From Shore to Core: Building Secure and Resilient Subsea Networks

October 2025

From Shore to Core: Building Secure and Resilient Subsea Networks

October 2025

Partner Institutions

United Services Institution of India (USI) is a tri-service military think-tank on matters of national security. It works on multi-disciplinary progressive policy research and narrative building in comprehensive national security with a military focus in a wider global geopolitical context. For more information, please visit: https://www.usiofindia.org/index.php

Koan Advisory Group is a New Delhi-based public policy consultancy. It specialises in policy and regulatory analysis in both traditional and emergent sectors and markets. For more information, please visit: www.koanadvisory.com

Authors
Vedika Pandey and Samrridhi Kumar

contactus@koanadvisory.com | **www.koanadvisory.com**

From Shore to Core: Building Secure and Resilient Subsea Networks

On October 16, 2025, the United Service Institution of India and Koan Advisory Group co-hosted a roundtable to explore approaches to building secure and resilient subsea cable infrastructure. The event drew participation from equipment manufacturers, end-users, legal and policy experts, as well as government and military stakeholders. There was consensus that redundancy, diversity, and resilience are the three cornerstones of a secure and sustainable subsea cable ecosystem. These cables form the backbone of global digital connectivity, carrying over 95 percent of international data traffic.

Although subsea cable systems are primarily financed, built and operated by private industry, their uninterrupted functioning is vital to national security and economic continuity. Each year, an estimated 150-200 cable cuts occur worldwide,[1] with the vast majority (70 percent) resulting from accidental human activities, such as fishing or anchoring. Even brief disruptions affect critical sectors including defence, finance, trade and public administration.

Geopolitical contestation has extended to creating physical disruptions, as witnessed by recent incidents in the Baltic Sea and the Red Sea, which led to multiple subsea cable faults, resulting in temporary outages that disrupted internet traffic between Europe, Asia, and the Middle East.[2] In the Taiwan Strait, the number of disruptions in January 2025 alone exceeded those recorded over the previous two years, resulting in traffic being rerouted onto slower satellite links, increasing latency for users.[3] On the other hand, China has reduced its internal regulatory friction considerably in recent years.

As the industry increasingly locates data centres at or near subsea cable landing stations, discussions on subsea cable infrastructure must be conducted in tandem with questions about how data is stored, transmitted, and powered. The clustering of infrastructure means that any disruption at a landing site can now affect not only data flow but also processing and storage. This links subsea infrastructure resilience to concepts such as digital sovereignty (control over and security of data within national borders), data localisation (where data is physically stored), and the energy consumption that underlies this infrastructure.

In this context, the roundtable participants shared several suggestions, which are captured in this outcome report and summarised in the order of appearance below:

1. **National Subsea Cable Policy:** Develop a comprehensive National Subsea Cable Policy addressing key issues like cable diversity, redundancy, repair capacity and protocol, security and inter-agency coordination.
2. **Domestic Repair and Maintenance Capacity:** Establish sovereign or industry consortium-led repair capacity, supported by a streamlined clearance and approval mechanism for efficient repair and maintenance operations.
3. **Ensure Security of Cable Landing Stations:** Designate cable landing stations as protected systems under the Information Technology Act, 2000, with appropriate security coverage, or designate subsea cables as critical telecommunication infrastructure under the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024.
4. **Marine Spatial Planning and Resource Coordination:** Implement marine spatial planning and coordinated fishing management to minimise risks of accidental cable damage. This could also entail establishing cable-protection zones and creating industry-led cooperative mechanisms with fishing communities.
5. **Technological Resilience and Threat Detection:** Invest in fibre sensing and AI-based predictive resilience mechanisms to detect vulnerabilities, forecast disruptions, and optimise network performance.
6. **Regional and International Collaboration:** Deepen regional collaboration through frameworks like the QUAD to enhance subsea cable security, redundancy and shared response capabilities across trusted partners.

The key themes discussed during the roundtable are detailed in the following sections.

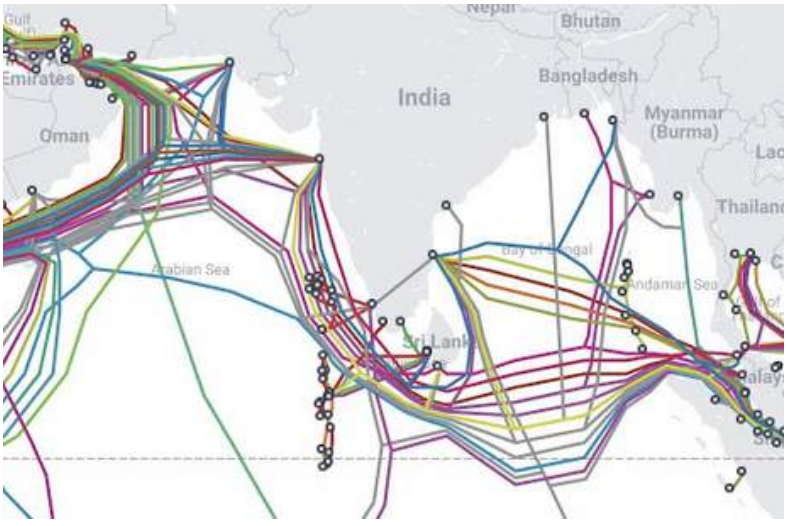
1. Redundancy, Diversity and Concentration

India's expanding digital economy depends heavily on subsea cables for international connectivity. The distribution and resilience of this infrastructure requires continuous policy and industry focus to meet the growing demands for data. Some of the structural issues meriting attention in India's subsea network and accompanying strategic considerations for improving redundancy and security are outlined below:

Asymmetry in Indian Data Needs and Subsea Infrastructure: Since subsea cable routes mirror historical maritime trade routes, India's geographic location makes it a natural hub for connectivity between the East and West (*see Figure 1*).[4] At present, the global average tele-density stands at approximately 111 percent, while in India, it is around 85 percent, with wireline data consumption estimated to be between 250 GB and 500 GB per month.[5] These numbers highlight a growing appetite for data consumption. Indian cable landing stations are situated in only five locations – indicating an asymmetry between data consumption and available landing station capacity. In contrast, Australia, with an average monthly data consumption of 40 GB[6], has over eight cable landing locations and multiple landing points.[7]

Lack of Geographical Diversity: While India's subsea cable network has expanded in capacity and coverage, it remains concentrated along a few routes and landing points. Mumbai dominates cable landings, with 15 out of India's 17 cables landing in a 6 km patch at Versova.[8] This poses a disproportionate strategic risk, since a lack of route diversity and landing sites (*see Figure 1*) increases the risk of large-scale outages in the event of natural disasters or targeted disruptions. For instance, during Cyclone Vardah, which struck the eastern coast of India in 2016, an undersea cable located across the Bay of Bengal was damaged, resulting in a loss of connectivity in several regions of West Bengal.[9] Such disruptions can severely affect the functioning of entities such as Gujarat International Finance Tec-City (GIFT City), a growing global financial hub, and also cause further reputational damage.

Figure 1: India's subsea cable connectivity and landing stations



(source: https://www.submarinecablemap.com/***)***

Concentration vs. Diversification: While the concentration of cable landing points can simplify physical security and maintenance, it also increases the impact of a single-point failure if those sites are disrupted by natural disasters or hostile activity. On the other hand, a diversified network with multiple, geographically dispersed routes and landing stations lowers the risk of failure but is more costly and complex to manage. The optimal approach lies in striking a balance between these models.[10]

2. Repair Infrastructure

India's capacity to repair damaged subsea cable infrastructure needs urgent attention to overcome procedural delays, fragmented responsibility, and limited domestic capability. The key operational and governance challenges in cable repair and maintenance, as well as possible measures for strengthening resilience, are discussed below:

Dependence on Foreign Vessels: India lacks a sovereign repair vessel,[11] that is, a repair ship flagged, registered, and operated by the Indian state, which would enable it to repair its own critical infrastructure. The country also lacks assured and immediate access to repair vessels owned by private operators. In the event of cable damage, therefore, cable owners must collaborate with the government to employ foreign vessels and secure the necessary clearances.[12] Detailed clearances are required separately for the ship and crew members, as well as for operating in Indian waters.[13] This process can sometimes take months, even though vessels often arrive within days.

Alternative Approaches to Building Repair Capacity: Subsea cables and landing stations are critical infrastructure that require dedicated protection and maintenance capabilities. Repair systems, much like submarine rescue systems, are specialised capabilities that play an indispensable role in safeguarding connectivity. One approach to strengthen domestic repair capacity and self-sufficiency is for the Government of India to invest in a sovereign repair vessel, following models used by countries such as the United States, which operates specialised repair ships as a part of its naval support fleet. These vessels are equipped with advanced workshops, spare parts inventory, and skilled personnel, enabling rapid maintenance and repair of maritime assets.[14] Such vessels cost around USD 100 million, a nominal sum compared to the economic risks of outages.[15] On the other hand, studies have shown that unplanned downtime due to cable cuts costs around USD 5,600 per minute.[16]

If the approach of an Indian-owned sovereign repair vessel does not fructify, an alternative approach is to develop such capacities through private or industry-led consortia. Examples include the Southeast Asia and Indian Ocean Cable Maintenance Agreement, under which the vessel Cable Retriever is operated through a private consortium of telecom operators, who jointly fund and manage its operations.[17] Establishing arrangements with friendly governments or trusted private operators – e.g., Indonesia's state-owned Telekom Indonesia could also offer a viable, low-cost alternative. However, this will require political and administrative will.[18]

An alternative approach would involve engaging the Indian Navy, which recently demonstrated its submarine repair and rescue capabilities during an international exercise in the South China Sea.[19] Two vessels launched by the Indian Navy in 2022 to operate in the deep sea for submarine rescue can also be retrofitted for cable repair. This suggestion is also being considered by a joint committee comprising representatives from the Ministry of Ports, Shipping and Waterways, the Indian Navy, the National Security Council Secretariat (NSCS) and the Department of Telecommunication (DoT).[20]

Security and Responsibility: Another challenge in repair management is determining whether the responsibility for the physical and operational security of cable landing stations should be with private operators, local authorities, or central security agencies. Moreover, the level of security at these facilities is uneven, with no uniform standards across locations.

Submarine cable landing stations should be considered 'protected systems' under the Information Technology Act, 2000, thereby making them part of the Critical Information Infrastructure. The Telecom Regulatory Authority of India (TRAI) also suggested their inclusion under the National Critical Information Infrastructure Protection Centre for standardised security and protection.[21] Subsea cables were

recently notified as critical telecommunication infrastructure[22] under the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024.[23]

Suggestions to make the repair more efficient, discussed by roundtable participants, include:

1. Creating a pre-approved or empanelled list of repair vessels to avoid bureaucratic delays, with measures such as annual pre-clearance for crews, elimination of port entry requirements and enabling Free Ports with bonded storage facilities to waive customs duties, fees and other formalities for repair vessels, equipment and personnel. This will facilitate the swift restoration of connectivity in the event of an outage or emergency.
2. Designate a nodal government authority (potentially under the Ministry of Communications) for all repair-related communication. Currently, repair-related clearances and permits require the involvement of four ministries, in addition to pre-repair permits, such as import formalities and customs clearance.
3. Remove the requirement that a DoT official be physically present on repair vessels.[24] Alternatively, have pre-designated officials available at short notice.
4. Develop a national subsea cable policy to address the repair, security, and governance aspects under a unified framework, similar to Australia's Critical Infrastructure Resilience Strategy, which brings together government agencies and private operators to coordinate planning, risk management, and rapid response for critical infrastructure.[25]

3. Socio-Political Challenges

Fishing activity is the leading source of accidental cable damage to subsea cables.[26] This typically occurs when trawl nets, anchors, or dredging gear make contact with cables laid close to shore or along continental shelves.[27] In India, although both the Centre and the States have established maritime and fisheries frameworks, their enforcement is uneven and challenging in practice. The following are key points of discussion and potential solutions:

Lack of Regulatory and Institutional Capacity/Coordination: Fisheries is a 'state subject' under the Indian Constitution. This means that regulatory control, monitoring and enforcement largely rest with individual state governments rather than with the Union. As a result, coordination across coastal states, each with its own administrative priorities, jurisdictional boundaries, and resource capacities, is a significant challenge. This fragmentation also affects the ability of central ministries, such as the DoT (for subsea cables) or the Ministry of Ports, Shipping, and Waterways (for general navigation), to implement uniform standards or awareness campaigns across the coastline. Private sector companies may be hindered by financial/commercial viability, as well as regulatory constraints. The deployment of the Central Industrial Security Force, state maritime police forces, the coast guard, and the Indian Navy requires a coordinated effort.

Low Level of Awareness and Compliance: Low awareness and inadequate vessel-tracking practices among the fishing community compound institutional gaps discussed above. Many fishing vessels operate without functional Automatic Identification Systems (AIS), which are designed to transmit a vessel's location to help avoid restricted zones. In some cases, participants reported that vessels deliberately disable their AIS to evade detection or fish in prohibited waters. The absence of reliable tracking makes it difficult for authorities to monitor vessel movement near subsea cable corridors or to identify the source of damage.

In this context, the forum discussed the following solutions:

Establishing Cable-Protection Zones (CPZ): Indian law currently does not prevent fishing communities from damaging subsea infrastructure. India lacks a formal, enforceable zone-based regime that restricts fishing in the vicinity of cable routes.[28] Establishing dedicated CPZs is a viable solution. These zones generally rely on marine spatial planning to map and coordinate all relevant maritime uses, including subsea cables, gas pipelines, and fishing zones. This process would also designate specific areas where fishing and other potentially seabed-disturbing activities would be restricted or prohibited to minimise interference with submarine cable systems.

Under the Australian Telecommunications Act, the government can establish a protection zone around a submarine cable.[29] This is a relevant precedent because activities likely to damage cables within such a zone – such as trawling near the seabed, nets anchored to the seabed, dredging and sand-mining – are explicitly prohibited and attract criminal penalties.

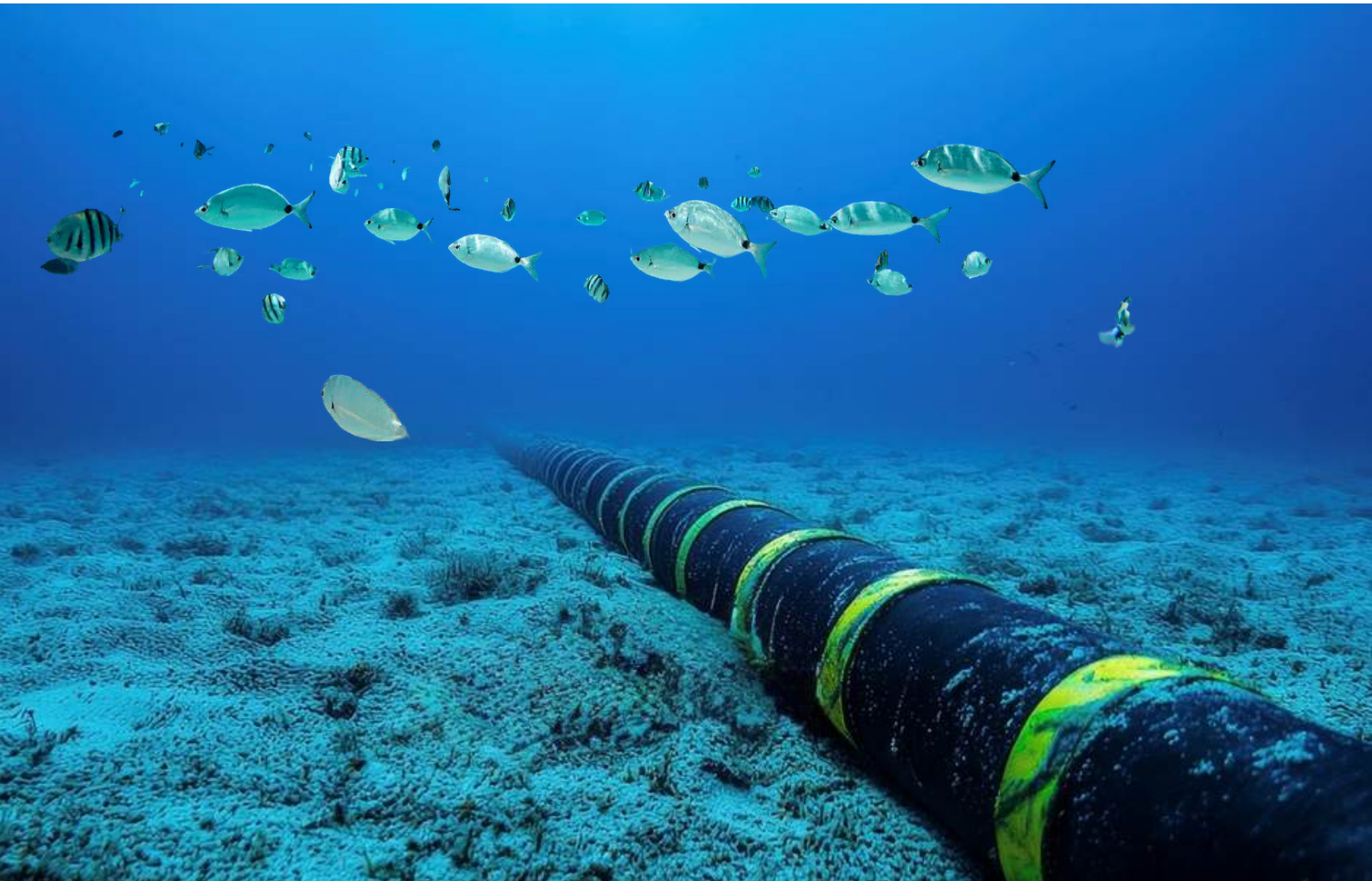
However, there may be instances where the creation of CPZs is not useful for cable operators, as they may not allow for sufficient spatial separation. Additionally, creating CPZs can add to deployment costs by forcing routing through areas that are not economically efficient or by requiring landings where no economic necessity exists. CPZs can also create risk by clustering cables, exposing multiple systems to the same anchoring cuts. Hence, it is imperative that CPZs not be mandatory in nature and that they be declared through consultations with wide-ranging stakeholders to facilitate the supply of efficient and cost-effective carriage services to the public.[30] Effective enforcement is also essential, and if a government is not willing or prepared to implement and enforce CPZs, particularly through penalising non-compliant fishing and shipping activities, then CPZs should not be pursued as a mandatory measure.

Similar CPZs in India would help clarify boundaries around subsea cable landing and route corridors, restrict high-risk seabed activities in those corridors, and ensure coordination between the cable sector, state governments, and maritime regulators.

Industry-Led Cooperation with Fishing Communities: The industry could collectively establish habits of cooperation with fishing communities.[31] A recent example of this is the Oregon Fishermen's Cable Committee in the United States, which serves as a formal liaison between submarine cable companies and commercial trawl fishers.

The OFCC mediates routing decisions, shares updated maps of cable corridors with fishers, provides emergency contact support for snagged-gear incidents, and administers a 'sacrificed-gear fund' so fishers are compensated immediately if they snag a cable, easing liability fears and fostering cooperation rather than conflict.[32]

The above solutions must be developed with robust stakeholder consultation and be adaptive by design. As ocean temperatures, currents and marine ecosystem dynamics change, so do fishing patterns. Therefore, CPZs and incentive structures must be revisited regularly to remain effective. Continuous dialogue between fishermen, cable authorities, and government instrumentalities will be crucial.



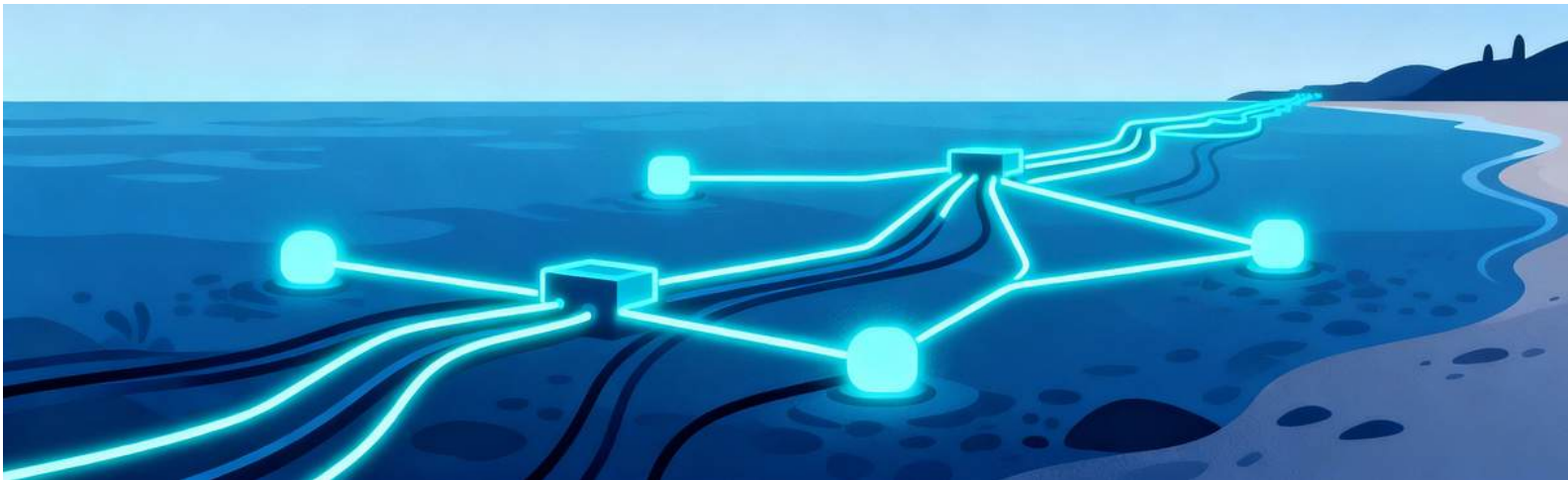
4. Coordination and Policy Direction

Despite the growing strategic importance of subsea cable infrastructure, policy responsibility in India remains dispersed across multiple ministries and agencies, each operating within its own mandate. This results in the overlapping but unclear jurisdictions, and the absence of a unified national framework governing cable deployment, maintenance and repair. An inter-ministerial effort, as mentioned earlier, is underway to enhance coordination on subsea cable security and facilitate repairs.

A whole-of-government approach necessitates collaboration between:

1. The Ministry of Defence and the Ministry of Home Affairs for security considerations.
2. The Ministry of Environment, Forest and Climate Change for environmental and coastal-zone clearances.
3. State governments, the Ministry of Ports, Shipping and Waterways and the Department of Fisheries, for fishing and maritime governance requirements.

The following infographic presents an indicative list of government instrumentalities involved in decision-making for subsea cable infrastructure, along with their respective broad mandates.



5. Data Exfiltration and Cybersecurity

In the broader discussion on subsea infrastructure resilience, an under-examined issue is data exfiltration – the interception or extraction of information from data streams transmitted through subsea cables. While physical damage tends to attract immediate attention, the potential for covert data interception represents an equally significant strategic and cybersecurity risk.

Exfiltration of data from subsea cables continues to be a difficult due to technical controls and operational practices in place. Submarine line terminal equipment, which includes the cable modems at each landing station, can detect almost immediately when a cable is cut, disturbed, or otherwise tampered with, making covert access highly unlikely. Further, although it is theoretically possible for an exfiltration attempt to occur during cable repair, this risk is mitigated by the presence of a cable operator's representative on the repair vessels. Currently, the prospect of gains from the extraction of large scale data is minimal due to limited quantum computing capabilities. This ensures that the vast majority of the data exfiltrated comprises of routine, low-value information with limited potential of intelligence gains from that in the immediate period.

Key aspects of this discussion are highlighted below:

Detecting Data Exfiltration: Subsea cables transmit data at speeds of up to 320 terabits per second, making it unfeasible to immediately exploit specific information due to its volume. However, malicious actors may store intercepted encrypted data for future 'harvest now, decrypt later' attacks, where stolen encrypted traffic is held until more powerful decryption methods become available.[33]

Encryption also limits the ability of network operators to trace the origin or scope of a potential breach. Emerging technologies, such as quantum computing and artificial intelligence, may enable the efficient decryption of large data volumes in the future. Quantum computers operate on principles that will allow them to process vast numbers of calculations simultaneously, potentially rendering many of today's encryption algorithms obsolete.[34] AI, on the other hand, can accelerate pattern recognition and anomaly detection, making it easier to identify weaknesses in encryption protocols or automate large-scale decryption efforts.[35]

Enhancing Data Continuity through Local Storage: Increasing the use of local caching (the temporary storage of frequently accessed data near users) and cloud storage within national borders can mitigate the impact of subsea cable disruptions. Such measures help ensure service continuity, maintain low latency, and minimise dependency on international data routes during outages.

However, it is important to note that most AI-generated data cannot be cached. These outputs are produced dynamically within the data centre in response to individual queries, which means they cannot be pre-stored. When the relevant data centre is located offshore and the responses are delivered via submarine cable, the information cannot be cached onshore, since they are generated specifically for each unique request.

Fibre Sensing for Early Threat Detection: Fibre sensing technology enables the continuous monitoring of optical fibre cables by analysing subtle variations in ambient noise or vibrations along the cable. Initially developed to reduce signal interference, it now serves as an early-warning system, identifying interference locations in real-time and determining whether a cable fault has been caused by environmental factors, accidental damage, or deliberate tampering. Integrating fibre sensing into India's subsea infrastructure could strengthen infrastructure resilience and enable faster response times to security incidents.

6. Geopolitics and International Cooperation

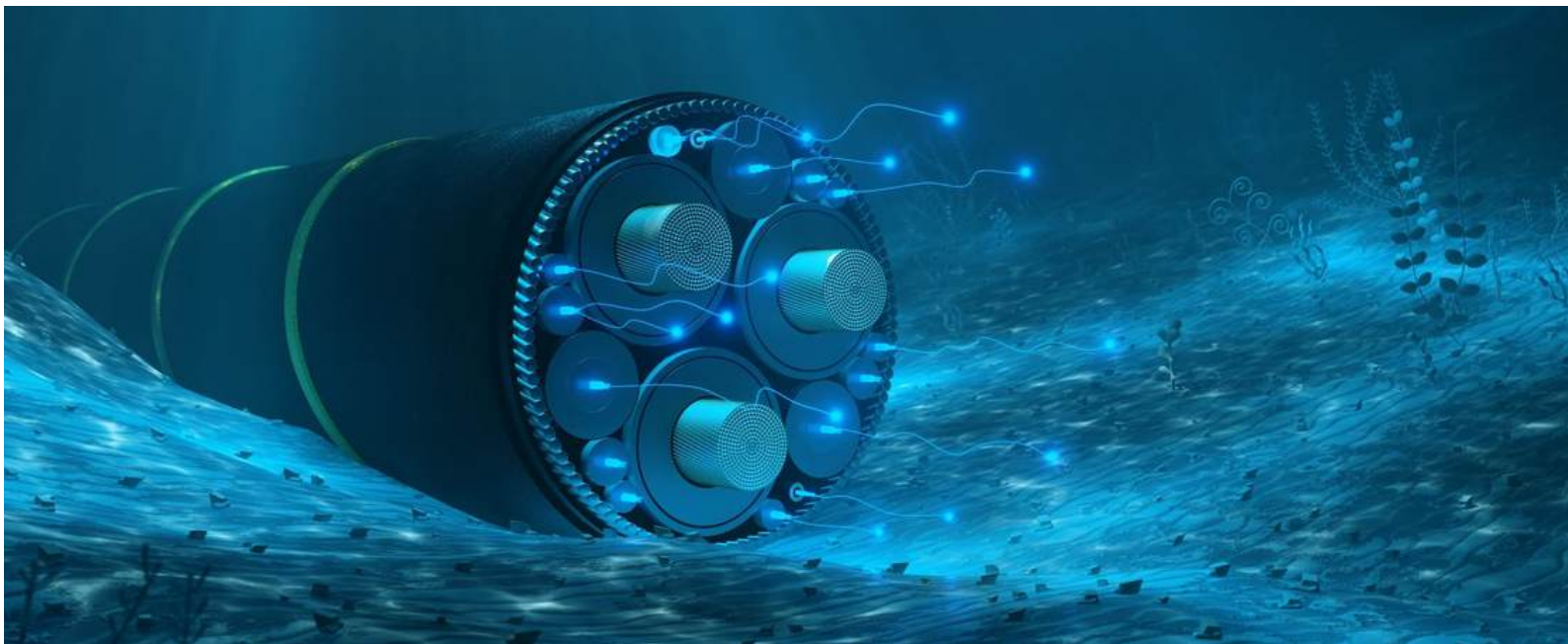
Differing National Priorities and Subsea Infrastructure: The United States and its allies have advanced 'clean network' initiatives to secure telecommunications and subsea infrastructure by excluding equipment from untrusted vendors.[36] India's trusted sources initiative follows a similar approach.[37] While related safeguards strengthen network security, they also slow down infrastructure deployment by narrowing the supplier base and increasing compliance burdens. In contrast, China, which imposes no comparable vendor restrictions, has adopted an agile, state-coordinated approach.[38] This has enabled it to rapidly expand its subsea cable infrastructure.

How Regional Coalitions Can Be Leveraged: The Quadrilateral Security Dialogue (QUAD) has placed growing emphasis on strengthening India's subsea cable ecosystem as part of its broader Indo-Pacific digital resilience strategy. Recent QUAD initiatives demonstrate a shift towards an India-focused strategy and capacity building,[39] recognising its position as a regional connectivity hub that accounts for nearly 20 per cent of global internet traffic and faces increasing demand for diversified cable infrastructure.

At the Wavelength Forum convened in New Delhi in July 2025, the QUAD held multistakeholder discussions examining strategies to expand India's cable infrastructure through regulatory reform, streamlined permits and enhanced maintenance and repair capacity.[40] Discussions also highlighted the need for coordinated responses to emerging threats, including cyberattacks and sabotage, and underscored the importance of collective action to safeguard the resilience of global connectivity systems. India must continue to leverage its regional centrality through coalitions like the QUAD to collaborate on subsea cable security and capacity-building.

India's Island Territories and Regional Cable Redundancy: The Andaman and Nicobar Islands and Lakshadweep Islands are increasingly pivotal to regional subsea network planning. Their geographic positioning enables them to serve as alternative landing points, helping to diversify traffic routes and mitigate concentration risk. This approach builds regional redundancy – a system design principle that ensures continuity of connectivity by enabling traffic rerouting in the event of a cable or landing station disruption.

The installation of the Kochi–Lakshadweep and Chennai–Andaman submarine optical fibre cables has substantially enhanced internet connectivity to India's island territories.[41] The expansion of cable connectivity to these islands supports both national and QUAD priorities for distributed, resilient digital infrastructure in the Indo-Pacific. These efforts position India not only as a key landing destination but also as a hub for regional cable interconnection and repair activity.



Endnotes

1 International Telecommunication Union (ITU), Submarine cable resilience – ITU - 29 November 2024, ITU (November 29,2024), https://www.unognewsroom.org/story/en/2441/submarine-cable-resilience-itu-29-november-2024

2 Andrea Palasciano & Oliver Cook, Baltic Sea Cable Cuts Can't Be Accident, EU Tech Chief Says, Bloomberg (January 14, 2025), https://www.bloomberg.com/news/articles/2025-01-14/baltic-sea-cables-damage-can-t-be-accident-eu-tech-chief-says

3 Keoni Everington, 2 Taiwan-Matsu undersea cables disconnected, Taiwan Times (January 22, 2025), https://www.taiwannews.com.tw/news/6021043

4 Vedika Pandey, Dhruv Shekhar & Samrridhi Kumar, Strengthening the U.S.-India subsea cable agenda, The Hindu (June 03, 2025), https://www.thehindu.com/opinion/op-ed/strengthening-the-us-india-subsea-cable-agenda/article69649909.ece

5 Broadband India Forum, Key Takeaways from India's 1st International Subsea Cable Systems Conference (March, 2025), https://broadbandindiaforum.in/wp-content/uploads/2025/04/Key-Takeaways_-BIF-GDIP-1st-Intl-Subsea-Cable-Systems-Conference.pdf

6 Marshall Thurlow, Australian internet usage, Swoop (November 09, 2024), https://www.swoop.com.au/blog/australian-internet-usage/

7 TeleGeography, Australia-Submarine Cable Map, https://www.submarinecablemap.com/country/australia

8 *Supra* Note 4

9 Sebastian Moss, Cyclone Vardah damages submarine cables to eastern India, Data Center Dynamics (December 14, 2016), https://www.datacenterdynamics.com/en/news/cyclone-vardah-damages-submarine-cables-to-eastern-india/

10 Alexander Botting, Subsea Security: A Comprehensive Action Plan to Promote Submarine Cable Resiliency, Security and Governance (September, 2025), Center for Cybersecurity Policy and Law Whitepaper, https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/68d4590cefdd47a519523ace_CCPL_SubseaWhitepaper_2025.09.pdf

11 Jatin Grover, Big tech submarine cables may see govt infra support, Financial Express (December 19, 2024), https://www.financialexpress.com/business/digital-transformation-big-tech-submarine-cables-may-see-govt-infra-support-3695353/

12 Telecom Regulatory Authority of India, Consultation Paper on Ease of Doing Business in Telecom and Broadcasting Sector (December, 2021), https://www.trai.gov.in/sites/default/files/2024-09/CP_08122021.pdf

13 Telecom Regulatory Authority of India, Consultation Paper on Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India (December, 2022), https://www.trai.gov.in/sites/default/files/2024-09/CP_23122022_0.pdf

14 Melissa B. Mahle, Subsea Cables and US National Security, Steptoe (August 8, 2025), https://www.steptoe.com/en/news-publications/stepwise-risk-outlook/subsea-cables-and-us-national-security.html

15 *Supra* Note 10

16 Subsea Cables by Telecom Review, Invisible Infrastructure, Visible Chaos: Building B2B Continuity in a Subsea-Dependent World, Subsea Cables by Telecom Review (August 06, 2025), https://www.subseacables.net/reports-and-coverage/invisible-infrastructure-visible-chaos-building-b2b-continuity-in-a-subsea-dependent-world/

17 Global Marine, SEAIOCMA Extends Cable Maintenance Agreement with Global Marine, Global Marine (July 20, 2021), https://globalmarine.co.uk/seaiocma-extends-maintenance-agreement-with-global-marine/

18 John Tanner, Telkom Indonesia to repair subsea cable break affecting Papua, Developing Telecoms (August 19, 2025), https://developingtelecoms.com/telecom-technology/optical-fixed-networks/18934-telkom-indonesia-to-repair-subsea-cable-break-affecting-papua.html

19 Press Information Bureau Delhi, Indian Navy Demonstrates Global Submarine Rescue Capability at Exercise Pacific Reach (Xpr-25), Press Information Bureau (October 01, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173604

20 Pratap Vikram Singh, As conflicts threaten undersea cables, India looks to retrofit naval vessels to protect assets, The CapTable (July 11, 2025), https://the-captable.com/2025/07/internet-india-navy-vessels-repairing-undersea-optic-fibre-cables/

21 Telecom Regulatory Authority of India, Recommendations on Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India (June, 2023), https://trai.gov.in/sites/default/files/2024-09/Recommendation_19062023_0.pdf

22 Gazette Notification S.O. 4703 (E). Link: https://egazette.gov.in/(S(i5nhxoaayfzgjd0gdsxlh3pd))/ViewPDF.aspx

23 Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024. Link: https://egazette.gov.in/WriteReadData/2024/256725.pdf

24 *Supra* Note 21.

25 Department of Home Affairs – Australian Government, Critical Infrastructure Resilience Strategy (February, 2023), https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf

26 Joint Research Centre: EU Science Hub, The JRC explains: Subsea cables: how vulnerable are they and can we protect them?, (August 8,2025), https://joint-research-centre.ec.europa.eu/jrc-explains/subsea-cables-how-vulnerable-are-they-and-can-we-protect-them_en

27 Geoff Macangus-Gerrad, Offshore Electrical Engineering Manual (Second Edition) (Elsevier 2018)

28 *Supra* Note 13

29 Australian Telecommunications Act, 1997, Part 2. https://classic.austlii.edu.au/au/legis/cth/consol_act/ta1997214/sch3a.html

30 Australian Communications and Media Authority, Declaring a submarine protection zone Guide for applicants (August, 2025), https://www.acma.gov.au/sites/default/files/2025-08/Guide%20-%20Declaring%20a%20submarine%20cable%20protection%20zone%20%28August%202025%29.pdf

31 Erin L. Murphy and Thomas Bryja, The Strategic Future of Subsea Cables: Japan Case Study, Center for Strategic and International Studies (August 26, 2025), https://www.csis.org/analysis/strategic-future-subsea-cables-japan-case-study

32 OregonFishermen's Cable Committee, Procedures to Follow While Operating Near Submarine Fiber Optic Cables (February 6, 2017), https://www.ofcc.com/Procedures2.6.17.pdf

33 *Supra* Note 10

34 Akitra, The Invisible Threat: How Quantum Computing Could Break Today's Encryption? (May 20,2024), https://akitra.com/the-invisible-threat-how-quantum-computing-could-break-todays-encryption/

35 Nachaat Mohamed, 'Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms' (2025) 67 (6969-7025) Knowledge and Information Systems < https://link.springer.com/article/10.1007/s10115-025-02429-y> accessed October 30 2025.

36 U.S Department of State, Clean Networks, https://2017-2021.state.gov/the-clean-network/

37 National Security Directive on Telecommunication Sector, https://trustedtelecom.gov.in/

38 Mouza Almarzooqi, Wired for Dominance: China's Undersea Cable Strategy, Trends Research and Advisory (August 08, 2025), https://trendsresearch.org/insight/wired-for-dominance-chinas-undersea-cable-strategy/

39 US Embassy and Consulates in India, Wavelength Forum Boosts Quad Collaboration on Subsea Cable Connectivity (July 16, 2025), https://in.usembassy.gov/wavelength-forum-boosts-quad-collaboration-on-subsea-cable-connectivity/

40 Rezaul H Laskar, Quad partners focus on strategies to protect subsea cables from threats, Hindustan Times (July 16, 2025), https://www.hindustantimes.com/india-news/quad-partners-focus-on-strategies-to-protect-subsea-cables-from-threats-101752672771792.html

41 Press Information Bureau Delhi, Economic Development of Union Territories, Press Information Bureau (April 02, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2117799

List of Participants

1. Sheela Kosaraju, General Counsel, Ciena
2. Amit Malik, Business Head (South Asia), Ciena
3. Major General Pawan Anand, Director, USI
4. Rahul Vatts, Chief Regulatory Officer, Airtel
5. Wing Commander Navin Kumar, Defence Policy and Armed Forces Wing, Ministry of Defence
6. Karnal Singh, Ex-Enforcement Directorate Chief
7. Dr. Sameer Guduru, Director, US-India Business Council
8. Lt. Gen. Anil Tandon, Director General, Broadband India Forum
9. Debashish Bhattacharya, Senior DDG, Broadband India Forum
10. Katyayinee Richhariya, Planning and Research Division, Ministry of External Affairs
11. Ebaad Khan, Manager, Meta
12. Kumar Deep, Country Director - India, Information Technology Industry Council
13. Sanjay Goel, ex-Ministry of Electronics and Information Technology
14. Admiral S.Chawla
15. Mohit Gupta, Expert
16. Atul Jain, Broadband India Forum
17. Vivan Sharan, Partner, Koan Advisory Group
18. Samrridhi Kumar, Legal Analyst, Koan Advisory Group
19. Dr. Ajai Garg, Advisor, Koan Advisory Group
20. Wing Cdr. Rajiv Anand, Senior Director, AMCHAM
21. Tarun Chitkara, Vice President - Regulatory Affairs, Airtel
22. Deepak Maheshwari, Sr. Policy Advisor, Center for Social and Economic Progress
23. Saurabh Puri, ADG, Cellular Operators Association of India
24. Dr. Shailendra Kumar Saxena, Director (Planning), Ministry of Defence
25. Capt. SS Parmar, Distinguished Fellow, USI

KOAN