UNDERWATER COMMUNICATION CABLES:

VULNERABILITIES AND PROTECTIVE MEASURES RELEVANT TO INDIA

PART-2

Soham Agarwal & Vice Admiral Pradeep Chauhan
08 April 2021

This is the second and concluding part of an article on submarine communications cable systems relevant to India. Part-1 focussed upon providing an overview of these systems and the vulnerabilities to which they are subject. This concluding segment not only highlights the inadequate protection that these systems receive under international law but also under India's domestic legislation. To mitigate the several ensuing vulnerabilities, it strongly recommends that submarine communications cables landing in India be included within India's "Critical Information Infrastructure System" (CIIS), and that India exercise prescriptive jurisdiction over such submarine cables even under the High Seas, under the principle of "protective jurisdiction". It is hoped that the two parts, taken in aggregate, would be useful to Indian policy-makers and practitioners, as also to legal academic and research institutes in India and the larger Indian Ocean Region. This second part specifically addresses legal authorities of the Indian Navy/Ministry of Defence, the Ministry of External Affairs, as well as India's national security apparatus.

Protection under International Law

Where legal protection to underwater/ submarine communication cables is concerned, the basic issue revolves about the exercise of "jurisdiction". While surveillance, alerting and warning systems are necessary to prevent human activity from damaging cables in the first place, the existence and robustness of rules and enforcement mechanisms required to ensure deterrence are equally important. However, since much of the damage can occur outside the territory of the concerned State, extending a State's jurisdiction, especially criminal jurisdiction, is problematic.

Submarine cables (albeit in the form of telegraph cables) have, of course, been around since the 1850s. As early as 1884, the international community understood the need to reach a consensus to protect these cables even in areas outside national jurisdiction. Thus, the *"Convention for the Protection of Submarine Telegraph Cables, 1884"*[1] focussed upon interference with telegraph cables. The jury is still out on whether this treaty has a fundamental norm-creating

[1] "Convention for the Protection of Submarine Telegraph Cables, Paris, 14 March 1884", https://cil.nus.edu.sg/wp-content/uploads/2019/02/1884-Convention-for-the-Protection-of-Submarine-Telegraph-Cables-1.pdf

character and whether it has the force of customary international law.[2] The non-reliance of many articles in the 1884 Convention by the International Law Commission while developing UNCLOS 1982, as also the small number of signatory State Parties are strong arguments against it.[3] The Convention is nevertheless important as it is applicable *"outside territorial waters to all legally established submarine cables landed on the territories... of one or more of the High Contracting Parties"*[4] and hence sets a precedent for the exercise of jurisdiction. Article 2 of this Convention made the breaking or injury of a submarine cable, done wilfully or through culpable negligence that results in partial or total interruption in telegraphic communication, a punishable offence. While Article 8 of the Convention adheres to the principle of Flag State jurisdiction by providing competence to take cognizance of the offence, to the Flag State of the vessel aboard which the infraction took place, Article 10 empowers other High Contracting Parties to collect evidence for violations of this Convention and transmit them to the Flag State.

The attribution of jurisdiction was, however, slightly altered with the coming into force of the 1982 UNCLOS, due to the newly created/clarified maritime zones and the rights within these zones, which were afforded to coastal States. The coastal State has sovereignty in its Territorial Sea and is competent to enact rules and regulations to protect submarine cables within its Territorial Sea (Article 21(c) UNCLOS). The jurisdiction of the coastal State in the Exclusive Economic Zone (EEZ), however, is limited to the exercise of 'sovereign rights' with respect to the exploration and exploitation of resources. Therefore, the coastal State may restrict only such activities within its EEZ over which it has jurisdiction. This has been used effectively by Australia and New Zealand by creating 'cable protection zones' in which certain activities are restricted in an area declared as such with respect to identified submarine cable(s). Schedule 3 of the Telecommunications Act (Australia), *inter alia*, prohibits anchoring and the use of trawls and other fishing gear designed to work on the seabed, within these 'cable protection zones'. This has been done to prevent bottom fishing or any such activity in these areas that may cause damage to a submarine cable. Similarly, Section 12 and Section 13 of the *"Submarine Cables and Pipelines Protection Act, 1996"*[5] of New Zealand, empower the Governor-General to declare an area — including within the EEZ — a 'protected area' within which fishing operations and anchoring of a ship is an offence. In this way, a common cause of damage to submarine communication cables has been sought to be addressed.

However, the issue of intentional human damage does not get addressed by this measure. UNCLOS, 1982, does provide for measures for the protection of submarine cables on the High Seas but affords jurisdiction to the Flag State of the vessel/nationals that effect the protection. Article 113 of the UNCLOS, in terms similar to those of the 1885 Convention, obligate the Flag State exercising jurisdiction over nationals/vessels to adopt laws and regulations necessary to provide that the breaking or injury of a submarine cable below the high seas, or any conduct calculated or likely to result in such breaking or injury, done wilfully or through culpable

---

[2] Wolff Heintschel von Heinegg, "Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine communications Cables under International Law', in Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, ed. Katharina Ziolkowski (Tallinn 2013 NATO CCD COE Publication), 297.

[3] Heinegg, "Protecting Critical Submarine Cyber Infrastructure", 297

[4] 1884 Convention for the Protection of Submarine Telegraph Cables, Article 1

[5] Submarine Cables and Pipelines Protection Act 1996 (New Zealand)

negligence, is a punishable offence if it obstructs telegraphic or telephonic communications. Article 58(2) UNCLOS extends this provision and makes it applicable within the EEZ as well.

This notwithstanding, there has been very poor compliance, with this provision, with the majority of States, including the Republic of India, not having enacted any comprehensive domestic legislation to this effect. Even a liberal reading of the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA)[6] would, at a minimum, require *"Flag State authorisation"* and give preference to *"Flag State jurisdiction"*.[7] It would appear that submarine cables fall into a legal gap and are left inadequately protected, particularly in the absence of vigorous measures to enact domestic legislation.

It is also not clear whether the State that owns the cables or the nationals of the State(s) which own or have laid the cables, can exercise jurisdiction (criminal or otherwise) over cables laid on the seabed under the high seas. It is quite doubtful, therefore, whether they would be able to enforce their own national laws over an incident damaging 'their' submarine cables in Areas Beyond National Jurisdiction (ABNJ).

Alternative Bases of Jurisdiction

Solutions to this problem of the protection of submarine communications cables laid on the seabed under the high seas may, perhaps, be more readily found in alternative bases of attributing jurisdiction. Jurisdiction essentially concerns the extent of each State's right to regulate the conduct or the consequences of events.[8] Currently, under UNCLOS, the right to regulate an incident on the High Seas rests with the Flag State of the perpetrator. However, it is questionable whether this confers exclusive jurisdiction to the Flag State. Is no other State competent to exercise jurisdiction, especially when the Flag State has not exercised their jurisdiction by enacting laws and regulations to that effect? This is a vital question that needs to be squarely and urgently addressed.

The extra-territorial application of the laws of a State was addressed in the MV *Lotus* case,[9] which made clear the proposition that a State may exercise its jurisdiction only within its territory, i.e., 'enforcement jurisdiction', but there is nothing prohibiting a State from extending the application of its laws and jurisdiction of their courts to persons, property, and acts outside their territory, i.e., exercising its 'prescriptive jurisdiction'.[10] Therefore, a State may, if it so wishes, extend its laws to persons and acts outside its territory but may only enforce them within its territory. This principle has been refined to require a 'linking point' or connecting factor between the act to be legislated and the legislating State.[11] These connecting factors are the recognised 'bases of jurisdiction' in international law.

---

[6] Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Done at Rome, 10 March 1988 (entry into force: 1 March 1992)
[7] Heinegg, "Protecting Critical Submarine Cyber Infrastructure", 314
[8] Christopher Staker, "Jurisdiction" in International Law (ed.) Malcolm D. Evans (Oxford: Oxford University Press, 2014), 316
[9] *SS Lotus* (France vs Turkey) 1927 PCIJ (Ser A) No 10
[10] *SS Lotus* pp 18-19
[11] Alan V. Lowe, "*International Law"* (Oxford University Press 2007)

The recognised bases of jurisdiction of particular interest to this scenario are the "passive personality", the "protective principle", and the "universality principle".

Passive Personality

The principle of "passive personality" draws from the principle of nationality. It holds that sovereign States have a right to extend their laws over their nationals and have the prerogative to define the scope of 'nationality'. States have, in the past, ascribed nationality to offshore oilrigs on the basis of the State of registry.[12] Therefore, it is possible that submarine cables too could be brought under the scope of this principle and 'nationality' may also be ascribed on the basis of the nationality of ownership of the cables. Unfortunately, however, the ascertaining of nationality over private and consortium-based ownership is riddled with significant complexities. As explained earlier, it is difficult to ascertain the ownership of cables under consortium ownership. If the SEA-ME-WE 4 (Serial 6 of **Table 1** in Part 1 of this article refers) is cut in the Mediterranean Sea, but all that TCL owns is the cable and landing station in Indian territory, a nationality claim would probably not suffice for the exercise of prescriptive jurisdiction. Even though the Government of India has a 26.1% stake in TCL (which it is, in any case, in the process of divesting),[13] establishing nationality over TCL would not amount to establishing nationality over the Mediterranean Sea portion of the cable. Under the private ownership model, too, the establishment of nationality is at the mercy of complicated corporate ownership structures. For instance, FALCON-1 (see Serial 8 of **Table 1** in Part 1 of this article), which lands in Mumbai, is not directly owned by Reliance Communications (an Indian registered entity). Instead, it is owned by Global Cloud Xchange, which is a wholly owned subsidiary of Reliance Globalcom BV (registered in Netherlands), which itself is a wholly owned subsidiary of Reliance Communications.[14] Therefore, establishing Indian nationality in this case would be a significantly convoluted process that would give rise to multiple competing jurisdictions. Perhaps the promotion of public-private partnerships within the ownership of cable systems may be effective in addressing this issue.[15]

Protective Principle

In some States, but not yet in India, the "Protective Principle" has been recognised as a legitimate exercise of a State's prescriptive jurisdiction when the vital interests of a State are threatened, even if such a threat is posed by non-nationals outside the territory of the State.[16] What constitutes 'vital interests' is not an exhaustive list, but it does, nevertheless, have some limited scope for expansion.[17] The United States has utilised this principle to extend jurisdiction

---

[12] Staker, "Jurisdiction" 320
[13] Reeba Zachariah, "Tatas' stake in Tata Communications will rise to 59%", *The Times of India,* 18 March, 2021 https://timesofindia.indiatimes.com/business/india-business/tatas-stake-in-tata-comm-will-rise-to-59/articleshow/81557327.cms
[14] Beryl Menezes, "Global Cloud Xchange announces debut in international capital markets" *Live Mint* 25 July, 2014 https://www.livemint.com/Companies/pZPQeC0F7sQhbxqwgkkVVL/Global-Cloud-Xchange-announces-debut-in-international-capita.html
[15] See Sechrist, "*Cyberspace in Deep Water*" for more details.
[16] Staker, "Jurisdiction", 321
[17] Staker, "Jurisdiction", 321

to tackle drug trafficking on the High Seas as it considers such trafficking to be an attack on vital American interests. In the US Court of Appeals, 11th Circuit Judgment of US vs Gonzales[18], the arrest of six crew members aboard a Honduran vessel in the High Seas for the possession of a controlled substance under US legislation was not held to be an *ultra vires* exercise of American jurisdiction. However, it may be pertinent to note that a crucial factor was the consent (albeit verbal) taken by the US authorities from the Flag State (Honduras) to board and arrest their nationals. It is clear that here, too, Flag State authorisation does play a role but only to the extent of permitting the boarding of the vessel and the arrest of the crew. This, too, comes within the scope of the enforcement jurisdiction of a State. It has been argued, especially within the USA, that the US was competent to exercise "prescriptive jurisdiction" even without the consent of the Flag State.

Thus, protection to submarine cables too could (and should) be afforded under the protective principle, at least until States build consensus to ascribe "universal jurisdiction", i.e., one in which all States have jurisdiction (as in the case of piracy) for the protection of submarine cables, due to the sheer value of submarine cables to the international community as a whole. There has been growing regional cooperation to address this issue. An example is that of the Indian Ocean Commission (IOC) working with United Nations Office for Drug Control (UNODC), where the responsibility of UNODC could possibly indicate a push towards ascribing "universal jurisdiction", in order to draft a Submarine Cables Protection and Resilience Plan to "promote international law and best practices in the region".[19]

However, the 'vital interests' position needs to be reflected within national law to justify its vital nature, not least due to the restrictive pressure on increasing the scope of the term. This pressure is why the USA has sought to adopt the "effects doctrine" to exert jurisdiction and prosecute economic effects felt in the US for acts committed by non-nationals abroad, rather than opting for the "protective principle".[20]

The UN General Assembly Resolution 58/199[21] on the protection of critical information infrastructure, too, recognises that each country has the right to determine its own critical infrastructure. Likewise, a recent experts-meeting of the UNODC concludes that designating submarine cables as critical communications infrastructure and supporting national and international legislation to criminalise wilful or grossly negligent damage, are, indeed, the next logical steps.[22]

---

[18] *US vs Gonzales* 776 F.2d 931 (1985)

[19] "Key actions to protect submarine cables from criminal activity identified at UNODC global expert meeting", United Nations Office on Drugs and Crime, accessed 17th March 2021 https://www.unodc.org/easternafrica/en/Stories/protection-of-submarine-cables-in-indian-ocean.html

[20] See Anindita Jaiswal, "Effects Doctrine in India versus the US: Developing & Developed Country Perspectives" *Manchester J Int'l Econ L* 12, 2015 for detailed examination of the effects doctrine.

[21] General Assembly resolution 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* A/RES/58/199 (30 January 2004) available on undocs.org/en/A/RES/58/199

[22] "Protecting submarine cables in the Indian Ocean", United Nations Office on Drugs and Crime Eastern Africa News and Stories, accessed on 17 March 2021 https://www.unodc.org/unodc/en/frontpage/2019/February/key-actions-to-protect-submarine-cables-from-criminal-activity-identified-at-unodc-global-expert-meeting.html

Regrettably, while India does have a Critical Information Infrastructure (CII) structure, submarine cable systems have not yet been made a part of it.

India's Critical Information Infrastructure (CII)

India's CII derives its status, protection, and authority from the *"Information Technology Act 2000"* (ITA).[23] Article 70 of the ITA authorises the *"appropriate Government"* to declare by notification, any *"computer resource"* that directly or indirectly affects *"the facility of CII"*, a *"protected system"*. The 'Explanation' to this Section defines CII as any 'computer resource' the incapacitation of which shall have a debilitating impact on national security, economy, public health or safety.
A "computer resource" under Section 2 (k) of the ITA is defined as a *"computer, computer system, computer network, data, computer database or software"*. These terms have been further individually defined.

Section 2 (j) of the ITA [inserted in 2009 via an amendment] defines a 'computer network' as the: *"inter-connection of one or more computers or computer systems or communication device through:*

(i) the use of satellite, microwave, terrestrial line, wire, wireless, or other communications media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device"

Section 2 (l) of the ITA defines a "computer system" as a *"device or collection of devices including output and input support devices…which contain computer programs…input data and output data that performs…data storage and retrieval, communication control and other functions"*.

It is unclear whether submarine communications cables would fall under the definition of a computer network, and therefore, a 'computer resource' for the purposes of being classified as a CII. While the cable landing stations may well fall under the ambit of a 'computer system', the use of the term 'terrestrial' line would seem to exclude submarine cables. Submarine cables could, on the other hand, albeit under a very broad interpretation, be included within the term 'wire', owing to the physical 'wires' in the cables.

The other alternative is to interpret the whole cable system as a terminal or a complex consisting of two or more interconnected communication devices. This, too, would be a matter of interpretation because there is no explicit recognition as such. Further, there is an issue as to whether the status as a CII needs to be notified. Section 70 of the ITA requires a *"protected system"* that *"affects the facility"* of a CII to be notified. It is unclear whether a CII is a distinct category from a protected system, and whether it is only the latter which needs be officially notified.

The National Critical Information Infrastructure Protection Centre (NCIIPC), which is the national nodal agency notified on 16th Jan 2014 by the Central Government under Section 70A of the ITA,[24] has released guidelines on the identification and protection of CII. However, these guidelines do not even once use the term 'protected system' but, instead, use the expression,

[23] Information Technology Act 2000 (India) https://www.meity.gov.in/content/information-technology-act-2000-0
[24] "About us", National Critical Information Infrastructure Protection Centre, accessed 17 March 2021 https://nciipc.gov.in/

'protected CII'.[25] Further, the definitions of CII elaborated in the guidelines seem to hinge on the *"impact of any sudden failure or outage on our national wellbeing or national security"*. They also seem to include information infrastructure (defined in guidelines as the totality of inter-connected computers and networks and information flowing through them) that support operations of critical sectors. Five broad 'critical sectors' that have been recognised are:[26]

- Power & Energy
- Banking, Financial Institutions & Insurance
- Information and Communication Technology
- Transportation
- E-Governance and Strategic Public Enterprises

Since submarine cables are the lifeline of these sectors, it is intuitively a CII and should be declared as such. However, in somewhat sharp contrast to the Australian domestic legislation alluded to earlier in this article, this has yet to be done in specific terms. The benefits that would accrue from such a designation is that the protection of these submarine cables would come within the ambit of the NCIIPC, which has a mandate to facilitate protection of CII. There would then be a dedicated agency looking to highlight and advocate for the protection of vulnerabilities of submarine cables. It is pertinent to note that Rule 4(5) of the *"Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013"* makes it clear that the basic responsibility of protecting the CII system shall be with the agency running the CII. The role of the NCIIPC is research, policy-guidance and expertise-sharing with the agency responsible for protection. Therefore, it promotes Public-Private synergy in protection of these cable systems.

The *"Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018*" further prescribes rules and best practices for private agencies running these systems, such as the appointment of an "Information Security Steering Committee" with representatives of the organisation, NCIIPC and experts. Therefore, the State would be invested in the protection of these cables.

Further it would bring submarine cables under Section 66F of the ITA, which prescribes life imprisonment as a penalty for the damage inflicted to a CII, as the infliction of such damage is classified as an act of 'cyber terrorism'. This would be a substantial development from the present provisions in the Indian Telegraph Act 1885 which in section 25 stipulates meagre penal provisions of imprisonment for three years or fine for wilful or negligent damage to telegraphs. Only the former truly reflects the gravity of the offence.

---

[25] "Guidelines for the Protection of National Critical Information Infrastructure", National Critical Information Infrastructure Protection Centre, (New Delhi January 2015)
https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf
[26] Saikat Datta, "The NCIIPC and its evolving framework", *Digital Debates: The CyFy Journal* (2016)
https://www.orfonline.org/expert-speak/nciipc-its-evolving-framework/#_edn3

Concluding Recommendations

It is a matter of utmost priority for the NCIIPC to advise the central government to notify the submarine cable system and bring it within the CII system of India, thereby affording it better protection and enabling the possibility of extra-territorial application of Indian law.

The government should also enact specific legislation for the protection of these cables by identifying 'cable protection zones' and exercising Flag State jurisdiction by penalising wilful or culpably negligent acts aboard Indian vessels that damage submarine cables.

It is important for this study to now move to its next stage of examining comparative legislation obtaining in the various States of the Indian Ocean Region, as well as those of the Indo-Pacific, on the subject of underwater communication cables. Such a comparison should be undertaken specifically in order to draw out best practices that can then be contextualised to India, so as to generate a first-draft of an Indian piece of legislation that would address this vital facet of 'maritime India'.

This is what the NMF would be undertaking, hopefully in conjunction with other leading academic, legal and strategic institutions of the country.

About the Authors

Soham Agarwal holds a Bachelor of Law (Honours) degree from the University of Nottingham, UK, and is currently undergoing a two-year B.A. LLB Bridge Course programme at the National Law University, Delhi. Having completed a twelve-week intensive internship at the National Maritime Foundation (NMF), he has developed a strong passion for Public International Maritime Law and is now an Adjunct Research Associate (ARA) at the NMF. He may be contacted at soham.agarwal.email@gmail.com

Vice Admiral Pradeep Chauhan, AVSM & Bar, VSM, IN (Retd), is the Director-General of the National Maritime Foundation (NMF). He is a prolific writer and a globally renowned strategic analyst who specialises in a wide-range of maritime affairs and related issues. He may be contacted at directorgeneral.nmfindia@gmail.com