International Journal of Applied Social Science
(An International Double Blind Peer Reviewed / Refereed Research Journal of Social Science)
Volume 13 (5 & 6), May & June (2026) : 751-761
Received : 29.04.2026; Revised : 15.05.2026; Accepted : 29.05.2026

RESEARCH ARTICLE
ISSN : 2394-1405 (Print)
DOI : https://doi-ds.org/doilink/08.2026-31335693/IJASS/13.5&6/751-761

Chokepoints, Repair, and Rules: The Vulnerability Politics of India's Submarine Cable Order

RISHABH MAHAN
Doctoral Candidate
Centre for European Studies, School of International Studies
Jawaharlal Nehru University, New Delhi (India)

ABSTRACT

Submarine cable politics becomes legible at the moment of breakdown. Cuts near Jeddah in September 2025 and in the Red Sea in early 2024 disrupted traffic between Asia and Europe and briefly made an invisible infrastructure a matter of public policy. Taking failure as its method, this paper reconstructs the vulnerability profile of India's cable order along three axes: physical fragility, arising from the concentration of fifteen of roughly seventeen international systems on one Mumbai beach and from the absence of an Indian-flagged repair vessel; geopolitical exposure, arising from dependence on the Suez, Bab el-Mandeb, and Hormuz corridors; and domestic regulatory constraint, arising from clearance procedures that lengthen repair. China's PEACE cable serves as a controlled contrast in which financing, manufacture, ownership, and operation are held within a single national system, and the comparison indicates that the vertically integrated and the networked architectures generate different capabilities and different failure modes rather than a ranking. Against projected bandwidth growth of 38 percent a year, the analysis suggests that resilience, not capacity, is the binding constraint, and that sovereign repair, dispersed landings, and single-window clearance are the measures on which the credibility of the strategy rests.

Keywords: Submarine cables, Critical infrastructure, Chokepoints, Resilience, Repair capacity, Cable governance, India

INTRODUCTION

Two of the world's busiest undersea cables were cut near Jeddah on 6 September 2025, slowing internet speeds in India, Pakistan, and the United Arab Emirates and obliging Microsoft to reroute Azure cloud traffic until the severed links could be repaired the following day (Insikt Group, 2025)[1]. The episode was not isolated. Damage to AAE-1, EIG, and SEACOM in the Red Sea in early 2024 affected roughly a quarter of traffic between Asia and Europe, and the operator reporting the figure described the simultaneous interruption of four systems as unprecedented (HGC Global Communications, 2024)[2]. Events of this kind carry more analytical value than their duration suggests, since they render visible a system that ordinarily disappears into the background of everything built on top of it.

Roughly 99 per cent of intercontinental data traffic moves along fibre-optic cables laid on the ocean floor (International Telecommunication Union, 2025; Starosielski, 2015). India's exposure to that layer is unusually concentrated. About seventeen international

1. The one-day restoration was unusually quick and reflects proximity to an available repair vessel and a shallow-water fault location. It should not be read as typical, since deep-water faults in contested waters have taken substantially longer to address.

2. The share is an operator estimate issued during the disruption rather than a measured figure, and it refers to traffic affected by rerouting rather than to traffic lost. Independent verification of estimates of this kind is rarely possible.

How to cite this Article: Mahan, Rishabh (2026). Chokepoints, Repair, and Rules: The Vulnerability Politics of India's Submarine Cable Order. *Internat. J. Appl. Soc. Sci.,* **13** (5 & 6) : 751-761.

systems serve the country, fifteen of which come ashore within a six-kilometre stretch of Versova beach in Mumbai, with Chennai as the secondary gateway (Khanna, 2025). Singapore, on 733 square kilometres of territory, hosts twenty-six systems across three separate landing sites. The chairman of the Telecom Regulatory Authority of India observed at the first International Subsea Cables Conference in 2025 that the country held about one per cent of the world's cable landing stations and required many more (Khanna, 2025)[3].

Breakdown is treated here as a method rather than as an anecdote. Following Star's (1999) observation that infrastructure becomes visible on failure, the analysis works backwards from disruption to the structural conditions that make disruption consequential, and asks what those conditions imply for policy. Three questions organise the account. The first concerns the composition of India's vulnerability, disaggregated into its physical, geopolitical, and regulatory components. The second concerns what the comparison with a vertically integrated architecture reveals about the failure modes of a networked one. The third concerns which of the announced governance responses would change the vulnerability profile and which would leave it intact.

The argument is that India's cable order has been built for capacity and is now constrained by resilience. Landings, fibre pairs, and designed capacity have grown quickly since 2020, while the repair fleet, the dispersal of landing sites, and the clearance regime that governs both have not. Vulnerability of that composition is not reducible by adding cables, because the additions terminate on the same coastline, transit the same corridors, and depend on the same foreign repair consortia. Section 2 situates cables as security objects. Section 3 sets out the three axes. Section 4 applies them to India. Section 5 develops the contrast with China's PEACE cable. Section 6 assesses the governance response, Section 7 places it against the demand trajectory, and Section 8 concludes.

Cables as Security Objects

Cable security has moved from a technical concern to a recognised field of international security scholarship within roughly a decade. Bueger and Liebetrau (2021) mapped the protection of the global submarine data network as a governance problem, showing that responsibility is divided among private owners, flag states, coastal states, and international bodies in a way that leaves no actor accountable for the whole. Subsequent work extended the agenda to critical maritime infrastructure more broadly and to the European policy response (Bueger and Liebetrau, 2023; Bueger *et al.*, 2022). Franken, Reinhold, Reichert, and Reuter (2022) added a comparative dimension by measuring state vulnerability to cable failure, finding that exposure varies sharply with the number of independent landings a state commands.

The material properties of the network explain why governance is difficult. Starosielski (2015) showed that cable routes are shaped by a narrow set of technically viable corridors, that these corridors often retrace nineteenth-century telegraph geographies, and that the resulting topology concentrates traffic rather than distributing it. Concentration is efficient for operators and fragile for states, and the same nodes that reduce cost also assemble risk. Historical work on the telegraph era describes an analogous coupling of route geography and imperial control, which suggests that the present contest is a recurrence rather than a novelty (Headrick, 1991; Winseck and Pike, 2007).

An earlier body of work concentrated on the legal architecture and its gaps, examining the protections that the law of the sea affords cables outside territorial waters, the weakness of enforcement against negligent or deliberate damage, and the limited obligations that attach to flag states (Beckman, 2014; Broeders, 2015; Burnett *et al.*, 2014; Davenport, 2015; Sechrist, 2010, 2012; Sunak, 2017). A parallel technical literature documented the empirical baseline for risk, showing that the large majority of faults arise from fishing gear and anchors rather than from hostile action, that faults cluster in shallow and heavily trafficked water, and that natural hazards such as submarine landslides and seismic events account for a smaller but severe share (Carter *et al.*, 2009; Clare *et al.*, 2023)[4]. Both bodies of work bear directly

3. The comparison is with landing stations rather than with cable systems, and station counts include domestic and regional facilities. The regulator's point concerns the distribution of terminal infrastructure rather than the volume of capacity available.

4. The predominance of accidental causes matters for policy design, since measures aimed at deliberate interference do not address the majority of faults. Protection zones, route planning, and accurate charting reduce the ordinary fault rate more directly.

on the Indian case. The legal literature indicates why a coastal state's remedies concentrate at the landing station and in the repair regime, since those are the points at which jurisdiction is unambiguous. The technical literature indicates why the concentration of landings on one stretch of shallow, heavily used coastline is the exposure that matters most, since it maximises the probability of the ordinary fault while ensuring that any single fault is consequential.

Threat perception has broadened accordingly. Grey-zone activity in the Baltic and around Taiwan during 2022 and 2023, involving vessels linked to Russian and Chinese interests and the dragging of anchors across cable routes, moved deliberate interference from hypothesis to plausible scenario (Atlantic Council, 2025; Braw, 2022). Tonga's communications blackout in 2022 demonstrated what happens where a single cable serves an entire state. The expansion of the Digital Silk Road, with HMN Technologies as supplier and China-friendly ports as landing points, has raised parallel concerns about supply-chain security and the jurisdictional reach that landing-station control confers (Hemmings, 2020; Hillman, 2021; Sherman, 2021). A qualification belongs with the last of these. Farrell and Newman (2019) theorise that the government of a central node may derive panopticon leverage over the network, but hosting a landing station confers regulatory jurisdiction over a terminus and does not by itself indicate visibility into the traffic crossing it, and the two claims are kept apart throughout.

What the literature has not produced is a disaggregated vulnerability profile for a major Indian Ocean state. Work on India's maritime security concentrates on naval capability and sea-lane protection (Brewster, 2018; Khurana, 2008; Upadhyaya, 2020), while work on Indian digital policy concentrates on data governance and Digital Public Infrastructure (Jiang and Belli, 2024; Nilekani, 2018). Between the two sits the physical layer on which both depend, and the sections that follow address it directly.

Three Axes of Vulnerability

Vulnerability is disaggregated here into three axes that differ in what produces them and in what would reduce them. Physical fragility concerns the concentration of landings, the absence of sovereign repair capacity, and the dependence on foreign consortia to restore service; it is largely within the reach of national policy. Geopolitical exposure concerns dependence on maritime corridors whose security is determined by other actors; it can be redistributed but not removed. Domestic regulatory constraint concerns the clearance procedures, licensing conditions, and shipboard requirements that determine how quickly the first two can be addressed; it is entirely within national control and is the least visible of the three. Table 1 records the empirical manifestation of each axis and the response the regulator has proposed.

An incident register grounds the scheme empirically and clarifies what each axis is doing analytically. Table 2 records four recent events, the mechanism involved, the effect reported, and the state of attribution at the time of writing. Two patterns are visible across them. The reported consequence tracks the number of independent routes serving the affected party rather than the severity of the physical damage, which is why the Tonga blackout was more severe than the Red Sea cuts despite involving fewer cables. And attribution remains unresolved in the cases where deliberate interference is suspected, so that

Table 1 : Vulnerability axes in India's cable order and the corresponding governance responses

Vulnerability axis	Empirical manifestation	Proposed governance response	Locus of control
Physical fragility	Fifteen of about seventeen systems landing on one Mumbai beach; no Indian-flagged repair vessel; repair timelines of three to five months under foreign consortia	Critical-infrastructure designation for landing stations; essential-service status for repair; Indian-flagged repair and depot capacity; dispersal of landings beyond the Mumbai-Chennai axis	National
Geopolitical exposure	Dependence on the Suez, Bab el-Mandeb, and Hormuz corridors; land-bridge reliance on Israeli-Arab stability; Red Sea insurance and security costs	Sustained route diversification eastward, westward, and overland; redundancy so that no single corridor is indispensable	Shared with others
Domestic regulatory constraint	Multi-agency clearances; mandatory official presence aboard repair vessels; deterred landings and slow repairs	Single-window clearance; two-tier landing-station classification; tax and right-of-way concessions; auto-renewal of unchanged clearances	National

Source: Compilation based on Telecom Regulatory Authority of India (2023) and Khanna (2025).

Table 2 : Recent cable disruption events and their reported consequences.

Event	Mechanism	Reported effect	Attribution status
Tonga, 2022	Volcanic eruption and submarine landslide	National communications blackout on a single-cable dependency	Natural cause documented
Baltic Sea, 2023 to 2024	Suspected anchor dragging by transiting vessels	Damage to regional cables and pipelines	Contested; investigations unresolved
Red Sea, early 2024	Cuts to AAE-1, EIG, and SEACOM	About a quarter of Asia to Europe traffic affected	Linked to regional conflict conditions; not determined
Jeddah, September 2025	Cuts to two major systems	Slower speeds in India, Pakistan, and the UAE; cloud traffic rerouted; repaired within a day	Not determined

Source: Compilation based on Aben (2024), Atlantic Council (2025), HGC Global Communications (2024), and Insikt Group (2025).

policy on grey-zone risk is made under evidentiary conditions that do not support confident causal claims[5]. Both patterns argue for treating route redundancy and restoration speed, rather than attribution, as the operative policy variables.

Two features of this scheme matter for the argument. The axes interact rather than sum: a clearance regime that delays repair converts a physical fault into an extended outage, and a corridor closure that lasts longer than domestic repair capacity can bridge converts exposure into disruption. And the axes are unequally tractable, so that a strategy which invests in the least tractable of them, meaning route diversification, while leaving the most tractable ones unaddressed, will produce visible activity and limited change in the vulnerability profile.

India's Exposure Profile

Landing concentration

The Versova concentration is the clearest single point of failure in the system. Fifteen international cables terminating within six kilometres of coastline share not only a landfall but the terrestrial backhaul, power supply, and access roads that serve it, so that a fire, a flood, a construction accident, or a deliberate act at the landing site would affect a large share of the country's international connectivity at once (Khanna, 2025). Comparative work indicates that the number of independent landings, rather than aggregate capacity, is the variable most closely associated with resilience against cable failure (Franken *et al.*, 2022). By that measure India's position has improved little despite the capacity added since 2020, because the new systems have largely terminated on the same two coastlines.

The post-2020 landings do change the picture in one respect. Trunk systems that originate at Mumbai and Chennai rather than branching off cables designed for other markets give India control over where its own traffic enters and leaves, and additional landings from 2 Africa Pearls and the announced Project Waterworth deepen the pattern (Bharti Airtel, 2025; Meta, 2025). Origination is not dispersal, though, and a third coastal entry point on the eastern or western seaboard away from the existing pair would alter the failure profile more than an additional system at Versova would.

The trajectory of policy attention explains why the concentration persisted. Before 2020, India was a landing on other states' trunks: capacity was purchased rather than owned, routes were designed for the Singapore to Marseille corridor, and cable policy was administered as telecommunications licensing rather than as security. Between 2020 and 2022, India-originated systems were announced and the regulatory vocabulary shifted towards critical infrastructure, though little had been built. Between 2023 and 2024, construction and landings materialised alongside coalition commitments. From 2025 into early 2026, further landings arrived and the regulator's reform agenda was elaborated, while several headline systems remained incompletely in service. Announcement, construction, and operation have therefore run several years apart, and the vulnerability profile reflects the state of construction rather than the state of announcement.

Corridor exposure

Most Indian westbound traffic passes through the Bab el-Mandeb strait and Egypt, where sixteen cables cross an area measuring roughly 160 kilometres. Telecom

5. Attribution is difficult because a dragged anchor produces damage similar to that of an accidental grounding, and because vessels transiting international waters are subject to limited inspection. Investigations into the Baltic incidents have not produced published findings.

Egypt estimates that 17 per cent of the world's internet traffic transits Egypt, and some independent analyses place the figure closer to 30 per cent (Center for Strategic and International Studies, 2025)[6]. The divergence between the two estimates is itself informative, since neither operators nor regulators publish the traffic data that would settle it, and policy is therefore made against a range rather than a number. Fig. 1 sets out the corridor and the alternatives available to it.

Two mitigation routes exist and neither escapes the underlying condition. The overland alternative, in which a terrestrial segment across Israel joins a Mediterranean cable to a Red Sea cable and avoids Egyptian waters altogether, substitutes dependence on Israeli-Arab stability for dependence on Egyptian transit, and the war following the October 2023 attack on Israel has strained precisely that condition (Middle East Institute, 2025). Eastward routing through Southeast Asia relieves pressure on the western corridor for traffic destined for Asia but not for traffic destined for Europe. Diversification, on this evidence, redistributes exposure into other geopolitical spaces rather than removing it, and the conditions that motivate a bypass are capable of delaying the bypass itself, as elevated insurance costs and Houthi activity in the Red Sea have done.

Repair dependence

Repair capacity is where the vulnerability profile is least ambiguous and least discussed. India operates no cable repair vessel under its own flag and relies on consortia based in Dubai and Singapore, under arrangements in which restoration has taken three to five months (Insikt Group, 2025; Khanna, 2025)[7]. Three factors compound in that figure: the vessel must be released from a shared maintenance pool serving many systems, permits must be obtained from multiple agencies, and an official is required to be present aboard the repair ship, so that an operation measured in days of splicing becomes an outcome measured in months of waiting.

The consequence is a mismatch between the two halves of the system. A country that has added trunk systems, fibre pairs, and hyperscaler landings at speed depends for restoration on assets it neither owns nor schedules, and that dependence is invisible until a fault occurs. Two deep-water diving support vessels launched

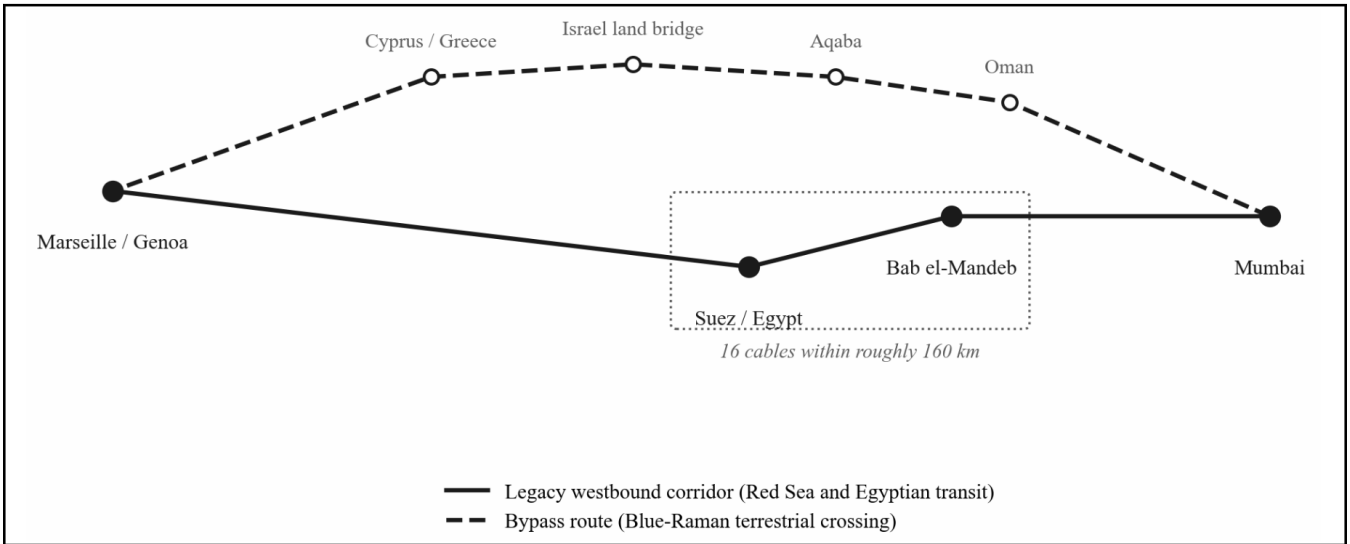

Fig. 1 : The western corridor from Mumbai to the Mediterranean, showing the Bab el-Mandeb and Suez chokepoints and the overland alternative. Source: Elaboration based on Center for Strategic and International Studies (2025) and TeleGeography (2025b)

6. The two estimates rest on different bases. The operator figure counts traffic on cables transiting Egyptian territory, while higher independent figures include capacity on systems that a disruption in the corridor would affect indirectly.

7. Restoration time varies with vessel availability, fault depth, weather, and permitting. The reported range reflects incidents in which several of these worked against a quick repair; shorter restorations have occurred where a vessel was already close at hand.

for the Indian Navy in 2022 offer a partial and adaptable base for a sovereign capability (Press Information Bureau, 2022), and international best-practice guidance on landing-station protection and repair readiness supplies the standard against which such a capability would be assessed (International Cable Protection Committee, 2021). Neither has yet been converted into a standing repair capacity, which is why repair rather than capacity is treated here as the binding constraint.

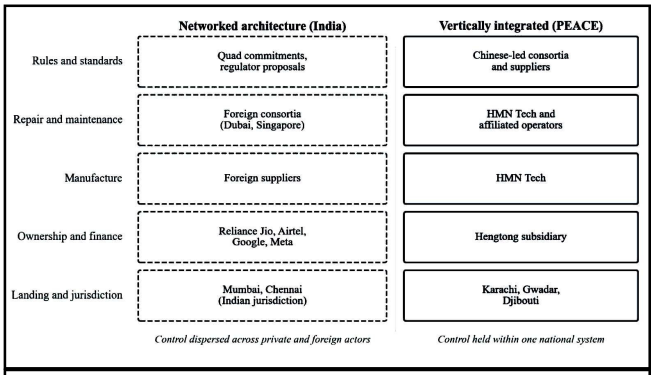

Fig. 2 : Vertically integrated and networked cable architectures compared across the financing, manufacture, ownership, operation, and repair layers. Source: Elaboration based on Middle East Institute (2022), TeleGeography (2025b), and consortium disclosures

Two Architectures, Two Failure Modes

China's PEACE cable supplies a controlled contrast, since it occupies the same ocean, the same corridor to Europe, and the same period as the Indian systems, so that what varies between them is the ownership and governance architecture rather than the geography. Owned by PEACE Cable International, a subsidiary of Hengtong, manufactured by HMN Tech, and commercially operated by PCCW Global of Hong Kong, the roughly 15,000 kilometre system, with an extension of about 6,500 kilometres toward Singapore, runs from Pakistan through Djibouti and Egypt to Marseille, with landings at Karachi and at the Chinese-operated port of Gwadar and branches to the Maldives, Malta, Cyprus, and Tunisia; the Pakistan to France route entered service in 2022 (Middle East Institute, 2022; TeleGeography, 2025b)[8].

Its landings at Gwadar and Djibouti, both sites of Chinese port operation and, in Djibouti, of military presence, exemplify a co-location of digital and physical infrastructure that Indian planners read as strategically significant, since it places the jurisdictional reach that landing-station control confers alongside the capabilities that forward basing supplies (Atlantic Council, 2023; Blanchard and Flint, 2017; Doshi, 2021). Fig. 2 sets the two architectures side by side across the layers at which each is assembled, and Table 3 records the failure mode each configuration generates.

The comparison is between architectures rather than between countries, and the claim is that the two configurations generate different capabilities and different failure modes rather than a ranking. Vertical integration aligns financing, manufacture, ownership, operation, and repair within one system, which shortens decision chains and secures restoration, while

Table 3 : Architectural comparison and the failure modes each configuration generates

Layer	Vertically integrated model (PEACE)	Networked model (Indian portfolio)	Implication for vulnerability
Financing	State-linked and programme-aligned	Private carriers and hyperscalers	Networked builds follow commercial demand and may bypass a state
Manufacture	National supplier	Foreign suppliers selected by consortium	Neither model gives India supply-chain control
Ownership and operation	Held within one national system	Dispersed across consortia and platform owners	Dispersal complicates coercion but disperses control
Landings	Co-located with operated ports	Concentrated on two national coastlines	Concentration is the sharper physical exposure
Repair	Aligned with the national fleet	Contracted to foreign consortia	Restoration time is set outside national policy

Source: Compilation based on Middle East Institute (2022), TeleGeography (2025b), Insikt Group (2025), and Khanna (2025).

8. The ownership chain bears on the architecture claim: Hengtong owns the cable company, HMN Tech supplies the manufacture, and PCCW Global operates the system commercially, so financing, build, and operation remain within one national industrial system.

concentrating political risk in the sponsoring state and inviting the supplier restrictions that the SEA-ME-WE 6 award illustrated. A networked portfolio assembled from private capital, foreign hyperscalers, and multinational consortia distributes political risk and complicates any attempt to weaponise interdependence against the host, since no single owner commands the whole, while leaving the host without the repair fleet, the supply chain, and the scheduling authority that vertical integration supplies. Read this way, India's exposure follows from the architecture it has adopted rather than from a deficit of investment, and the remedies that would matter most are those that add sovereign capability at the layers the networked model leaves out.

One consequence of the networked model deserves a separate statement, since it cuts against the vulnerability reading. Where a hub-and-spoke configuration concentrates regional traffic on nodes a single sponsor controls, the Indian portfolio spreads across India-led systems, a hyperscaler-led bypass, and consortium participation on a trunk built by a non-Chinese supplier, so no single corridor or owner commands the whole. Farrell and Newman (2019) theorise that a state at a network's centre may derive coercive leverage from that position, and the plural configuration complicates the exercise of such leverage against India, since an adversary would have to close several dissimilar routes at once. Gjesvik's (2023) proposition that private ownership diminishes state power is qualified in the same way, because a state able to draw on several privately owned options is not simply at the mercy of any one owner. The qualification is genuine and bounded: plurality raises the cost of coercion at the routing layer while leaving repair, manufacture, and clearance untouched, and it is at those layers that the disruptions of 2024 and 2025 produced their consequences.

The Governance Response

The regulator has set out the most detailed remedy. The 2023 recommendations of the Telecom Regulatory Authority of India propose designating landing stations as critical information infrastructure[9], according repair the status of an essential service, incentivising a domestic repair industry, creating coastal depots, and dispersing new landings across the peninsula, alongside a single-window clearance process, a two-tier classification of landing stations, tax and right-of-way concessions, and automatic renewal of unchanged clearances (Telecom Regulatory Authority of India, 2023). The package addresses all three axes and is notable for treating the regulatory axis as a security matter rather than as an administrative one, since the clearance regime determines how quickly the physical remedies can be delivered.

Coalition arrangements supply the external component. The Quad Partnership for Cable Connectivity and Resilience, announced at Wilmington in September 2024, allocated to India a feasibility study on expanding maintenance and repair capability in the Indian Ocean, created a Cable Connectivity and Resilience Centre in Australia, and delivered American training and technical assistance to telecommunications officials from more than fifteen Indo-Pacific states, with over 1,300 personnel trained in 2024 alone (Hemrajani, 2023; The White House, 2023a, 2024). Bilateral relationships add depth: Japan, whose NEC ranks among the three largest cable manufacturers and built the Chennai-Andaman system; France, which operates the Marseille gateway; and European Union institutions, through the Global Gateway and the Indo-Pacific strategy (European Commission, 2021; NEC Corporation, 2020; Satake and Sahashi, 2021).

Multilateral machinery has developed alongside the coalition track. The International Telecommunication Union and the International Cable Protection Committee launched an International Advisory Body for Submarine Cable Resilience in 2024, giving the resilience agenda a standing forum in which operators, suppliers, and states participate together (International Telecommunication Union, 2024a). Forums of that kind matter for a state in India's position because the operative rules of the sector are technical and procedural rather than treaty-based, covering route surveys, protection standards, repair prioritisation, and the notification arrangements that determine how quickly a fault is addressed. Influence at that layer is exercised by supplying the expertise and the data that standards are written from, which is a form of participation India has begun but not yet consolidated, and it is also the layer at which the domestic reform agenda and the external agenda meet, since a state with its own repair capacity and its own incident record has

9. Designation would place landing stations under the protective regime applied to other critical information infrastructure, which carries obligations for incident reporting, access control, and audit rather than any change in ownership.

more to contribute to both.

Announcement and operation should nonetheless be distinguished. India's governance role so far consists of feasibility studies, training programmes, and declaratory commitments rather than standards it has written or rules it has set, and a sceptical reading holds that participation of this kind is transactional and reversible, which would make the role contingent on a continued convergence of interest rather than settled (Tellis, 2023). Sequence supports that caution: announcement, construction, and operation have run several years apart across the whole post-2020 record, and the regulator's recommendations remain recommendations. The measures that would change the vulnerability profile are also the ones with the least visible progress, namely an Indian-flagged repair vessel, a third coastal entry point, and an operating single-window clearance.

Demand and the Resilience Deficit

The urgency of these measures follows from the demand trajectory. TeleGeography (2022) projects that India's international bandwidth will grow at a compound annual rate of 38 per cent between 2021 and 2028[10], more than tenfold over the period, and notes that demand would outstrip supply were the announced systems not entering service. Fig. 3 plots that trajectory against the sequence of landings, and the shape of the two together is the analytical point: capacity has been added in response to a forecast shortage, while the resilience of the capacity has been addressed more slowly.

Growth of that order changes what a disruption costs. As bandwidth rises and as government services, payments, and enterprise operations migrate onto networks that assume continuous international connectivity, the economic value at risk during a three to five month restoration rises with it, so a repair regime that was tolerable at the traffic volumes of 2021 becomes a material exposure at those projected for 2028. The first-order returns to connectivity depend on capacity and route diversity together (World Bank, 2016), and the second of the two has grown more slowly than the first.

Conclusion

Read through its failures rather than its announcements, India's cable order presents a specific and partly tractable vulnerability profile. Physical fragility is the axis over which national policy has the

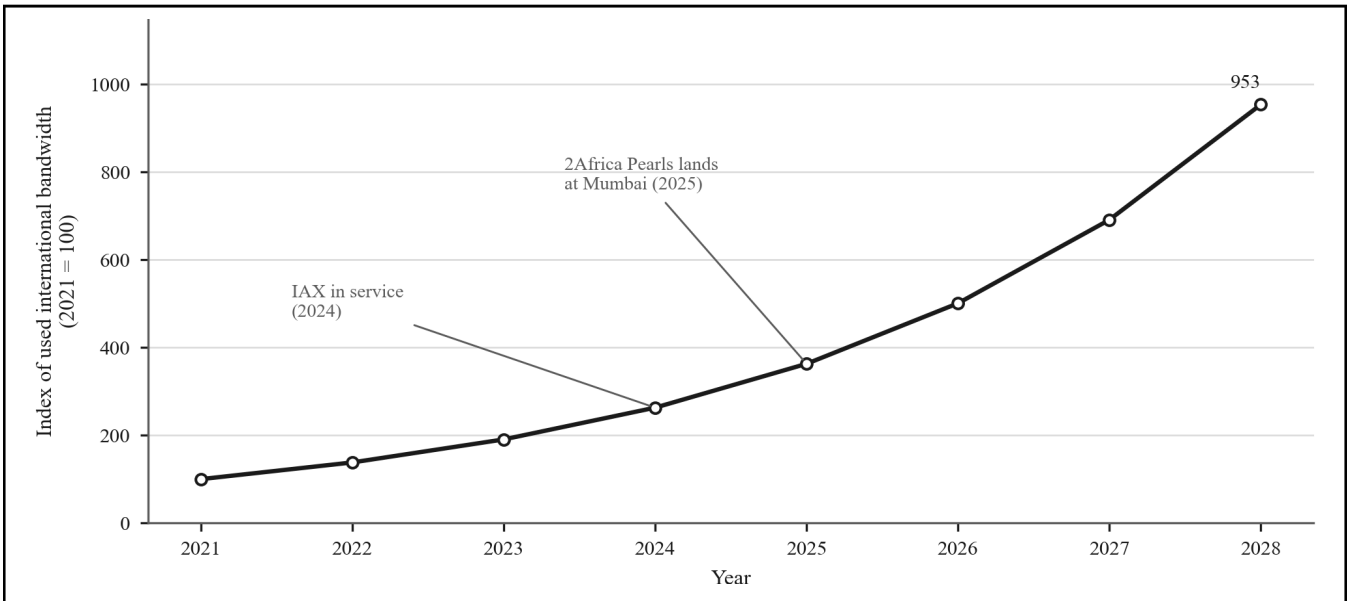

Fig. 3 : Indicative trajectory of India's used international bandwidth, 2021 to 2028, indexed to 2021, plotted against major cable milestones. The curve applies the projected 38 percent compound annual growth rate; milestone placement is the author's. Source: Elaboration based on TeleGeography (2022) and consortium landing announcements

10. The projection was issued in 2022 and extends to 2028, so the later years are extrapolation rather than observation. Growth of this order is consistent with regional trends but sensitive to data-centre siting decisions capable of shifting traffic patterns.

greatest influence and where the least has been delivered, since the Versova concentration persists and no repair vessel flies the Indian flag. Geopolitical exposure can be redistributed through eastward, westward, and overland routing but not removed, and the delayed opening of the overland alternative indicates that a mitigation route can share a fault line with the vulnerability it was built to address. Domestic regulatory constraint is wholly within national control, is the least visible of the three, and determines how quickly the other two can be addressed.

The comparison with a vertically integrated architecture locates the source of that profile. A networked portfolio distributes political risk and resists coercion by any single owner, and it leaves the host state without the repair fleet, the supply chain, and the scheduling authority that vertical integration supplies. The implication is not that India should replicate the alternative model, which carries its own concentration of political risk and its own exposure to supplier restriction, but that a networked strategy requires sovereign capability precisely at the layers it does not otherwise reach. An Indian-flagged repair vessel with coastal depots, a third coastal entry point away from the Mumbai and Chennai axis, and an operating single-window clearance regime are the three measures that would convert announced intent into a changed vulnerability profile.

Three limits qualify the account. Traffic and utilisation data that would show how much of the country's international traffic actually depends on the Versova landings are not public, so concentration is measured in systems rather than in flows. The Egyptian transit estimates diverge by a factor approaching two, which places a corresponding uncertainty on any assessment of corridor exposure. And restoration times are drawn from reported incidents rather than from a published series, so the three to five month figure indicates an order of magnitude rather than a distribution. Each of these is a case for disclosure as much as for research, since a vulnerability profile that cannot be measured is also one that cannot be governed with precision.

REFERENCES

Aben, E. (2024). *Does the internet route around damage? Baltic Sea edition*. RIPE Network Coordination Centre (RIPE Labs).

Atlantic Council (2023). *China's subsea cable power play in the Middle East and North Africa*. Atlantic Council.

Atlantic Council (2025). *How the Baltic Sea nations have tackled suspicious cable cuts*. Atlantic Council, Transatlantic Security Initiative.

Beckman, R. (2014). *Protecting submarine cables from intentional damage: The security gap*. In D. R. Burnett, R. Beckman, & T. M. Davenport (Eds.), Submarine cables: The handbook of law and policy (pp. 281-297). Martinus Nijhoff.

Bharti Airtel (2025). A*irtel brings 2Africa Pearls cable to India in partnership with Meta and center3*. Press release.

Blanchard, J.M.F. and Flint, C. (2017). The geopolitics of China's Maritime Silk Road Initiative. *Geopolitics*, **22**(2) : 223-245.

Braw, E. (2022). *The defender's dilemma: Identifying and deterring gray-zone aggression*. AEI Press.

Brewster, D. (2018). *India and China at sea: Competition for naval dominance in the Indian Ocean*. Oxford University Press.

Broeders, D. (2015). *The public core of the internet: An international agenda for internet governance*. Amsterdam University Press.

Bueger, C. and Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, **42**(3) : 391-413.

Bueger, C. and Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy*, **155**, 105772.

Bueger, C., Liebetrau, T. and Franken, J. (2022). *Security threats to undersea communications cables and infrastructure: Consequences for the EU*. European Parliament, Directorate-General for External Policies.

Burnett, D. R., Beckman, R. and Davenport, T. M. (Eds.). (2014). S*ubmarine cables: The handbook of law and policy*. Martinus Nijhoff.

Carter, L., Burnett, D., Drew, S., Marle, G., Hagadorn, L., Bartlett-McNeil, D. and Irvine, N. (2009). Submarine cables and the oceans: Connecting the world (UNEP-WCMC Biodiversity Series No. 31). UNEP World Conservation Monitoring Centre & International Cable Protection Committee.

Center for Strategic and International Studies (2025). The strategic future of subsea cables: Egypt case study. CSIS.

Clare, M. A., Yeo, I. A., Bricheno, L., Aksenov, Y., Brown, J., Haigh, I. D., Wahl, T., Hunt, J., Sams, C., Chaytor, J., Bett, B. J. and Carter, L. (2023). Climate change hotspots and implications for the global subsea telecommunications network. *Earth-Science Reviews*, **237**, 104296.

Davenport, T. (2015). Submarine cables, cybersecurity and international law: An intersectional analysis. *Catholic University Journal of Law & Technology*, **24**(1) : 57-109.

Doshi, R. (2021). *The long game: China's grand strategy to displace American order*. Oxford University Press.

European Commission. (2021). *The Global Gateway (JOIN(2021) 30 final)*. European Commission and High Representative of the Union for Foreign Affairs and Security Policy.

Farrell, H. and Newman, A.L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, **44**(1) : 42-79.

Franken, J., Reinhold, T., Reichert, L. and Reuter, C. (2022). The digital divide in state vulnerability to submarine communications cable failure. *International Journal of Critical Infrastructure Protection*, **38**, 100522.

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, **30**(2) : 722-746.

Headrick, D.R. (1991). *The invisible weapon: Telecommunications and international politics, 1851-1945*. Oxford University Press.

Hemmings, J. (2020). Reconstructing order: The geoeconomic thrust of the Digital Silk Road. *Asia Policy*, **15**(1).

Hemrajani, A. (2023). *The Quad Partnership for Cable Connectivity and Resilience (RSIS Commentary)*. S. Rajaratnam School of International Studies.

HGC Global Communications (2024). *HGC provides update on Red Sea submarine cable damage and rerouting arrangements*. Press release.

Hillman, J. E. (2020). *The emperor's new road: China and the project of the century*. Yale University Press.

Insikt Group (2025). Submarine cable security at risk amid geopolitical tensions and limited repair capabilities. Recorded Future.

International Cable Protection Committee (2021). Government best practices for protecting and promoting resilience of submarine telecommunications cables. ICPC.

International Telecommunication Union (2024a). ITU and ICPC launch International Advisory Body for Submarine Cable Resilience. ITU.

International Telecommunication Union (2025). The role of submarine cables in global connectivity. ITU.

Jiang, M. and Belli, L. (2024). Models of state digital sovereignty from the Global South: Diverging experiences from China, India and South Africa. *Policy & Internet.*, **16**(3).

Khanna, M. (2025). A roadmap for securing India's undersea cables (ORF Special Report No. 266). Observer Research Foundation.

Khurana, G. S. (2008). China's "string of pearls" in the Indian Ocean and its security implications. *Strategic Analysis*, **32**(1) : 1-39.

Meta (2025). Project Waterworth: Building the world's longest and highest capacity subsea cable. Meta Engineering Blog.

Middle East Institute (2022). Connecting Beijing's global infrastructure: The PEACE cable in the Middle East and North Africa. MEI.

Middle East Institute (2025). The India-Middle East-Europe Economic Corridor: A backgrounder. MEI.

NEC Corporation (2020). NEC completes submarine cable system for BSNL connecting Chennai, India and the Andaman and Nicobar Islands. Press release.

Nilekani, N. (2018). Data to the people: India's inclusive internet. *Foreign Affairs*, **97**(5).

Press Information Bureau (2022). Launch of two diving support vessels for the Indian Navy. Ministry of Defence, Government of India.

Satake, T. and Sahashi, R. (2021). The rise of China and Japan's "vision" for free and open Indo-Pacific. *Journal of Contemporary China*, **30**(127) : 18-35.

Sechrist, M. (2010). Cyberspace in deep water: Protecting undersea communication cables by creating an international public-private partnership. Harvard Kennedy School.

Sechrist, M. (2012). New threats, old technology: Vulnerabilities in undersea communications cable network management systems.Belfer Center for Science and International Affairs, Harvard Kennedy School.

Sherman, J. (2021). *Cyber defense across the ocean floor: The geopolitics of submarine cable security*. Atlantic Council.

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, **43**(3) : 377-391.

Starosielski, N. (2012). "Warning: Do not dig": Negotiating the visibility of critical infrastructures. *Journal of Visual*

Culture, **11**(1) : 38-57.

Sunak, R. (2017). Undersea cables: Indispensable, insecure. Policy Exchange.

Telecom Regulatory Authority of India (2023). Recommendations on licensing framework and regulatory mechanism for submarine cable landing in India. TRAI.

TeleGeography (2022). India surges in international bandwidth demand, expects a 38% compound annual growth rate between 2021 and 2028. Press release.

TeleGeography (2025b). Submarine cable map 2025. TeleGeography.

Tellis, A. J. (2023). America's bad bet on India. Foreign Affairs.

The White House (2023a). Fact sheet: Quad leaders' summit. The White House.

The White House. (2024). The Wilmington Declaration: Joint statement from the leaders of Australia, India, Japan, and the United States. The White House.

Upadhyaya, S. (2020). *India's maritime strategy: Balancing regional ambitions and China*. Routledge.

Winseck, D. and Pike, R. M. (2007). *Communication and empire: Media, markets, and globalization, 1860-1930*. Duke University Press.

World Bank (2016). *World development report 2016: Digital dividends*. World Bank.

****