on the use of force.

B. Submarine Cables and Article 39

The Security Council’s treatment of ‘threat to the peace’ under Article 39 of the UN Charter has generally been described as ‘fluid and arbitrary’, political in nature, grounded in an ambiguous mandate, lacking in consistency,

flexible, and only fettered by the Purposes and Principles of the Charter itself. Paige has challenged these assumptions by undertaking an historical discourse analysis on the public justifications in meetings by the P5 in relation to their positions on whether situations constituted a ‘threat to the peace’. So while Österdahl correctly said that ‘the Security Council may basically decide or do anything it wishes and it will remain within the limits of the legal framework for its action’, Paige’s work has demonstrated that each member of the P5 has a relatively consistent approach to the question of what constitutes a threat to the peace. As a result, the impact of intentional severing of a submarine cable can be examined against the criteria used by each individual P5 member in order to suggest the likely outcome were the Security Council to consider the intentional severing of a data cable and any resulting Chapter VII resolution. However, history suggests that should any of the P5 nations be involved in such an act, they would veto any proposed resolution out of hand. One of the common aspects in P5 approaches to the existence of a ‘threat to the peace’ is whether the situation is of sufficient gravity to warrant such a finding. While the question of gravity is inherently amorphous and difficult to define, it would be difficult to suggest that the intentional severing of a submarine cable would fail to meet this threshold. In addition to the economic impact noted above, there is significant evidence to show that society now relies upon Internet infrastructure for many day-to-day activities, ranging from the provision of government services to the running of household thermostats. Given that cutting off Internet access to a State by severing a submarine cable would put at risk all of these societal infrastructures which depend upon the Internet, the question of gravity is self-evidently met. This accords with the General Assembly’s position taken in its annual ‘Oceans and the law of the sea’ resolution which says that such cables are ‘vitaly important to the global economy and the national security of all States’. Similarly, the UN Security Council had its first public debate on cybersecurity and the need to maintain

109 TP Paige, Petulant and Contrary: Approaches by the Permanent Five Members of the UN Security Council to the Concept of “Threat to the Peace” under Article 39 of the UN Charter (Brill 2019).
110 Österdahl (n 103) 98.
111 Paige (n 109) 277–87.
113 Oceans and the law of the sea UNGA Res 76/72 (9 December 2021) UN Doc A/RES/75/72 (adopted by 131 votes to 1 with 4 abstentions) (emphasis added).
international peace and security in cyberspace on 29 June 2021. While the debate did not directly address cables, speakers noted the reliance of States on, and the potential fragility of, critical information and communications technology infrastructure. These observations apply equally to submarine cables.

The biggest hurdle to a Security Council finding that severing a submarine cable amounted to a ‘threat to the peace’ would be gaining the support of China and Russia. France, the UK, and the US have demonstrated a propensity to vote in accordance with actions designed to uphold individual human rights and civil liberties. That propensity, combined with the fact that access to the Internet has been obliquely linked to Article 19 of the Universal Declaration of Human Rights, suggests that those countries would be unlikely to block such a resolution. Therefore, persuading Russia and China would be critical. Such persuasion would require showing that any proposed action would be: a) within the Security Council’s mandate for the maintenance of international peace and security; b) supports, or is it least not at odds with the rights to self-determination and non-interference in domestic affairs; and c) is focused upon generating a peaceful outcome and not upon regime change. This last point is possibly the most significant hurdle in practice, given the recent history of members of the P5 attempting to use the Security Council as a vehicle to engage in geopolitical regime change.

Assuming that the intentional severing of a submarine cable meets the factual requirements for an armed attack under Article 51 of the Charter (see below), demonstrating that responding to such an incident is within the Security Council mandate presents no difficulty. Similarly, demonstrating that the Security Council does not violate rights of self-determination and non-interference is likewise unproblematic. The real difficulty lies in ensuring that any draft resolution being put before the Security Council is non-partisan in nature and wholly focused on achieving a peaceful resolution.

Finally, the likely form of any Security Council response under Chapter VII should be considered. Given the reluctance of China and Russia to support any mandates involving the use of force - following the use of such mandates for regime change in the past - non-forcible measures such as targeted embargoes, travel bans and financial restrictions seem most likely.

---

116 Paige (n 109) 238–60.
118 Paige (n 109) 260–76.
119 See eg ibid 177–82 and 204–15.
C. Article 51 and Submarine Cables

When considering whether an incident that results in severing a submarine cable constitutes an ‘armed attack’ giving rise to self-defence (individually or collectively) under Article 51 of the Charter, regard must be had to the Oil Platforms case.\footnote{Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America) (2003).} Reinforcing the principles of the Nicaragua case,\footnote{ibid 51; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) 192 (1986).} this makes it clear that is a question of fact\footnote{ibid 51–64.} and that the ‘scale and effects’ test, set out in the Oil Platforms case, is the appropriate test to use. Severing a cable can also be understood as a form of cyber-attack which might itself quality as an armed attack. In such cases scholars, such as Hathaway, have argued that the ‘scale and effects’ test is still the appropriate test to apply.\footnote{OA Hathaway et al., The Law of Cyber-Attack (2012) 100 California Law Review 817, 847–8.} Thus that test is applicable irrespective of whether the severing of an undersea cable is seen as a physical act or as a form or cyber-attack and the full consequences of the physical act of severance need to be taken into account when applying that test.\footnote{ibid.}

For the reasons given earlier, the potential scale of harm to a State, or group of States, resulting from the severing of a submarine cable is potentially catastrophic, affecting almost all aspects of national life, including, economic activity, education, political activities, the provision of government services and much else besides.\footnote{ibid.} This is especially the case in small States with fragile Internet connectivity. Tonga’s two-week interruption in connectivity following accidental cable damage caused serious economic harm when the ‘tourism sector—the country’s main source of income—was hit … with all flight and hotel bookings halted.’\footnote{ibid 402.}

Unlike a cyber-attack, which may have only a temporary and limited impact, the severing of a submarine cable is almost certain to cause long-term disruption to all such services to the region. Given this wide scale impact, it is difficult to characterise the intentional severing of a submarine cable as anything other than an armed attack. Further, and as will be discussed below, the scale of effect is relevant when considering whether or not submarine cables can be considered a valid military target, taking proportionality considerations into account.

Data cables have no nationality or regulatory guardian in the same way as satellites. That means that interference with data cables is to a large extent much like espionage—unfriendly, but not unlawful under international law. However, despite their vital economic, social and security importance there is no coherent body of regulatory law governing the assignment of roles and jurisdictions with respect to the protection of undersea data cables.\footnote{See, inter alia, F Rose, ‘Emerging Threats: Outer Space, Cyberspace, and Undersea Cables’ (2017) 47(1) Arms Control Today 52; R Sunak, ‘Undersea Cables: Indispensable, Insecure’, Policy
IV. SUBMARINE CABLES AND THE LAW OF ARMED CONFLICT (LOAC)

A. Introduction

It is very likely that in the event of a significant inter-State conflict one of the first acts will be the severing of submarine cables. Such operations have a long history, but remain very thinly regulated by LOAC. Their likelihood has, if anything, increased given the decline in the importance of broadcast communication relative to data cables and, as noted, the ability to rely on terrestrial cable networks as an alternative is both limited and not available to all States. This conspicuous risk profile raises a series of important questions regarding the scope of permissible actions against submarine cables under LOAC. Three are as follows: submarine data cables as neutral objects; submarine data cables as military objectives; and proportionality in relation to attack on submarine data cables. However, in order to address each, it is necessary to first review the nature of the risk in historic context and some early features of the manner in which LOAC has dealt with submarine cables.

B. The Past and Future of Submarine Cable Cutting in Conflict

In August 1914, one of Britain’s first acts of hostility against Germany was to cut German submarine communications cables. This not only reduced German access to communications infrastructure (Britain owned 60 per cent of the global cables network), but facilitated the interception of re-routed German traffic—including the ‘Zimmerman Telegram’, which played a role in the US entry into the war.
likewise cut British and imperial cables connecting empire, colonies, and outposts.\textsuperscript{131}

Today, concerns as to the strategic effect of a submarine data cable denial operation (eg cable cutting) are gaining renewed traction.\textsuperscript{132} States clearly have relevant capabilities. In 2019 a deadly fire was reported in a special purpose Russian research submarine, the \textit{Losharik}. While details of the submarine remain a State secret,\textsuperscript{133} it was widely reported that it deploys specialised data cable tapping and cutting technology and that other States also have these capabilities.\textsuperscript{134} The consequences, in an armed conflict, of cable cutting can be significant. In 2008 ‘unmanned US surveillance flights’ in Iraq were compromised when an ‘anchor had snagged a cable hundreds of miles away from the base’. That ‘severed cable had linked controllers based in the United States with unmanned aircraft flying intelligence, surveillance and reconnaissance missions’.\textsuperscript{135}


\textsuperscript{131} A Jose, \textit{The Official History of Australia in the War of 1914–1918}, Vol. IX (The Royal Australian Navy, Australian War Memorial, Canberra 1928, UQ Press edn, 1987) 33 – such as at the cable station on Fanning Island 200 miles NW of Christmas Island, in the Indian Ocean. Germany also redirected and rerouted some cables – see, for example, A Pearce Higgins, ‘Submarine Cables and International Law’ (1921–1922) 2 BYBIL 27, 29.


Consequently, as Wolf Heintschel von Heinegg has observed, ‘there is a high probability of attacks [on cables] from under the sea because detection is a rather difficult task (stealth), because they imply the advantages of surprise and of economy of force, and because they can circumvent defensive measures’. The following sections consider how LOAC addresses these risks.

C. Early Efforts to Apply LOAC to Submarine Cables

As noted previously, the 1884 Convention for the Protection of Submarine Telegraph Cables (the Paris Convention) has some limited provisions relating to security matters. However, Article 15 of the Paris Convention expressly provides that ‘It is understood that the stipulations of this Convention shall in no wise affect the liberty of action of belligerents.’ This excision raised a variety of important LOAC questions. Such questions included the territorial status of cables (i.e. what rules applied if they linked belligerent or neutral territories?); whether in the event of a declared blockade action could be taken against cables (as if cable messages were equivalent to blockade-running ships or small boats); and whether neutral cables could be targeted for unneutral service if they carried enemy messages (not unlike a vessel carrying contraband).

The Institute for International Law, at its Brussels session in 1902, passed an important resolution on treatment of cables during war. This resolution effectively proposed three rules: (1) That cables connecting two neutral territories are ‘inviolable’; (2) that cables connecting two belligerents or two parts of the territory of a belligerent can be cut anywhere except in neutral waters; and (3) that cables connecting a belligerent with a neutral may be cut in the belligerent territorial sea, and—if a blockade is in place—also in the high seas. This resolution was highly influential on the 1913 Oxford Manual which was itself subsequently adopted by the Institute.

However, the Institute’s opinion was not universally accepted. Discussion at the US Naval War College (NWC) in 1902 concluded in respect of ‘neutral’ cables carrying enemy messages: (1) that if a blockade was in place, the cable could be cut because ‘the blockading belligerent can interrupt the cable as he

136 Heintschel von Heinegg (n 98) 295.
139 See eg ‘Imperial Cable Communications and Strategy, 1870–1914’ (1971) 86(341) The English Historical Review 728, 729; ‘International Law Situations: 1900 US Naval Code—Section 1—Hostilities’ (1903) 3 International Law Studies 13, 28–9; Report of the Interdepartmental Committee on Cable Communications, reported to Parliament on 26 March 1902 (Cd. 1056).
would a dispatch boat; (2) but that classifying the cable (or its traffic) as contraband was the least favourable legal approach, as it unnecessarily complicated the concept; and (3) that the cable was liable to be cut because it was an instrument of unneutral service. Contrary to the Institute’s approach, the discussants concluded that, ‘It is taken as a matter of general acceptance that cables will be cut in the high seas’, citing US and British doctrine and practice.

The NWC continued to consider the issue in 1903 in light of revisions to the 1900 US Naval War Code. By that time, the NWC took the view that the principle legal test was not the existence of a blockade on unneutral service, but military necessity. As a result, the proposed revision of Article 5 of the 1900 Code was that:

… (b) Submarine telegraphic cables between the territory of an enemy and neutral territory may be interrupted within the territorial jurisdiction of the enemy or at any point outside of neutral jurisdiction, if the necessities of war require.

(c) Submarine telegraphic cables between two neutral territories shall be held inviolable and free from interruption.

It was, however, the 1907 Hague Regulations Respecting the Laws and Customs of War on Land that furnished the most significant attempt to grapple with submarine cables. Article 54 states that:

Submarine cables connecting an occupied territory with a neutral territory shall not be seized or destroyed except in the case of absolute necessity. They must likewise be restored and compensation fixed when peace is made.

However, this obligation applies only to cables connecting territory occupied by a belligerent with neutral territory. Furthermore, this rule ‘applies only to activities on land and does not deal with seizure or destruction of cables in the open sea’.

In an attempt to provide further guidance, the 1913 Oxford Manual of the Laws of Naval War proposed a more detailed rule, largely following the 1902 Institute for International Law approach. In essence this held (also as Article 54): (1) ‘connecting the territories of the two belligerents’, or parts of the territory of one belligerent, could be targeted outside neutral waters; (2) a ‘cable

---

connecting a neutral territory with the territory of one of the belligerents’ could be cut only where strictly necessary and within a three-mile limit of a belligerent coastline or on the high seas under conditions of blockade; (3) the status of cables is not affected by the nationality of their owners; and (4) cables ‘connecting belligerent territory with neutral territory, which have been seized or destroyed, shall be restored and compensation fixed when peace is made’ not be cut in neutral waters.\footnote{146}

Nonetheless, John Hall—writing in late 1913—declared that very little had actually been agreed to that date. He held instead that ‘acts of war’ below the threshold of a confrontation between forces, ‘such as … the cutting of submarine cables’, remain ‘illegal in neutral waters’ even if those cables ‘connect two portions of enemy territory’.\footnote{147}

During WWI, the US view was clearly that cables linking a belligerent and a neutral were liable to be cut, in the high seas, with the test now being ‘the necessities of war’. The only cables immune from cutting were those connecting two neutrals.\footnote{148} Thus, Article 40 of the 1917 US Instructions for the Navy of the United States Governing Maritime Warfare indicates:

(b) Submarine telegraph cables between points in territory belonging to or occupied by the enemy and neutral territory may be interrupted within the territorial jurisdiction of the enemy or at any point outside of neutral jurisdiction, if the necessities of war require.

(c) Submarine cables connecting an occupied territory with a neutral territory shall not be seized or destroyed except in the case of absolute necessity. They must likewise be restored and compensation shall be fixed when peace is made.

(d) Submarine telegraph cables between two neutral territories shall be held inviolable and free from interruption.\footnote{149}

Following WWI, an interesting question arose concerning post-hostilities treatment of destroyed, or recovered and relaid, German submarine cables. As Pearce Higgins noted, the questions of law coalesced around ‘whether such cables were liable to be treated as prize or booty of war and whether their retention by the victors by way of reparation was in accordance with international law’.\footnote{150} The 1919 Treaty of Versailles dealt with German cables

\footnote{146} Oxford Manual of the Laws of Naval War, 9 August 1913, art 54 (the sub-paragraphs and italics have been added by the authors for ease of reference) \url{<https://ihl-databases.icrc.org/ihl/INTRO/265?OpenDocument>}.\footnote{147} JA Hall, The Law of Naval Warfare (Chapman and Hall 1914) 64.\footnote{148} Its view prior to entry into the war may have been different. See ‘Memorandum by the Counselor for the Department of State (Lansing) on Professor Hugo Münsterberg’s Letter to President Wilson of November 19, 1914’, in Papers Relating to the Foreign Relations of the United States (The Lansing Papers) 1914–1920 (Volume I), US Government Printing Office, Washington, 1939, 166–79.\footnote{149} Instructions for the Navy of the United States Governing Maritime Warfare, 30 June 1917, art 40 (emphasis added).\footnote{150} Pearce Higgins (n 131).
in Article 156 and Annex VII to the Treaty, essentially through compensation for private cables being credited to the German reparation account.\(^{151}\) Contrary to the 1913 Oxford Manual position, no reparation was made for seized or damaged State-owned cables. This outcome was no aid to clarity and by mid-century Columbos could reasonably observe that, as regards the rules applicable to cables in war, ‘there do not appear to be any very clearly ascertainable’.\(^{152}\)

This contradictory legacy of doctrine and practice has resulted in a lack of legally-binding guidance as to the treatment of cables under LOAC.\(^{153}\) As noted, UNCLOS itself does not address wartime concerns. Nor do technically-focused recommendations by the International Cable Protection Committee,\(^{154}\) and occasional activity by the International Telecommunication Union, advance our understanding of the position of undersea cables under LOAC.\(^{155}\) Additionally, the 1971 Seabed Treaty\(^{156}\) contains a non-prejudice clause as regards cables within national jurisdiction and says nothing specific about cables on the seabed in areas beyond national jurisdiction. That said, any use of high-seas cable infrastructure to support placing on the seabed structure or

151 Treaty of Peace with Germany (Treaty of Versailles), 28 June 1919.
155 The ITU does deal with submarine cable issues—see, for example the workshops on Enhancing access to submarine cables for Pacific Islands Countries <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events2017/Submarine%20Cable/submarine-cables-for-Pacific-Islands-Countries.aspx>; a summary of the outcomes of the meeting is at <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events2017/Submarine%20Cable/submarine-cables-for-Pacific-Islands-Countries/Submarine%20Cable%20Workshop%20Summary%20circulation.pdf>; however, ITU sponsored guidance on the security implications and security-focused regulation of submarine cables is scant—see, for example, the ITU-led publication Guide to Developing a National Cybersecurity Strategy: Strategic Engagement in Cybersecurity (2018), which does not refer to the undersea cable network <https://www.itu.int/dms_pub/itu-d/opb/str/STR-CYB_GUIDE.01-2018-PDF-E.pdf>. By comparison, there are several international agreements that cover registration, jurisdiction, cooperation, and offences in relation to space-based data assets such as the satellites regime for the 2100 satellites in near earth orbits: treaties, a UN Office of Outer Space Affairs, regular meetings on regulatory issues, and so on. There are also dedicated projects—such as the Woomera Manual—devoted to ascertaining how this body of law interacts with, inter alia, LOAC. Nothing of the same scope exists in relation to undersea data cables.
156 Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof 955 UNTS 115 (1971), art I(1): ‘The States Parties to this Treaty undertake not to emplant or emplace on the seabed and the ocean floor and in the subsoil thereof beyond the outer limit of a seabed zone, as defined in article II, any nuclear weapons or any other types of weapons of mass destruction as well as structures, launching installations or any other facilities specifically designed for storing, testing or using such weapons.’ See also J Kraska, *Maritime Power and the Law of the Sea: Expeditionary Operations in World Politics* (Oxford University Press 2011) 279.

https://doi.org/10.1017/S0020589322000227 Published online by Cambridge University Press
facilities specifically designed for storing, testing or using’ weapons of mass destruction would be prohibited.

D. More Recent Commentary on the Application of the Laws of War and Neutrality to Submarine Cables

The 1995 San Remo Manual on International Law Applicable to Armed Conflicts at Sea provides little additional guidance. Rule 37 states that ‘Belligerents shall take care to avoid damage to cables and pipelines laid on the sea-bed which do not exclusively serve the belligerents’, with the equally succinct commentary observing the importance of ‘protection of cables and pipelines laid on the sea-bed of all parts of the oceans’. Nevertheless, the rule ‘recognises … that cables or pipelines exclusively serving one or more of the belligerents might be legitimate military objectives’. Neither the provenance of, nor the justification for, the caveat that the cable ‘exclusively serve’ belligerents is explained; nor does the rule or commentary ‘adequately deal with undersea communication cables that are no longer “bi-polar”’. The San Remo Manual also deals with the targetability of an enemy merchant vessel engaged in cable cutting, declaring that such conduct may render that vessel a military objective.

Other sources on point similarly reflect a very thin regime in respect of the treatment of submarine cables in LOAC. Relevant military manuals tend to echo the sparse San Remo provisions, albeit with minor variations. The Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0 reiterates the narrow 1907 Hague Regulations rule, but also takes the view that ‘neutral cyber infrastructure located outside neutral territory, such as undersea cables, may be attacked if it constitutes a lawful military objective’. In the absence of a definitive and comprehensive statement of the law, it is therefore necessary to ask how high-seas cables might be dealt with under LOAC in terms of both status (neutral or belligerent), and character (military object or otherwise).

---

158 ibid 111 (emphasis added).
160 San Remo Manual (n 160) Rule 60(a).
163 ibid, 556—Rule 150, para 5.
E. Submarine Cables as Neutral Objects?

It has been suggested by some that the law of neutrality can no longer practically apply to submarine cables in order to protect them from belligerent use or attack on the one hand, nor impose duties upon neutrals to prevent their belligerent use on the other. However, the conclusion that belligerents may therefore both make unrestricted use of cables and attack cables serving neutrals is not one to be lightly reached given their importance. It is agreed that under conditions of modern warfare strict application of traditional concepts of neutrality would seem, to say the least, impractical. We no longer live in an age of bipolar cable connections when it was relatively ‘simple to conduct an analysis of whether a neutral State was affected by cutting a cable’. One possibility would be to suggest, *de lege ferenda*, that as a universal public good submarine cables should enjoy special protection from wartime damage as objectively neutral objects. There is, however, no realistic prospect of such a development in the law in the short term. It is therefore useful to attempt to assess the law, especially the law of targeting, as it presently stands.

A useful start point is to revisit the three rules as to geographic (and national) linkage proposed in the 1913 Oxford Manual. First, that submarine cables connecting two points within a belligerent’s territory may be cut at any point, including in the high seas. This rule is uncontentious and—as the historical survey above indicates—appears generally accepted. Second, a submarine cable connecting belligerent and neutral territory may be cut in the territorial sea of the belligerent but not in that of the neutral. This is consistent with the broader law of neutrality, mandating that neutral waters may not be used for belligerent activities. Third, a cable connecting belligerent and neutral territory may only be cut in the high seas where an effective blockade is in place (itself a separate legal test) and within the blockaded area of the high seas.

As noted, this third rule is directly descended from the Institute for International Law 1902 Resolution. It appears to treat the submarine cable as a ‘ship’ analogous to a merchant vessel seeking to breach the blockade. The parallel with a neutral merchant vessel is not entirely misplaced if one considers the cable to be breaching the blockade with its ‘cargo’ of

---

165 Tallinn Manual 2.0 (n 165) 556—Rule 150, para 5.
166 Kraska (n 164).
168 1907 Hague (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, art 2.
169 See eg 1856 Paris Declaration, art 4; San Remo Manual, Rule 95.
170 See below on Latifi’s use of this analogy in 1909.
171 See below on, *inter alia*, Stockton’s use of this analogy.
‘contraband’ information which the adversary may put to military use.\(^\text{172}\) By analogy one could then apply the permissive rule allowing attack of blockade-running merchant vessels. Here the only viable act against the cable would be to cut it.

However, the force of this analogy is reduced by other sub-rules that the Oxford Manual applied to cables linking neutral and belligerent territory. The first is that the attack on the cable—its cutting—had to be ‘on consideration of the restoration of the cable in the shortest time possible.’ No equivalent obligation applies to merchant vessels attacked or captured on the grounds that they breached a blockade. Indeed, such delinquent vessels, once condemned in prize (that is, once their capture has been ruled legal by an admiralty court), become the property of the capturing State and their loss is not compensable or recoverable.

The second sub-rule is that cutting a submarine cable brings with it a belligerent obligation that the cable ‘be restored and compensation fixed when peace is made’. \textit{Lex lata} this obligation only applies in respect of cables connecting neutral and occupied territory. No equivalent provision applies in the case of blockade-running ships. Divergent practice also casts doubt on any customary status the rule could claim. The Versailles Treaty approach has been noted above. Other instances are also ambiguous. As Pearce Higgins recorded,

\begin{quote}
Chile cut the British-owned cable connecting her territory with Peru in the war which ended in, 1883, but made compensation to the cable company. The United States, in 1898, found that military necessities required the cutting of the cables uniting Cuba, Porto Rico and Manila with the outer world (though neutral – British – owned), and compensation was refused to the Eastern Extension Telegraph Company for damage suffered from lawful acts of war.\(^\text{173}\)
\end{quote}

Finally, a test of ‘absolute necessity’ has sometimes been said to apply. Again, this obligation appears in Article 54 of the 1907 Hague IV Regulations. But as a matter of \textit{lex lata}, it is limited to the very discrete situation of a cable connecting occupied territory with that of a neutral, not the more general situation of a cable connecting adversary belligerent territory with a neutral. By definition, one cannot blockade occupied territory. ‘A blockade to be valid must be confined to ports and coasts of the Enemy’\(^\text{174}\), which occupied territory, for these purposes, is not. In sum, the apparent linkage between high-seas cable cutting and the law of blockade upon which the Oxford Manual explicitly posits has no \textit{lex lata} provenance.

Ultimately, however the limitation to situations of blockade is questionable simply because State practice is contrary. The US view has never required a blockade to be in place in order for high seas cutting of a belligerent-to-
neutral cable to be legitimate. Furthermore, Britain cut the five trans-Atlantic German cables (including Germany–US cables) on 3–4 August 1914, in advance of its declaration of a state of war at 2300 on 4 August 1914. Of note, that declaration did not refer to a blockade.

Further, the British naval blockade of Germany may not in fact have been formalised until an Order in Council of 20 August 1914, which specifically referred to ‘the existence of a blockade’. Similarly, Germany cut the Russia (enemy belligerent) to Bulgaria (neutral, until late 1915) Black Sea cable on 1 November 1914. The Germans had no blockade in the Black Sea at the time as they did not have the forces in situ to implement one. Finally, Peace Higgins felt secure in 1922 in declaring that: ‘The views held by most naval authorities to-day on the subject of blockade render such a limitation as that proposed impracticable.’

The conclusion to be drawn, arguably, is that the high seas cutting of cables connecting a belligerent and a neutral is permissible so long as the cable has become a military objective (in the same way as a delinquent merchant vessel becomes a military objective if it is employed to military advantage by the adversary). This is the long held US and UK view and (in WWI and WWII) practice, and the logic behind, inter alia, the Tallinn Manual 2.0 approach.

But this conclusion leaves unanswered the question of whether a submarine data cable that links two neutrals can be cut by a belligerent in the high seas. The 1917 US Naval Code maintained that this was impermissible; the 1995 San Remo Manual equivocates; the 2017 Tallinn Manual 2.0 simply applies the military objective test. In this respect historical context is important. The 1917 US Naval Code position was taken at time when entirely neutral telegraph cables were not generally a conduit for belligerent communications. (Hence Germany resorting to extensive wireless communications when its access to submarine telegraph cables was cut or required routing through British cable stations.) This said, however, there is evidence from WWI of British action against German attempts to reroute communications through

178 Privy Council, Order in Council, 20 August 1914, para 4: ‘The existence of a blockade shall be presumed to be known: (a) to all ships which sailed from or touched at an enemy port a sufficient time after the notification of the blockade to the local authorities to have enabled the enemy Government to make known the existence of the blockade, (b) to all ships which sailed from or touched at a British or allied port after the publication of the declaration of blockade…’; Supplement To The London Gazette, 22 August, 1914, 6673–74 <https://www.thegazette.co.uk/London/issue/28877/supplement/6674>; see also P Drew, The Law of Maritime Blockade: Past, Present, and Future (OUP 2017) 46–8; and Holland (n 174) paras 108–114.
179 Winkler (n 175) 856.
181 Pearce Higgins (n 131) 31.
entirely neutral cables (that is, cables that landed in neutral territory at both ends). Today, of course, cables as a matter of course carry all manner of traffic and it is practically certain that a cable connecting two neutral States might in a given situation carry belligerent military data and communications. In this case, the question needs to be answered. Can it be answered, as the Tallinn Manual 2.0 proposes, by asking whether a submarine data cable can be a military objective?

F. Submarine Cables as Military Objectives?

The primary use of submarine data cables is, of course, as a data transmission and access conduit. However, submarine cables have the potential to be employed as components of a weapons system, as a sensor system, or as command, control, and communication (C3) infrastructure. Such uses could include submarine cables as seismic detection infrastructure;182 as climate monitoring and data collection infrastructure;183 and as a dispersed facility for command and control over, and communications with, autonomous underwater vehicles.184 Such escalating securitisation of the submarine data cable network185 presages significant questions of characterisation under LOAC. That is, submarine data cables represent both military capabilities, and military vulnerabilities, beyond their primary role as data conduits. They are thus classic ‘dual use’ infrastructure which may potentially be either a ‘civilian object’ or ‘military objective’.

Since its adoption in API in 1977 the classic definition of ‘military objective’ has been:

… military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.186

It is clear that the use of submarine data cables could certainly make ‘an effective contribution to military action’ such that their cutting could offer ‘a definite military advantage’.

Early analysts reached similar conclusions by analogy. Thus Charles Stockton concluded cables were targetable in 1902 through an analogy with

185 Ross (n 127).
186 1977 Additional Protocol I art 52(2); San Remo Manual, Rule 40.
‘contraband of war’. In 1909, Latifi proposed that cables be conceptualised either as ‘ships’ (and thus treated as a neutral mail steamer is treated), or as a bridge connecting two territories and thus liable to attack on the same basis as a bridge under LOAC ashore. In an assessment closer to modern sensibilities, Pearce Higgins argued as early as 1922, that

... there appears ... no need for ‘bridge’ or ‘ship’ theories. Cables are a means which a belligerent has of keeping open his communications with the world. The great object of naval warfare is to stop the circulation of enemy commerce and to cut his means of communication, whether for the carriage of troops, property or intelligence, and cables are of the utmost importance for the last purpose.

This is arguably the correct approach: the extent of a cable’s contribution to enemy hostilities is key. This could range from simple transmission of military data (making it as targetable in the same manner as ordinary communications infrastructure ashore), through to more advanced uses as C3 infrastructure for at-sea military systems, or as sensor systems facilitating detection of enemy platforms or activities.

To some extent, therefore, this is in fact the easiest question to answer: Yes, submarine cables can be military objects; furthermore, they have in fact historically been treated as such both in doctrine and practice. The more challenging query then is the final one: Could an attack on a submarine data cable today ever not be disproportionate?

G. Proportionality in Attack on Submarine Cables?

At present, the submarine cable network constitutes fundamental and critical global critical infrastructure. It carries, ‘In a single day... some $10 trillion of financial transfers and process[es] some 15 million financial transactions’. Cable communication also makes the coordination of complex global manufacturing supply chains possible. As one analyst has observed, ‘Even though there are hundreds of cables crossing the global seabed, there are just not enough ... redundancies available to handle the vast amount of
bandwidth needed to keep global banking transactions in check. As we have discussed, the impacts of cable cutting would extend well beyond financial damage. Many public and private organisations are dependent on cloud-based applications and data storage for their ordinary functioning. The loss of access to patient data or software used to schedule surgery or treatment could lead to harm and loss of life. Additionally, the compounding effect of cutting multiple cables is not merely arithmetic:

As the amount of cable disruptions increases (ie, more cables are cut) … the amount of data traffic that is lost increases exponentially… For example, an analysis was done of possible disruptions of the cable lines connecting Europe and India. It found that although ‘India is fairly resilient in the case of one or two cable disruptions’, nearly seventy percent of traffic to and from India would be lost with just three concurrent cable disruptions.

Redundancy is also critical. For example, if all of the Pacific and Atlantic Ocean cables landing in the US ‘were suddenly cut, only seven per cent of the US traffic could be restored’ using satellites. Network interruptions at scale can and have had social, commercial, and political consequences beyond mere delay. In June 2017, for example, ‘the anchor of a container ship accidentally cut the only [submarine cable] linking Somalia to the world Internet … for more than three weeks’ resulting in economic losses estimated at ‘more than 10 million dollars a day’. Assessing the proportionality of civilian damage in the case of infrastructure attacks can be complex. But the scale of damage likely to be wrought in the case of cable cutting is of a different order. Consequently, while ‘belligerents regularly snipped enemy cables during World War II’ to sever today’s ‘fibreoptic lines without affecting a much larger and more interdependent system’ would be exceptionally difficult, ‘making a potential attack all the more damaging’. Could such an attack ever be proportionate?

The doctrinal approach to proportionality focusses upon the language of Additional Protocol I (API) Article 57(2)(a)(iii). The belligerent should...
‘refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated’. This test applies equally to targeting submarine cables. This follows either because they are an example of an attack from or at sea that affects the civilian population ashore under API, or because customary law effectively imposes the same test.

The question whether the cutting of a submarine data cable can today meet the proportionality test cannot be answered on the basis that it was considered permissible in the past. The answer must now consider the criticality of the cable network to modern global life. This may be, however, a difficult assessment to conduct. Before turning to that question it is important to recall one caveat, namely the Hague IV Regulations rule regarding ‘submarine cables connecting an occupied territory with neutral territory’: these ‘shall not be seized or destroyed except in the case of absolute necessity’. Such cases are governed by the law of occupation and it will be this test of ‘absolute necessity’, not proportionality, which applies.

Setting occupation to one side, the final answer to the proportionality question needs to take into account three difficult assessments. The first of these concerns the questions of fact to be resolved on a case-by-case basis. One of these is the ability of the commander to be satisfied that the particular cable being considered for targeting carries enemy data or provides enemy capability. In this sense, it will be highly relevant to the ‘military necessity’ evaluation if the cable in question has capabilities beyond simply serving as a data conduit. Evidence that the cable is used for other military purposes—such as sensor systems, or C3 of military systems at sea—will speak to the targetability of such cables. Thus, if cable X is known to provide military sensor data, this will be significant. Conversely, where the commander does not have sufficient information upon which to base an assessment—for example, good reason to believe that the routing system is employing a specific cable as the data transmission conduit for the adversary’s military communications—this will weigh heavily against cable X being a military objective.

Another challenging factual assessment is the extent to which redundancy in the submarine cable network may mitigate the effects from cutting a particular cable (either in terms of achieving a military objective or for the civilian population). If, for example, cutting cable X will have minimal military

---

203 1977 Additional Protocol I, art 49(3): ‘The provisions of this Section apply … to all attacks from the sea or from the air against objectives on land …’; AP I Commentary para 1898: ‘The provision of this paragraph has the advantage of clearly establishing the fact that attacks from the sea or from the air against objectives on land are subject to the restrictions and conditions imposed by the Protocol.’
effects because the adversary is able to quickly reroute data traffic through other cables but disruption to civilian users who do not have such capabilities, the attack may well be disproportionate. Any commander considering the proportionality of cutting a submarine data cable would be remiss in not asking for intelligence on this issue. Indeed, it might be that cable cutting fails a proportionality assessment precisely because in order to achieve anything close to the intended effect—for example, degradation of enemy communications—one would have to commit to systemic cutting of cables resulting in cascading effects for both belligerent and neutral civilian populations.

The second set of challenging assessments are of a more theoretical and legal nature. Nonetheless, a commander would need to resolve them before ordering an attack. The first of these is the extent to which tests of ‘absolute necessity’, and obligations of restoration ‘in the shortest time possible’ reflect narrowly applicable treaty law obligations, as opposed to attempts to lay out general principles de lege ferenda. The requirement for ‘absolute necessity’ certainly appears in the 1907 Hague VI Regulations; but, as noted, that rule applies only to cutting cables originating in occupied territory. Otherwise, proposals for a general test of ‘absolute necessity’ such as that of the 1913 Oxford Manual do not appear to have been taken up in State practice or military manuals. This contrary State practice and doctrine weighs heavily against any general rule of ‘absolute necessity’ having passed into custom.

The third challenging assessment is the broader debate as to the place of second-order—but foreseeable—effects upon assessing civilian harm/collateral damage under the proportionality test. As regards cable cutting, this will be critical. It is the civilian consequences that will almost inevitably follow—economic chaos, social and political dislocation, information gridlock—that represent the most deleterious effects. Indeed, the cutting of cables that land in a belligerent’s territory no longer simply affects that belligerent; the transmission effects are felt much more widely by the global community of users including, for example, the ability of users to even access their own data in cloud storage. Consequently, ‘reliable access to [the] cloud is not merely important—it is critical [for individuals and businesses]. The concerns … are thus two-fold: the security of the data itself and the security of our access to that data.’

As (inter)dependence upon the submarine cable network increases, commanders will be faced with the question of how to quantify such readily foreseeable second-order effects and factor them into proportionality assessments prior to cable cutting. One counterargument could be that such a calculation involves a difficult, even

205 Heintschel von Heinegg (n 98) 292 n 6; Assertions of a higher threshold than simple proportionality are not foreign to LOAC—permission for targeting a specially protected vessel such as a hospital ship (eg San Remo Manual, Rules 49-51) can require the application of a second level of additional tests beyond the proportionality test alone.

206 Hantover (n 9) 2–3.
impossible exercise, due to the extremely widespread and unpredictable nature of those consequences. It is argued that any such conclusion militates against the attack being legal.

V. CONCLUSION AND WAYS FORWARD

The more than 2000 communications satellites currently in geosynchronous or geostationary orbit are subject to a much more fully elaborated regime of governance than submarine cables. Given the much greater economic, social and security significance of undersea data cables, it is anomalous that there is no coherent body of law that comprehensively assigns rights, roles and jurisdictions regarding the protection of undersea cables. At present, policymakers must rely on the piecemeal scheme constructed by amalgamating instruments such as the freedom to lay submarine cables in the 1982 Law of the Sea Convention, the outdated 1884 Convention for the Protection of Submarine Telegraph Cables, technical recommendations by the International Cable Protection Committee, and soft law access guidelines promulgated by (inter alia) the International Telecommunication Union. While some gaps regarding damage to be cables may be filled by novel, but in the view of the authors entirely tenable, progressive development of the transboundary harm principle or interpretation of the law of piracy, the situation remains unsatisfactory – though less unsatisfactory, perhaps, than has been presumed.

Unfortunately, the law regulating the use (or destruction) of cables in wartime is in no better shape; indeed, it is in worse. This article has surveyed historic efforts at LOAC rule-making in relation to cables. Paths based on analysis of cable-specific rules have been found to be dead ends.

The critical question then becomes the application of general principles of LOAC—what constitutes a military objective and proportionality in attack—to these specific facts. Given that cutting submarine cables can, inter alia, inhibit communications and halt UAV activities, it is clear they can make ‘an effective contribution to military action’ and could be legitimate military objectives. Consequently, the key issue is whether such action could satisfy the proportionality test. It is suggested that any application of this test will

207 For example: Convention on Registration of Objects Launched into Outer Space, 1023 UNTS 15 (1974), and the UN Office for Outer Space Affairs Register of Objects Launched into Outer Space (http://www.unoosa.org/oosa/en/spaceobjectregister/index.html).

208 See, inter alia: Rose (n 127); Sunak (n 127); Davenport (n 16); R Martinage (n 127); Ross (n 127); Hantover (n 9); Wrathall (n 127); Damico (n 127).

209 UNCLOS, at inter alia arts 19, 21, 58, 87, 112–115.

210 Convention for the Protection of Submarine Telegraph Cables 1884, arts 2, 5–6, 8–10.

always come back in the negative. This is because the combination of the scale of impact on civilian social and economic infrastructure, and the likelihood of this damage spreading beyond the targeted State to neutral third States, means such an attack could only be excessive in relation to any military advantage. This conclusion is grounded in the interconnected nature of the Internet through submarine data cables, and the sheer extent of foreseeable civilian harm that would result. This is not overstatement. As discussed, redundancy and rerouting could require systemic cable cutting to achieve a desired military outcome with any degree of efficiency. This would result in even more widespread, if not global, effects for civilian populations in both belligerent and neutral territories. When all of these consequences are considered it is close to impossible for any military advantage gained to be considered proportional to the widespread collateral damage that would occur. Thus, it is concluded that the severing of submarine data cables, while theoretically permissible under LOAC and the law of naval warfare, is functionally unlawful.