# CHAPTER 14

## SAFEGUARDING INDIA'S SUBMARINE CABLES

Divya Rai

*Connectivity is the new geography*

— Parag Khanna, *Connectography*, 2016

### Introduction

In the Indo-Pacific's evolving strategic landscape, the contest for digital dominance is playing out beneath the sea.[1] Submarine cables—carrying 95% of the world's international data—form the unseen backbone of the global economy,

DOI: 10.71236/QAXD6468 

financial systems, and military communications. As states seek to control information flows and assert influence in the digital domain, these cables have emerged as critical infrastructure and strategic targets.

India stands at the center of this high-stakes environment. Its geographic position in the Indian Ocean Region is at the crossroads of vital global data routes, linking Europe, Southeast Asia, and the Middle East. India's ambitions to become a global digital hub are accelerating through projects such as the 2Africa Pearls, India-Asia-Express (IAX), and India-Europe-Express (IEX) submarine cable systems. These initiatives will significantly expand its bandwidth capacity and deepen its integration into the world's digital economy.[2] But with this opportunity comes heightened vulnerability—and responsibility.

Recent sabotage incidents—from the Nord Stream pipeline attacks to cable disruptions in the Red Sea—underscore the emergence of undersea infrastructure as a new frontier in geopolitical competition. A growing concern in the strategic landscape is the potential for seabed warfare. In particular, the weaponization of seabed assets, including by state-backed actors operating in legal gray zones, highlights the fragility of global connectivity.[3] India's limited repair capabilities and reliance on foreign-owned infrastructure expose a critical gap at a time when secure, resilient communications are paramount to national power.

The chapter explores the strategic importance of India's submarine cable network within the broader context of Indo-Pacific competition. It examines the composition and vulnerabilities of these systems, identifying gaps in international and domestic legal protections, and evaluates India's current infrastructure posture and the importance of Quad initiatives on cable repair partnerships. Most importantly, it outlines a roadmap for India to transform its submarine cable ecosystem—from a soft target to a pillar of strategic advantage. Through legal reform, alliance coordination under its SAGAR initiatives,[4] and domestic capability development, India can assert itself as a rule-shaper in securing the Indo-Pacific's digital arteries.

## Strategic Stakes in Subsea Connectivity

The global submarine cable network, spanning nearly 1.5 million kilometers (km) beneath the oceans, forms the digital foundation of 21st-century power.[5] These cables carry nearly $10 trillion in daily financial transactions and enable virtually all international traffic.[6] From global banking to real-time intelligence sharing, their uninterrupted function underpins modern economies, diplomacy, and defense.

Control over these digital arteries is increasingly viewed as a strategic advantage. The system's physical fragility—where a single severed cable can disrupt millions of lives—starkly contrasts its critical importance. As states and private

actors race to build, secure, and influence subsea routes, the geopolitical significance of cable networks has surged.

India's role is central. Positioned at the maritime crossroads of Asia, its waters host vital east-west data routes that connect Europe, the Middle East, Southeast Asia, and beyond. This location gives India more than connectivity—it gives it leverage. Whether through economic interdependence or digital deterrence, India's stewardship of submarine cable infrastructure is becoming a decisive factor in the Indo-Pacific security architecture.

## India at the Crossroads of Digital Power

India's geographic position at the heart of the Indian Ocean gives it more than geographic relevance—it grants strategic leverage in the global competition over digital infrastructure. With east-west data cables converging off its coasts, India serves as a digital fulcrum between Europe, West Asia, Southeast Asia, and East Asia. This convergence makes Indian waters a critical artery in the global data bloodstream—and a potential point of failure if left unprotected.

The stakes are rising. India's major undersea cable initiatives, including 2Africa Pearls and India-Asia-Express (IAX) systems, and India-Europe-Express (IEX), are not merely infrastructure projects—they are instruments of economic ascendancy and strategic signaling. Both cable systems are owned by Reliance Jio, where the IAX connects Chennai and Mumbai with major Southeast Asian hubs

including Singapore, Thailand, and Malaysia. The IEX connects with France, Greece, Saudi Arabia, Egypt, and Djibouti. These systems will elevate India as a primary conduit for intercontinental data flows, reinforcing its value to global tech giants, regional governments, and security coalitions alike.

But with strategic centrality comes strategic risk. As cable volume increases in Indian territory, so does exposure to sabotage, espionage, and disruption. India's credibility as a digital power will increasingly rest on its ability not just to expand cable capacity but also to secure it.

Through mechanisms like the Quad, India is beginning to translate its geographic advantage into strategic influence, pushing for norms, partnerships, and infrastructure resilience in a contested domain. To understand how India can protect this emerging edge, it is first necessary to examine the cables themselves—their structure, fragility, and the actors who build and maintain them.

## Beneath the Surface: Anatomy of a Strategic Vulnerability

Despite appearing impervious from the surface, submarine cables are physically fragile. Just 70 to 210 millimeters in diameter—no thicker than a garden hose—these fiber-optic lines carry enormous volumes of data across continents.[7] Bundles of glass strands, thinner than human hair, transmit light pulses that enable everything from international banking

to secure military communications. Insulated and armored, the cables vary in thickness depending on water depth and proximity to human activity.

To maintain signal strength, repeaters—optical amplifiers—are embedded every 40 to 80 kilometers along the cables route.[8] These devices, critical to long-distance transmission, are among the system's most sensitive components and require uninterrupted power and precise calibration.

Despite these protections, submarine cables remain vulnerable to both environmental and deliberate interference. Their complex construction makes them expensive to produce, challenging to install, and even harder to repair. The very factors that make them essential to global function—submerged location, long-distance span, and reliance on specialized hardware—also render them soft targets in a world of intensifying competition below the surface.

## Who Owns the Seafloor? Strategic Control in the Cable Industry

While submarine cables are global assets, their development, ownership, and maintenance are controlled by a narrow group of powerful players. Historically led by Western telecommunications firms, the landscape is now being reshaped by a new breed of actors—private tech giants and strategic state-backed companies.

As of 2021, four companies accounted for 98% of global submarine cable production and installation:[9] SubCom (U.S.), Alcatel Submarine Networks (France), Nippon Electric Company or NEC (Japan), and HMN Technologies (China).[10] The latter, formerly Huawei Marine, has raised alarm among Western security officials for its deep integration into China's Digital Silk Road strategy. In this concentrated market, supply chain security and geopolitical influence are inseparable.

Meanwhile, private tech firms are becoming digital superpowers in their own right.[11] Amazon, Google, Meta, and Microsoft now own or lease over 50% of global subsea bandwidth,[12] making them both infrastructure providers and strategic actors in global governance. Their growing control over global information flows reflects a deeper shift, where dominance in the digital economy increasingly depends on physical infrastructure beneath the oceans.

India's major contributors—Tata Communications, Reliance Jio, Bharti Airtel, and Bharat Sanchar Nigam Limited or BSNL—remain dependent on foreign manufacturing and repair capabilities. This reliance, combined with the absence of a domestically flagged cable repair fleet, exposes India to strategic coercion and operational delays in the event of a crisis.

India's path to strategic autonomy in the digital domain will require more than investment—it will demand ownership, industrial capacity, and trusted partnership. As great powers

race to harden and weaponize the digital commons, India must treat undersea cable sovereignty as a pillar of national security.

## The Strategic Gap: Repair as a Measure of Resilience

Owning cable infrastructure is only half the equation: maintaining and repairing it swiftly under stress is what defines a state's digital resilience. Submarine cable repairs are technically complex, financially costly, and time sensitive. Each kilometer of cable costs $30,000 to $50,000 to lay,[13] and a single repair can run between $1 million and $3 million.[14] These operations require specialized ships and highly trained crews—assets that only a handful of countries possess.

Globally, cable repair capabilities are concentrated in nations with longstanding maritime infrastructure and industrial depth: France, Japan, Singapore, the United Arab Emirates, the United States, and the United Kingdom.[15] Their vessels – often stationed across multiple ports – enable rapid response to disruptions that could cripple financial systems, delay military communications, or destabilize public services (Table 14.1).

Table 14.1: Global Submarine Cable Repair Ships and Their Base Ports

| Country of Registration | Base Port | Cable Ship Name |
|---|---|---|
| **Canada** | Halifax, Nova Scotia, Canada | IT Integrity |

| | | |
|---|---|---|
| **France** | Worldwide | Ile de Batz, Ile de Brehat, Ile de Sein |
| | La Seyne sur Mer, France | Raymond Croze, René Descartes |
| | Calais, France | Ile d'Aix |
| | Cape Town | Léon Thévenin |
| | Mindelo, Cape Verde | Peter Faber |
| | Brest, France | Pierre de Fermat |
| **Indonesia** | Jakarta, Indonesia | Ile de Re, Teneo, Wave Venture |
| | Batam, Malaysia | Cable Empowered |
| **Japan** | Yokohama, Japan | KDD Ocean Lin, Subaru |
| | Moji Port, Kita-Kyushu, Japan | KDD Pacific Link |
| | Worldwide | KDDI Cable Infinity |
| **Marshall Islands** | Baltimore, MD, USA | Decisive, Dependable, Durable, Responder |
| | Noumea, New Caledonia | Reliance |
| | Taichung, Taiwan | Resolute |
| **United Arab Emirates** | Abu Dhabi, UAE | CS Maram, CS Wasel, Etisalat, Niwa, Umm Al Anber |

| | | |
|---|---|---|
| **United Kingdom** | Worldwide | Cable Innovator |
| | Portland, UK | CS Global Symphony, CS Recorder, Sovereign |
| | Curacao, Netherlands | Wave Sentinel |
| **United States** | Portland, Oregon, USA | Global Sentinel |
| **Singapore** | Colombo, Sri Lanka | ASEAN Explorer |
| | Singapore | ASEAN Protector, ASEAN Restorer |
| | Batangas, Philippines | Cable Retriever |
| **Antigua and Barbuda** | Worldwide | MV Aniek, MV Layla, MV Lida |
| **Malaysia** | Port Klang, Malaysia | Cable Orchestra |
| | Keelung, Taiwan | Lodbrog |
| **Philippines** | Manila, Philippines | PLDT |

Source: International Cable Protection Committee. "Publications," updated August 14, 2024, https://www.iscpc.org

India, by contrast, owns no cable repair ships flagged or stationed domestically. In the event of a cable break near its shores, India must wait for foreign vessels to reroute, sometimes taking days or weeks. During the 2008 Mediterranean cable disruption, this lack of readiness led to an 80% loss of India's international internet capacity, affecting

more than 60 million users.[16] Therefore, threats to India's communication infrastructure is a timely reminder of the critical value of India-flagged and -crewed submarine cable repair ships.

These cables face risk not only at sea or on land, but also in cyberspace. This vulnerability is not merely logistical—it is strategic. In a gray-zone crisis, where attribution is murky and timelines are compressed, delayed repairs can translate into economic dislocation, diplomatic weakness, and military disadvantage.

Similarly, cyberattacks against network management systems that oversee cable infrastructure could give hackers a kill switch to the connectivity of entire regions. India's ambition to be a digital power cannot rest on borrowed tools. Without sovereign repair capacity, the country risks ceding control over its most critical communications infrastructure.

Building a domestic cable repair fleet and regional repair protocols is not just a technical upgrade—it is a strategic imperative in an era where time, access, and economy determine advantage.

## Exposed Lines: The Strategic Vulnerability of Submarine Cables

Power in the digital era flows not only through trade routes and air corridors, but also through glass fibers under the sea. Submarine cables carry almost all international data traffic, yet

their physical structure and geographic routing make them among the softest targets in the global infrastructure.[17]

Natural hazards like earthquakes, volcanic activity, and submarine landslides account for less than 10% of all documented cable faults. The remainder is overwhelmingly man-made.[18] International Cable Protection Committee (ICPC) records from 1959–2022 attribute about 87% of faults to human activity, with anchoring and fishing alone responsible for nearly 40%. A further 48% are logged as "unspecified,"[19] yet industry audits reveal most of these cases also involved accidental human interaction, such as stray dredges, trawls, or dragged anchors.

These statistics expose the vulnerability of India's cable corridors—especially the crowded approaches to Mumbai, Chennai, and Kochi—where intense trawling, dredging, and commercial shipping converge on key landing stations.

More alarming is the rise in deliberate interference,[20] a gray-zone tactic that seeks strategic effect without triggering overt conflict. Bangladesh's nationwide blackout in 2007, triggered by the severing of its lone international cable, offered an early warning.[21] Since then, similar probes have struck the South China Sea, the Taiwan Strait (where Chinese vessels allegedly tampered with links to the Matsu Islands),[22] the Baltic Sea, and in 2022, the Asia-Africa-Europe 1 (AAE-1) system.[23]

The tempo increased in 2023–2024, when suspected state-

backed Chinese and Russian vessels targeted fiber lines and the Balticconnector gas pipeline, employing anchor-dragging and GPS spoofing to mask their operations. These incidents show seabed warfare evolving into a multi-domain contest that mixes advanced sensors, unscrewed submersibles, and information operations to hold critical infrastructure at risk.

India's position at the nexus of regional connectivity magnified both its opportunity and its exposure. Most of its cables land in at three sites; a coordinated strike on any one node could cripple financial transactions and international communications. Limited route diversity and the absence of a domestic cable-repair fleet.

Safeguarding this infrastructure will require more than passive defense. Adversaries are increasingly willing to exploit these weak points for strategic leverage, signaling the urgent need for enhanced surveillance, international coordination, and resilient infrastructure against hybrid threats. It also demands proactive legal reform, all of which are now essential elements of the national security strategy in a contested Indo-Pacific.

### Law Beneath the Waves: Gaps in the Legal Armor

International law for submarine cables was drafted for the age of Morse code, not for the terabit traffic that now powers the global economy. The 1884 Paris Convention[24]—the first instrument to address undersea wiring—treated a cable cut as an inconvenience to telegram delivery, not a threat to financial

markets or military command and control.[25] Almost a century later, the 1982 United Nations Convention on the Law of the Sea (UNCLOS) updated the script by affirming the right to lay and maintain cables in exclusive economic zones (EEZ) and on the high seas,[26] while obliging flag States to police vessels flying their flag (Art. 94), punish willful damage (Art. 113), and exercise penal jurisdiction over maritime incidents, including cable damage (Art. 97).[27] UNCLOS was a considerable advance—but it still framed cables as commercial convenience, not strategic terrain.

This framing is now badly outdated. UNCOLS offers no doctrine to address hybrid or gray-zone coercion, and no mechanism for tackling sabotage executed from the victim's shoreline. It omits three elements modern security planners need most: (1) explicit protection in armed conflict, (2) clear rules for attributing and prosecuting non-state proxies, and (3) enforcement tools that reach beyond the narrow lens of flag-state jurisdiction.

Attribution illustrates the problem. Under the customary rules codified by the International Law Commission, a state is responsible for a private actor's misconduct only if that actor exercises "governmental authority" under domestic law, operates under the state's "instructions, direction, or control," or has its deed formally "adopted" by the state after the fact.[28] These are intentionally high thresholds, and sophisticated saboteurs know how to stay below them—masking intent behind leased trawlers, rented remotely operated vehicles, or

spoofed AIS tracks. The evidentiary gaps that frustrate criminal courts also blunt diplomatic response, allowing hostile actors to deny culpability long enough for the strategic effect to sink in.

Jurisdictional limits deepen the vulnerability. UNCLOS Article 113 assigns prosecutorial authority solely to the vessel's flag State and to the saboteur's State of nationality. If either government lacks the will or capacity to act, the investigation stalls and the countries that actually suffer the outage are become powerless spectators. This narrow prosecutorial aperture—coupled with the fact that many States Parties have never transposed Article 113 into domestic law—means that most cases never reach court. Even where statutes exist, they often track back to the 1884 Cable Convention and top out at modest fines, a penalty grossly inadequate with the billions of dollars a prolonged data blackout can erase.

Territorial waters offer no safe haven. UNCLOS rules in the 12-nautical-mile zone, territorial seas, hinge on whether sabotage renders a vessel's passage "non-innocent," a test that fits poorly when a through-running trunk line merely skirts the coast without serving it. A hostile actor can therefore damage a transit cable and still claim the protection of innocent passage, leaving coastal states unsure whether they may interdict, arrest, or simply protest.

Multilateral efforts to patch these defects have inched forward but delivered little. The International Law Association created a Submarine Cables and Pipelines Committee in

2018;[29] several UN General Assembly resolutions[30] and a 2019 UN Office on Drugs and Crime (UNDOC) experts meeting have warned of rising criminal threats, yet all remain non-binding and lack operational follow-through.[31] In this normative vacuum, state and proxy vessels increasingly employ gray-zone tactics—anchor dragging, AIS spoofing, remotely operated vehicles—to create rivals without crossing the legal threshold of armed attack.[32]

Nowhere is the risk-reward calculus starker than for India. Sitting astride the Indo-Pacific's data crossroads, it gains leverage from every new landing but also exposes itself to cascading disruptions. Closing the legal gap is therefore more than a compliance exercise; it is a strategic imperative. By championing tougher bilateral accords, pressing for a Quad-led cable security regime, and modernizing its own statutes with extraterritorial reach and meaningful penalties, New Delhi can both shield its networks and position itself as a rule-setter in a stronger era when the boundary between peace and conflict runs along the ocean floor.

## India's Legal Framework: Still Under Construction

India aspires to be the Indo-Pacific's digital fulcrum, yet the legal scaffolding supporting that ambition is incomplete and inconsistent. Responsibility for undersea cable security is scattered across a quartet of statutes drafted for other purposes. The Maritime Zones of India Act (1976) asserts general jurisdiction at sea but offers no cable-specific safeguards. The

Information Technology Act (2000) tackles cybercrime while ignoring the physical infrastructure that carries India's data. The Suppression of Unlawful Acts Against Safety of Maritime Navigation Act (2002) could, in theory, be applied to sabotage, but in practice, it rarely is.[33] Finally, the Telecommunications Act (2023) modernizes licensing rules without classifying cables or landing stations as critical infrastructure or prescribing strategic measures.[34]

This regulatory lag has real-world consequences. India's undersea cable landing points – clustered in Mumbai, Chennai, and Kochi – serve as high-value digital nodes, yet they remain legally indistinct from other infrastructure. In the absence of clear mandates, jurisdictional ambiguity can delay response, hinder coordination, and limit deterrence.

This patchwork has tangible costs. Most of India's 17 international landings are concentrated in Mumbai, Chennai, and Kochi—high-value targets that remain legally indistinguishable from ordinary commercial frameworks.[35] No statute grants extraterritorial reach to prosecute foreign saboteurs, clarifies agency roles during hybrid attacks, or synchronizes domestic response with alliance partners such as the Quad. Nor does current law streamline the thicket of pre-repair and post-repair clearances that private operators must secure from separate ministries.

The absence of a Critical Information Infrastructure (CII) designation for cables further weakens deterrence. Without CII status, landing stations fall outside India's highest tier of

cybersecurity monitoring and response and receive no priority for intelligence support or armed protection. The Telecom Regulatory Authority of India (TRAI) has already recommended an end-to-end, single-window procedure for cable installation and maintenance; until that reform is enacted, bureaucratic friction will remain a strategic liability.[36]

India's network is growing faster than the laws that govern it. New systems such as the India-Europe-Xpress (IEX) and India-Asia-Xpress (IAX) will extend the country's reach across three continents, just as domestic demand approaches one billion users.[37] Unless legislation evolves to match this scale, by consolidating statutory authority, introducing robust penalties, granting extraterritorial jurisdiction, and embedding cable security in multilateral agreements, New Delhi's digital rise will rest on fragile legal grounds. A forward-looking strategy must therefore combine streamlined permitting, indigenous repair capacity, CII designation, and alliance-based contingency planning. Only then can India transform its undersea arteries from soft targets into pillars of national power in an increasingly contested Indo-Pacific.

## Strategic Roadmap: From Vulnerability to Advantage

India's digital rise depends on transforming its undersea cable network from a latent vulnerability into a strategic asset. No longer mere technical infrastructure, submarine cables are now contested terrain—vital to national power and regional

influence. Safeguarding them requires a deterrence architecture grounded in three pillars: denial (through redundancy and rapid repair), detection (via persistent seabed awareness), and response (through legal, diplomatic, and coercive means). The roadmap below outlines a phased approach across three horizons, sequencing actions that build toward long-term resilience and regional leadership.

*Immediate Priorities (0–2 Years):*
*Fortify the Foundation*

1. **Designate Cables as Critical Infrastructure**

   Classify submarine cables and landing stations as CII under the IT Act of 2000. This enables priority protection, expedited prosecution of sabotage, and integration into national cyber defense strategy.

2. **Operationalize the Quad Repair Partnership**

   Move beyond summit statements. Translate the 2024 Quad Cable Connectivity and Resilience Partnership into actionable protocols: prepositioned spares, cross-trained repair crews, and joint repair exercises across the Indo-Pacific.[38]

3. **Formalize Partnerships with Big Tech**

   Hyperscale cloud firms—Google, Amazon, Meta, Microsoft—own and operate the majority of global undersea cable capacity. India should formalize

partnerships with these actors for co-investment, real-time threat sharing, and coordinated recovery plans.

4. **Charter an Indian-Flagged Repair Vessel**

   Establish a domestically flagged, India-based cable repair capability via public-private financing. Even one vessel slashes reliance on foreign operators, ensures sovereign repair response, and demonstrates India's strategic seriousness.[39]

5. **Establish a National Cable Security Center**

   Centralized responsibility for cable threat intelligence, incident response, and legal coordination under a new unit housed within the National Critical Information Infrastructure Protection Centre (NCIIPC). Empower it to lead domestic and international coordination. [40]

6. **Deploy Underwater Domain Awareness Systems**

   Adopt a robust Underwater Domain Awareness (UDA) framework, which is essential for effective monitoring and defense of the seabed.[41] Deploy a multi-platform detection network—combining AI-powered seabed sensors, UUVs, and satellite-linked data buoys—enabling rapid detection of anchor drags, ROV incursions, and sabotage attempts within minutes.[42] Seabed-to-Space Situational Awareness (S3A) will define the future of defensive operations, making real-time situational awareness the first line of deterrence.

*Medium-Term Goals (2–5 Years):*
*Expand Reach and Influence*

7. **Create Cable Protection Zones**

   Gazette no-anchor, no-trawl zones around high-risk cable corridors and lading sites. Modeled on Australian practices, CPZs reduce accidental damage and impose political friction on would be gray-zone actors.

8. **Geographically Diversify Cable Landing Points**

   Reduce chokepoint risk by expanding cable landings beyond Chennai and Mumbai to locations like Kochi, Trivandrum, and Tuticorin. Geographic dispersions insulate the network from single-point failure.[43]

9. **Secure Government Representation in ICPC**

   India's voice at the International Cable Protection Committee (ICPC) must go beyond corporate representation. Government delegates can shape global norms, influence enforcement standards, and drive international reforms.[44]

10. **Integrate Cable Security in Regional Dialogues**

    Make undersea infrastructure protection a standing item in Quad, ASEAN, and IORA security forums.[45] Deepen links with Australia's Cable Connectivity and Resilience Centre and push for region-wide

information-sharing and crisis coordination mechanisms.[46]

*Long-Term Strategic Investments (5+ Years): Cement Strategic Autonomy*

**11. Develop a Full-Capable Domestic Repair Fleet**

India must possess an Indian-flagged cable repair vessel—not just for resilience but to signal strategic independence, as it will provide it with the capability to respond swiftly to any cable disruptions.[47] This fleet would also enable India to use repair vessels as a diplomatic tool under SAGAR policy to assist Indian Ocean littoral countries and friendly states as part of its broader Indo-Pacific engagement.

**12. Enact a Comprehensive Cable Security Act**

Codify a modern, deterrent-oriented legal framework. The statute should mandate redundancy planning, define cable-related crimes, clarify public-private roles, and authorize extraterritorial pursuit of foreign saboteurs.

This roadmap is not a checklist—it is a strategic transformation agenda. India's future as a digital hub depends not just on connectivity, but on control. The seabed is a new frontier of national security. By acting decisively, India can shape Indo-Pacific norms, deter malign actors, and

demonstrate that infrastructure security is central to sovereignty in the 21st century.

## Conclusion: Securing the Backbone of Digital Power

Submarine cables are no longer invisible infrastructure. They are contested terrain—critical to economic continuity, national security, and geopolitical signaling. As digital interdependence deepens, so too do the threats: accidental damage, hybrid attacks, sabotage, and espionage by state-backed actors.

For India, the stakes are escalating. As it rises as a central node in the global digital network, legal ambiguity, technical gaps, and operational dependencies are no longer acceptable. The 2008 internet blackout and the absence of a domestic repair fleet exposed the cost of underpreparedness. In today's more volatile landscape, the consequences of inaction would be far greater.

Yet the challenge brings opportunity. India has the scale, capacity, and partnerships to not only secure its own cable infrastructure but to shape global norms for submarine cable protection. Strategic advantage will come not from exclusive ownership, but from enabling faster, more secure deployment and maintenance—by harnessing the capabilities of operators, leveraging international best practices, and accelerating zone-based protections using experienced, specialized crews.

By formally designating cables as critical infrastructure and embedding cable resilience into alliances such as the Quad, India can transform digital fragility into strategic strength. Securing the seabed is not just a technical task—it is a geopolitical imperative.

In an Indo-Pacific defined by competitive multipolarity, the contest for control beneath the waves will shape the balance of power above them. The state that can detect, defend, and deter threats to connectivity will wield outsized influence.

India possesses the geography, the momentum, and the mandate. What remains is action—bold, coordinated, and sustained—to convert vulnerability into resilience, and resilience into regional leadership.

## Endnotes

[1] This chapter, originally titled "Safeguarding Submarine Cables: Strategic Measures for India's Security and Connectivity," was first published in *The Indo-Pacific Mosaic: Comprehensive Security Cooperation in the Indo-Pacific,* edited by James M. Minnich (2025), https://doi.org/10.71236/CKNT3185. The current version has been updated and retitled for this volume, the first in the *Strategic Edge Series*.

[2] "Big Boost for India's Internet Quality! Three Large Undersea Cable Projects to Expand Capacity by More Than Four Times," *The Times of India*, August 21, 2024, https://timesofindia.indiatimes.com/business/india-business/big-boost-for-indias-internet-quality-three-large-undersea-cable-projects-

to-expand-capacity-by-more-than-four-times/articleshow/112672969.cms.

3 International Cable Protection Committee. "Publications," updated August 14, 2024, https://www.iscpc.org/publications/.

4 SAGAR (Security and Growth for All in the Region) is India's policy initiative for maritime cooperation in the Indian Ocean Region (IOR).

5 TeleGeography, "Submarine Cable Frequently Asked Questions," accessed September 27, 2024, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

6 TeleGeography, "Do $10 Trillion of Financial Transactions Flow Over Submarine Cables Each Day?," April 6, 2023, https://blog.telegeography.com/2023-mythbusting-part-1.

7 Yifang Electric Group Inc., "What is a Submarine Cable? What are the Types? How to Laying?," December 9, 2022, https://www.yifangcable.com/what-is-a-submarine-cable-what-are-the-types-how-to-laying/.

8 TeleGeography, "Submarine Cable FAQs."

9 Pioneer Consulting, "Suppliers of Undersea Telecommunications Systems: Executive Summary," March 2021, https://www.pioneerconsulting.com/wp-content/uploads/2021/03/Pioneer_Consulting_Suppliers_Report_Executive_Summary_Download.pdf.

10 Daniel F. Runde et al., "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition," *CSIS*, August 16, 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

11 Submarine Cable Own by: (1) Google - 16790.3 km (internationally) and 10,2362.325 km in consortium with Facebook, Amazon, and Microsoft; (2) Facebook - 92873.6 km; (3) Amazon - 30556.61 km; (4) Microsoft - 6604.76 km.

[12] "Submarine Cables Market Size, Share & Trends Analysis Report by Application (Submarine Power Cables, Submarine Communication Cables), by Voltage, by End-user, by Offerings, by Component, by Region, and Segment Forecasts, 2023–2030," Grand View Research, accessed September 27, 2024, https://www.grandviewresearch.com/industry-analysis/submarine-cables-market.

[13] R. L. Gallawa, "Estimated Cost of a Submarine Fiber Cable System," NTIA-Report-81-59, U.S. Department of Commerce, January 1981, https://its.ntia.gov/publications/download/81-59_ocr.pdf.

[14] "345 kV Submarine Cable - Preliminary Cost Estimate," Hatch, September 16, 2015, https://novascotia.ca/nse/ea/aulds-cove-transmission/Appendix_J_Submarine_Cable_Estimate.pdf.

[15] International Cable Protection Committee (ICPC), "Cableships of the World," updated February 11, 2022, https://www.iscpc.org/information/cableships-of-the-world/?items=0.

[16] "Submarine Cable Cuts in Jan-Feb, 2008 in the Persian Gulf and the Mediterranean," Submarine Cable Networks, March 18, 2011, https://www.submarinenetworks.com/en/nv/news/cable-cuts-in-jan-feb-2008.

[17] Runde et al., "Safeguarding Subsea Cables."

[18] Stephen C. Drew and Alan G. Hopper, *Fishing and Submarine Cables: Working Together*, 2nd ed. (International Cable Protection Committee, February 23, 2009), https://www.iscpc.org/documents/?id=142.

[19] Mike Clare, "A Publication from the International Cable Protection Committee (ICPC): Submarine Cable Protection and the Environment," *ICPC*, March 2021, https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf.

[20] Jill C. Gallagher, "Undersea Telecommunication Cables: Technology Overview and Issues for Congress," CRS Report 47237,

*Congressional Research Service*, September 13, 2022. https://crsreports.congress.gov/product/pdf/R/R47237.

[21] Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, Cath. U. J. L. & Tech 24 (2015), https://scholarship.law.edu/jlt/vol24/iss1/4.

[22] Elisabeth Braw, "China is Practicing How to Sever Taiwan's Internet," *Foreign Policy,* February 21, 2023, https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/.

[23] Thomas Claburn, "Cable Cut Blamed for Global Four-Hour Internet Disruption," *The Register*, June 7, 2022, https://www.theregister.com/2022/06/07/global_internet_disruption/.

[24] *International Convention for the Protection of Submarine Telegraph Cables*, Submarine Telegraph Act, 1885, https://www.legislation.gov.uk/ukpga/Vict/48-49/49.

[25] National Oceanic and Atmospheric Administration, "Submarine Cables - International Framework," updated April 15, 2024, https://www.noaa.gov/general-counsel/gc-international-section/submarine-cables-international-framework.

[26] United Nations (UN), *United Nations Convention on Law of the Sea*, 1982, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

[27] UN, *United Nations Convention on Law of the Sea*.

[28] Tara Davenport, *Intentional Damage to Submarine Cable Systems by States*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2305 (October 26, 2023), https://www.hoover.org/sites/default/files/research/docs/Davenport_finalfile_WebReadyPDF.pdf.

[29] International Law Association, *Submarine Cables and Pipelines Under International Law [Third] Interim Report 2024*, https://www.ila-hq.org/en/documents/ilathi-1.

[30] United Nations General Assembly (UNGA) Resolution, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructure*, A/RES/58/199, January 30, 2004, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf. UNGA Resolution, *Oceans and the Law of the Sea*, A/RES/66/231, https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_66_231.pdf; "Submarine Cables: A Crucial Infrastructure for India," *ETV* Bharat, June 13, 2024. https://www.etvbharat.com/en/!opinion/submarine-cables-a-crucial-infrastructure-for-india-enn24061305815.

[31] United Nations Office on Drugs and Crime (UNODC), "Key Actions to Protect Submarine Cables From Criminal Activity Identified at UNODC Global Expert Meeting," accessed September 24, 2024, 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.

[32] Jason Petty, "How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea," *Chicago Journal of International Law* 22, no.1 (2021): art. 18, https://chicagounbound.uchicago.edu/cjil/vol22/iss1/18.

[33] AK Harbola, "Submarine Cable Security-Jurisdiction and Legalities." Defence Research and Studies, June 1, 2023, https://dras.in/submarine-cable-security-jurisdiction-and-legalities/.

[34] The Gazette of India, *The Telecommunications Act, 2023,* December 24, 2023, https://egazette.gov.in/WriteReadData/2023/250880.pdf.

[35] Telecom Regulatory Authority of India (TRAI), "Recommendations on Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India," June 19, 2023,

https://www.trai.gov.in/sites/default/files/2024-08/PR_No.54of2023.pdf.

[36] TRAI, "Recommendations on Licensing Framework.

[37] "India's Three Subsea Cable Projects to Go Live By 2025," *India Briefing News*, August 28, 2024, https://www.india-briefing.com/news/india-three-subsea-cable-projects-launch-march-2025-34116.html/.

[38] Press Information Bureau (PIB). "Fact Sheet: 2024 Quad Leaders' Summit", September 22, 2024. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2057460.

[39] Telecom Regulatory Authority of India (TRAI), "Recommendations on Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India 19th June 2023

[40] TRAI, *International Telecommunication Access to Essential Facilities at Cable Landing Stations Regulations, 2007* (5 of 2007), Chapter 1, Section 2 (u): Definitions, https://www.trai.gov.in/sites/default/files/Regulation_07june07.pdf.

[41] Arnab Das, "Underwater Domain Awareness (UDA) Framework," Maritime Research Centre (MRC), and M/S NirDhwani Technology Pvt Ltd (NDT), n.d., accessed May 21, 2025, https://maritimeresearchcenter.com/wp-content/uploads/2024/04/Underwater-Domain-Awareness.pdf.

[42] Syeda Fizzah Shuja "Beneath the Surface: The Strategic Implications of Seabed Warfare." Daily Sabah, December 2, 2024. https://www.dailysabah.com/opinion/op-ed/beneath-the-surface-the-strategic-implications-of-seabed-warfare.

[43] Samuel Bashfield. "Digital Sovereignty: Securing India's Submarine Cables", The Diplomat, December 26, 2024. https://thediplomat.com/2024/12/digital-sovereignty-securing-indias-submarine-cables/.

[44] Brendon J. Cannon and Pooja Bhatt, "The Quad and Submarine Cable Protection in the Indo-Pacific: Policy Recommendations,"

*Institute for Security & Development Policy (ISDP)*, January 25, 2024, http://isdp.eu/wp-content/uploads/2024/01/Brief-Cannon-Jan-25-2023-final3-updated.pdf.

45 Cannon and Bhatt, "The Quad and Submarine Cable Protection."

46 "Cable Connectivity and Resilience Centre," Australian Government, accessed September 26, 2024, https://www.dfat.gov.au/international-relations/regional-architecture/quad/cable-connectivity-and-resilience-centre.

47 TRAI, "Recommendations on Licensing Framework."