National Maritime Foundation

https://maritimeindia.org/

A COLLABORATIVE INDO-PACIFIC ARCHITECTURE FOR THE PROTECTION OF CRITICAL MARITIME INFRASTRUCTURE

Captain KS Vikramaditya, Indian Navy

INTRODUCTION: WHEN INFRASTRUCTURE BECOMES STRATEGY

1. The Indo-Pacific is not simply a geographic designation. It is the beating heart of the global economy - a region that accounts for nearly two-thirds of global GDP, approximately 60 per cent of global maritime trade, and close to 70 per cent of seaborne energy flows.[1] Through its straits and sea lanes, trillions of dollars in goods, energy cargoes, and financial data move every day. The Strait of Malacca alone carries roughly 22 per cent of global maritime trade and handles over 100,000 vessel transits per year.[2] Undersea, a web of fibre-optic cables - carrying more than 95 per cent of intercontinental data traffic - links economies, military command structures, and financial systems in ways that are as consequential as any surface-level trade route.[3]

2. For most of the post-Cold War era, this infrastructure was treated as a backdrop to geopolitics rather than a subject of it. Ports were managed commercially, cables were laid by private consortia, and offshore platforms were secured primarily as industrial assets. The architecture of protection was designed for a world of accidental damage and localised disruption.

3. That world has changed. The deliberate severance of undersea cables in the Baltic Sea in November 2024 - attributed with high confidence to the Chinese-flagged bulk carrier Yi Peng 3 - marked a signal moment. Two cables were damaged within 24 hours: the BCS East-West Interlink connecting Sweden and Lithuania, and the C-Lion1 linking Finland and Germany.[4] These were not the first such incidents; since 2022, approximately ten subsea cables in the Baltic have been cut or disrupted, with seven incidents alone between November 2024 and January 2025.[5] In December 2024, the Estlink 2 power cable between Finland and Estonia was severed - a repair that ultimately

---

[1] United States Department of State, "Indo-Pacific Strategy," 03 June 2024. https://2021-2025.state.gov/indo-pacific-strategy/

[2] Huaxia, "Stability of Strait of Malacca Draws Spotlight Amid Global Chokepoint Tensions,", Xinhua News Agency, 08 May 2026. https://english.news.cn/20260508/f406941c8bcb432b910d235a3084d3c7/c.html

[3] Brendon J Cannon, "Undersea Cable Security in the Indo-Pacific: Enhancing the Quad's Collaborative Approach," *Marine Policy*, Vol. 171, January 2025. https://www.sciencedirect.com/science/article/pii/S0308597X24004159

[4] Kate O'Riordan, "Geopolitics of Baltic Subsea Infrastructure", Brussels Institute for Geopolitics, 11 April 2025. https://big-europe.eu/publications/2025-04-11-geopolitics-of-baltic-subsea-infrastructure

[5] Sophie Himaka, "Baltic Sea Undersea Cable Security," Henry M Jackson School of International Studies, University of Washington, 09 July 2025. https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/

took over seven months and cost an estimated €60 million.[6] These events did not occur in isolation; they occurred in a pattern, and that pattern speaks to a strategic logic.

4. The Indo-Pacific too is not immune to such disruption. The same structural conditions that enabled hybrid infrastructure warfare in the Baltic - diffused ownership, limited seabed monitoring, fragmented legal frameworks, and inadequate regional coordination - exist across the Indian Ocean and broader Indo-Pacific in even more complex forms. In the Taiwan Strait, Chinese-linked vessels have been implicated frequently in incidents concerning undersea cables.[7] In the Red Sea, Houthi attacks have disrupted multiple subsea cables, demonstrating that non-state actors can now impose significant costs on critical maritime infrastructure (CMI). Globally, over 200 submarine cable repairs are conducted annually, and while most involve accidental damage, the proportion associated with deliberate interference is rising.[8]

5. This article argues that the protection of critical maritime infrastructure in the Indo-Pacific has reached an inflection point. The architecture of risk has evolved faster than the architecture of protection. The challenge is not creation - many of the building blocks of a collaborative system already exist. The challenge is integration: aligning existing platforms, closing legal and capability gaps, and shifting the conceptual frame from asset-level protection to system-level resilience. The paper proceeds in five parts: a systemic definition of critical maritime infrastructure; a characterisation of the current threat environment; an analysis of structural gaps in existing frameworks; a five-pillar collaborative architecture; and a proposed implementation model.

FROM ASSETS TO SYSTEMS: REDEFINING CRITICAL MARITIME INFRASTRUCTURE

6. The conventional understanding of critical maritime infrastructure focuses on discrete physical assets such as ports and terminals, offshore oil and gas platforms, naval installations, and lighthouse networks. This asset-centric view reflects the historical origins of maritime security - a domain shaped by vessel-level incidents, port security protocols, and bilateral agreements governing specific facilities.

7. This framing is now inadequate. Maritime infrastructure today functions as a set of deeply interconnected systems spanning, what could be visualised as, discrete, yet frequently overlapping layers. Disruption to any single layer propagates across the others, producing cascading effects that are disproportionate to the original incident. A cyberattack on a port's digital management system does not merely cause operational delay - it degrades cargo throughput, distorts insurance pricing, and triggers downstream supply chain failures across multiple countries. A severed submarine cable does not merely reduce internet bandwidth - it may disrupt financial clearing systems, degrade military communications, and compromise the digital and navigational networks underpinning modern maritime operations.[9]

---

[6] Winston Qiu, "Repair of Estlink 2 Electricity Subsea Cable Costs Up to €60 Million," Submarine Cable networks, 28 May 2025. https://www.submarinenetworks.com/en/nv/insights/repair-of-estlink-2-electricity-subsea-cable-costs-up-to-%E2%82%AC60-million

[7] Alexander Lott, "The Baltic Sea Cable-Cuts and Ship Interdiction: The C-Lion1 Incident," Lieber Institute West Point, 26 November 2024. https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/

[8] Monty Khanna, "A Roadmap for Securing India's Undersea Cables," ORF Special Report No. 266, 27 June 2025. https://www.orfonline.org/research/a-roadmap-for-securing-india-s-undersea-cables

[9] Christian Bueger and Tobias Liebetrau, "Critical Maritime Infrastructure Protection: What's the Trouble?", Marine Policy, Vol. 155, Article 105772, September 2023. https://www.sciencedirect.com/science/article/pii/S0308597X23003056

8. A more adequate definition of critical maritime infrastructure must therefore encompass five functional layers (*Fig 1 refers*): a physical layer of ports, cables, platforms, and seabed infrastructure; a digital layer comprising control systems, data networks, and communication protocols; the energy layer of pipelines, LNG terminals, and offshore energy systems; the logistics layer of navigation routes, supply chain networks, and shipping lanes; and the governance layer of regulatory frameworks, international agreements, and institutional oversight mechanisms.

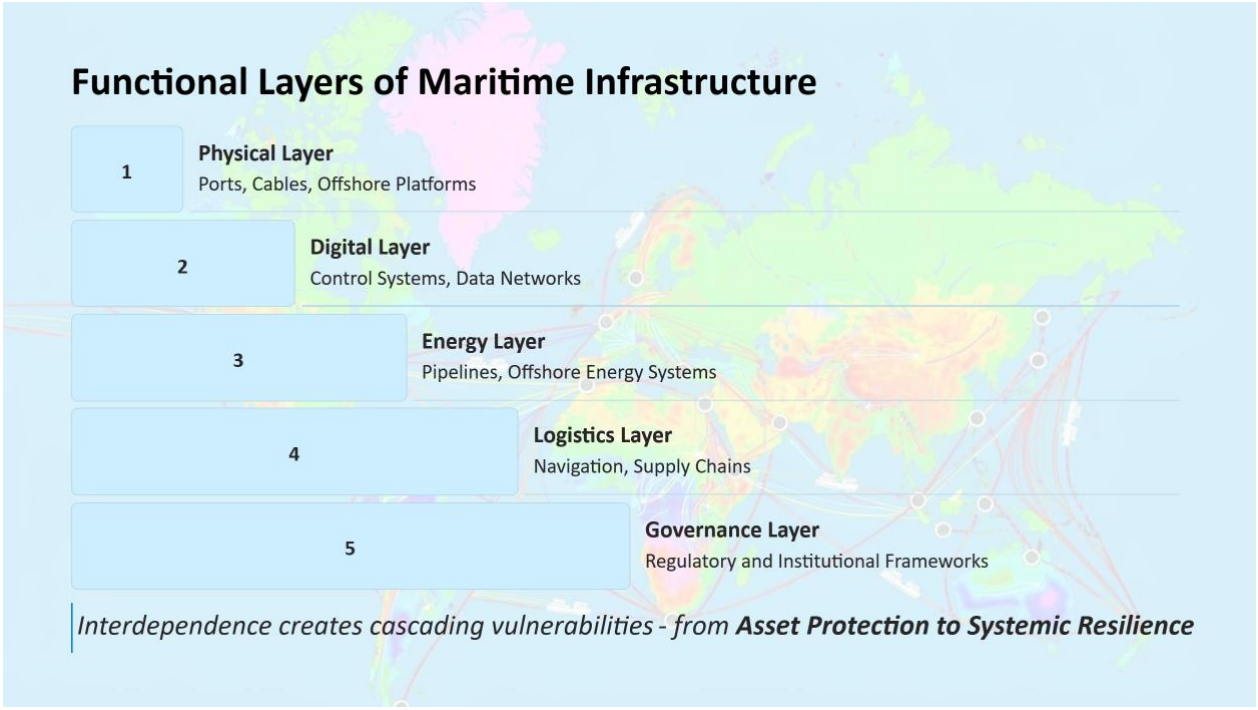

Figure 1: Functional Layers of Maritime Infrastructure
(Source: Author's own)

9. More importantly, what makes infrastructure "critical" is not its physical scale but its functional role: its centrality to system operation, its irreplaceability, its interdependence with other systems, and the concentration of risk it represents.

10. **Trends affecting Risk**. Four trends are compounding these risks simultaneously, creating a threat environment that is qualitatively different from anything the existing protection architecture was designed to address. First, growing *structural complexity*: the sheer density of maritime traffic, the proliferation of infrastructure nodes, and the deepening interdependence of global supply chains mean that the consequences of disruption propagate faster and further than before. Second, growing *digitisation*: the integration of digital systems into every layer of maritime operations - from port management to vessel navigation to offshore platform control - has dramatically expanded the attack surface and introduced cyber vulnerabilities into what were once purely physical domains. Third, growing *exposure*: commercially available satellite imagery, AIS tracking systems, and seabed mapping technologies mean that critical infrastructure is increasingly visible, precisely located, and traceable - by adversaries as much as by defenders. Fourth, *diffused ownership*: states, private operators, and foreign investors share ownership and responsibility for the same infrastructure in overlapping and often poorly coordinated ways, creating gaps in both accountability and response authority. The

cumulative effect is a paradox at the heart of modern maritime infrastructure: it is more efficient than at any point in history, and simultaneously more exposed and more vulnerable.[10]

11. India's maritime infrastructure provides a useful illustration of this complexity at national scale. With 11,098 kilometres of coastline, 12 major ports, over 200 non-major ports, at least 335 offshore platforms at any given time, and 17 active international submarine cable systems, India's maritime estate is vast, strategically located, and heavily interdependent.[11] The country hosts approximately 19 submarine cable landing stations concentrated primarily in Mumbai and Chennai, with an activated capacity of approximately 193 terabits per second - the nervous system of a digital economy projected to exceed USD 1 trillion in value.[12] Three new cable systems - 2Africa Pearls, India-Asia-Express, and India-Europe-Express - are expected to quadruple India's international bandwidth, deepening this dependence even as it expands it.[13]

12. Yet India currently lacks an indigenous cable repair vessel, relying entirely on foreign-flagged ships operating under complex regulatory clearance processes. Restoration timelines for cable breaks in Indian waters can extend to 50 days or more, reflecting not only logistical distance but also the friction of multi-agency clearance requirements.[14] India's vulnerabilities are not unique. In varying forms and degrees, similar dependencies, capability gaps, and coordination challenges exist across much of the Indo-Pacific littoral. The question of infrastructure protection cannot therefore be addressed state by state, layer by layer, or asset by asset. It requires a systems-level approach.

THE THREAT ENVIRONMENT: PERSISTENT, LAYERED, AND INTENTIONAL

13. The threat landscape facing critical maritime infrastructure has undergone a qualitative shift. Three dimensions of this shift merit particular attention.

From Incidental to Intentional

14. For most of the twentieth century, the principal threats to maritime infrastructure were incidental: fishing vessel gear, anchors of merchantmen, seismic events, shipping accidents, and storm damage. This framing shaped the legal and institutional response - focusing on accident prevention, insurance mechanisms, and bilateral repair arrangements rather than deterrence, attribution, or hardened defence.

15. The evidence now points clearly in a different direction. Three specific Chinese-linked incidents illustrate the emerging operational pattern with particular clarity. First, in February 2023,

---

[10] Su Wai Mon, "Protecting Critical Maritime Infrastructure: A Multi-Domain Approach to Maritime Security Governance," RSIS, 27 February 2026. https://rsis.edu.sg/rsis-publication/rsis/protecting-critical-maritime-infrastructure-a-multi-domain-approach-to-maritime-security-governance/

[11] Soham Agarwal and Cmde Debesh Lahiri, Retd, "Disaster-Resilience of Undersea Communication Cable Systems in India," National Maritime Foundation, 27 November 2024, https://maritimeindia.org/disaster-resilience-of-undersea-communication-cable-systems-in-india/

[12] Shruti Tripathi, "India Must Build 10x More Cable Landing Stations to Compete in Global Data Race," Outlook Business , 25 March 2025. https://www.outlookbusiness.com/start-up/india-must-build-10x-more-cable-landing-stations-to-compete-in-global-data-race-trai-chief

[13] Monty Khanna, "A Roadmap for Securing India's Undersea Cables"

[14] Soham Agarwal, "Enhancing Capacity-of and Capabilities-in Repair of Submarine Communication Cables through International Cooperation", National maritime Foundation, 14 May 2024. https://maritimeindia.org/enhancing-capacity-of-and-capabilities-in-repair-of-submarine-communication-cables-through-international-cooperation/

two undersea cables connecting Taiwan's main island to the Matsu Islands - located roughly 30 miles off the coast of mainland China - were severed within six days of each other by Chinese fishing and cargo vessels, cutting internet access for approximately 14000 residents for nearly two months.[15] Taiwan authorities identified the vessels involved; Beijing denied responsibility, attributing the damage to routine maritime accidents. Second, in January 2025, a Tanzanian-flagged vessel named Xingshun 39 - controlled by a Hong Kong company and crewed by Chinese nationals - disabled its AIS tracking transponder before dragging its anchor across a cable linking Taiwan to Asia and the United States; days later, a Mongolian-flagged vessel with a Chinese name was intercepted attempting a similar manoeuvre.[16] Third, in February 2025, the Hongtai 58 - a Togolese-flagged vessel with a Chinese crew and Chinese financing - severed a cable connecting Taiwan and the Penghu Islands; investigation of its voyage history revealed frequent flag and name changes and deliberate concealment of ownership, consistent with the operational profile of China's expanding shadow fleet.[17] A Taiwanese court subsequently convicted the Chinese captain of the Hongtai's precursor vessel of intentional cable damage.

16. These incidents share a common operational logic: commercially-flagged vessels, flags of convenience, AIS manipulation, plausible deniability, and the deliberate exploitation of gaps in attribution and enforcement - to achieve strategic effects below the threshold of armed conflict, in a legal environment that offers limited recourse to targeted states - the defining signature of grey-zone infrastructure warfare. By February 2025 alone, Taiwan had recorded five cable-disruption incidents in a single year - compared to three each in 2023 and 2024 - a frequency and pattern that left analysts at institutions from Stanford's SeaLight project to Taiwan's own Defence Ministry in little doubt about intent.[18]

Technology as Threat Enabler

17. The democratisation of sensing, monitoring, and autonomous systems has significantly lowered the barriers to high-impact infrastructure disruption. Commercially available satellite imagery, acoustic sensing capability, and AIS tracking systems allow non-state and state actors alike to develop detailed pictures of undersea infrastructure layouts, traffic patterns, and vulnerability nodes. Unmanned underwater vehicles - once exclusively the preserve of advanced military powers - are increasingly accessible for both reconnaissance and intervention at depth. AI-enabled analysis can now identify critical nodes and interdependencies in infrastructure networks at a level of precision that was previously unavailable to all but the most sophisticated intelligence services.[19]

18. The practical implication is a shift from general vulnerability to intelligent targeting. Infrastructure protection can no longer assume that adversaries lack the technical capacity to identify and exploit specific weak points with precision. The attack surface has expanded, and the barriers to exploiting it have contracted.

---

[15] Jason Hsu, "Testimony before the U.S.-China Economic and Security Review Commission", 02 March 2026. https://www.uscc.gov/sites/default/files/2026-03/Jason_Hsu_Testimony.pdf

[16] Timothy Boyle, "A New Strategy to Counter Chinese Sabotage of Taiwan's Undersea Cables", Just Security, 20 May 2025. https://www.justsecurity.org/113221/chinas-shadow-fleet-war-on-taiwans-undersea-cables/

[17] Jaime Ocan and Jonathan Walberg, "China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities", Global Taiwan Institute, 04 June 2025. https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities/
Also see: Timothy Boyle, "A New Strategy to Counter Chinese Sabotage of Taiwan's Undersea Cables"

[18] Timothy Boyle, "A New Strategy to Counter Chinese Sabotage of Taiwan's Undersea Cables"

[19] Divya Rai, "Safeguarding India's Submarine Cables," Chapter 14 in Edge of Competition: Disruption, Division, and Competition in the Indo-Pacific, Daniel K. Inouye Asia-Pacific Centre for Security Studies, 2025. https://dkiapcss.edu/wp-content/uploads/2025/08/CH-14-Safeguarding-Indias-Submarine-Cables_RAI_10.71236QAXD6468.pdf

Multi-Domain Interdependencies

19. Maritime infrastructure is no longer self-contained. Port operations, vessel navigation, and offshore platform management now depend on satellite-based positioning, terrestrial and undersea communication networks, and digital control systems that extend well beyond the maritime domain itself - creating interdependencies that neither traditional maritime security frameworks nor purely cyber-focused architectures were designed to govern. A disruption that originates in one domain propagates rapidly across others: physical damage to a cable degrades digital connectivity; digital interference with navigation systems creates physical consequences at sea and ashore; energy supply disruptions cascade into logistics and financial systems. Future threats, accordingly, are likely to be deliberately cross-domain - physically executed, digitally exploited, and spatially dispersed across jurisdictions and sectors. Protection architectures that address any single dimension in isolation will be structurally inadequate to this challenge.[20]

STRUCTURAL GAPS: WHY EXISTING FRAMEWORKS FALL SHORT

20. The Indo-Pacific is not without a maritime security architecture. The foundations that exist should not be underestimated. National maritime security and port protection frameworks are in place across the region. Institutional platforms supporting Maritime Domain Awareness are functioning. Regional cooperation mechanisms - information sharing, coordinated patrols, and capacity building - have demonstrated real and practical value. The challenge is not an absence of foundations - it is that the architecture of protection has not kept pace with the architecture of risk. Five structural gaps are particularly significant.

Fragmented Protection Architecture

21. The first gap is fragmentation. Maritime infrastructure operates as an interdependent system, but the protection mechanisms that govern it remain sectoral, siloed, and jurisdiction-bound. System-level risks, are in effect, being addressed through non-systemic approaches. That fundamental mismatch between the nature of the threat and the architecture of the response is the central structural problem that needs to be resolved.

Legal and Regulatory Inadequacy

22. The second gap is legal and regulatory. Existing structures were simply not designed for the threat environment that exists today. There is no framework of inter-state agreements to facilitate seamless, coordinated, and continuous action. Hot pursuit across maritime boundaries remains legally complex. UNCLOS provides the essential foundation, but complementary frameworks are urgently needed to address what it does not cover. Nowhere is this more true than in the case of undersea cables.

---

[20] GPSPATRON, "Maritime GNSS Interference Worldwide: A Cumulative Analysis 2025." https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/
Also see: IALA, "GNSS Jamming and Spoofing: Navigating Challenges in the Baltic Sea." https://www.iala.int/e-bulletin/gnss-jamming-and-spoofing-navigating-challenges-in-the-baltic-sea/

23. The international legal framework governing submarine cables rests primarily on UNCLOS Articles 112–115 and the 1884 Convention for the Protection of Submarine Telegraph Cables. Article 113 of UNCLOS requires states to criminalise the intentional or negligent damage of cables - but imposes no affirmative obligation to protect them, and applies penal sanctions only where states have enacted implementing legislation domestically, which most have not.[21] The 1884 Convention, though significant as the first multilateral instrument for cable protection, explicitly excludes actions taken by belligerents in wartime - an exclusion with obvious relevance to hybrid conflict scenarios.[22]

24. The enforcement gap is compounded by attribution difficulties. When damage occurs in Exclusive Economic Zones, coastal states have jurisdiction but face significant practical constraints - as the Yi Peng 3 case demonstrated, where Swedish and Finnish authorities launched criminal investigations but could not board the vessel without Chinese consent because it had moved beyond territorial waters.[23] As scholars of international maritime law have noted, "there is not a single regulatory regime for protecting subsea data cables," and the impracticality of continuous military patrol leaves enforcement almost entirely reactive.[24]

25. Safety zones around offshore infrastructure - typically 500 metres under existing frameworks - were designed for the hazards of the mid-twentieth century. They offer no meaningful protection against anchor dragging, UUV deployment, or precision targeting by adversaries who have pre-mapped the infrastructure.[25]

Surveillance and Awareness Deficits

26. The third gap is in surveillance and awareness. The underwater domain remains the least monitored of all maritime environments. While surface shipping is comprehensively tracked through AIS, radar networks, and satellite surveillance, the seabed environment - where cables, pipelines, and sensor systems lie - is largely invisible to real-time monitoring. Existing sensing capabilities are episodic rather than persistent, geographically uneven, and rarely integrated across national boundaries. The consequence is that infrastructure damage is typically detected only after the fact - when internet traffic degrades, energy flows cease, or pipeline pressure drops - rather than through early warning of anomalous behaviour near critical assets.[26]

27. This monitoring gap is not simply a technical problem. It reflects the absence of agreed protocols for data sharing, joint surveillance operations, and incident reporting among Indo-Pacific states. Regional Maritime Domain Awareness has advanced significantly in recent years - particularly through the setting up of information collation and fusion centres which have developed vibrant

---

[21] Kevin Frazier, “"On Protecting the Undersea Cable System," Lawfare, 24 January 2023. https://www.lawfaremedia.org/article/protecting-undersea-cable-system
Also see: Henrik Ringbom, “"New Threats — Old Rules: Law of the Sea Issues Raised by Suspected Attacks on Submarine Infrastructure in the Baltic Sea," Ocean Development and International Law, Taylor and Francis, 04 August 2025. https://www.tandfonline.com/doi/full/10.1080/00908320.2025.2534621

[22] Kevin Frazier, “"On Protecting the Undersea Cable System"
Also see: Alexander Lott, "The Baltic Sea Cable-Cuts and Ship Interdiction: The C-Lion1 Incident"

[23] Winston Qiu, "Finnish Court Dismisses Case Against Eagle S — Alleged Sabotage of Cables in the Baltic Sea," Submarine Cable Networks, 28 October 2025. https://www.submarinenetworks.com/en/nv/insights/finnish-court-dismisses-case-against-eagle-s

[24] Jacques Hartmann and Alexander Lott, "The Prosecution Gap for Attacks on Subsea Cables and Pipelines," EJIL:Talk!, 13 November 2025. https://www.ejiltalk.org/the-prosecution-gap-for-attacks-on-subsea-cables-and-pipelines/

[25] United Nations Convention on the Law of the Sea (UNCLOS), Articles 60(4)-(5) and 80. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[26] Christian Bueger and Tobias Liebetrau, "Critical Maritime Infrastructure Protection: What's the Trouble?”

international linkages and provide 24/7 regional information exchange.[27] But the current mandate of these centres is focused on surface shipping rather than maritime infrastructure, and their information networks, while substantial, do not yet constitute the persistent multi-layer surveillance architecture that infrastructure protection requires.

Coordination and Response Deficits

28. The fourth gap is a coordination and response deficit. The coordination and response deficit has two distinct but mutually reinforcing dimensions: an information gap and a response gap. Together, they ensure that even where individual states possess relevant capabilities, the absence of structured mechanisms transforms localised incidents into protracted crises.

29. The information gap is the more fundamental of the two. There is currently no dedicated, real-time, infrastructure-specific information network linking Indo-Pacific states. Existing maritime domain awareness channels are oriented primarily toward surface shipping, vessel tracking, and piracy-related incidents. They were not designed, and are not configured, to detect, flag, and share time-sensitive intelligence about anomalous behaviour near seabed infrastructure, cable corridor intrusions, or the early signatures of hybrid interference operations. The consequence is that disruptions are typically identified only after the fact - when bandwidth degrades, power flows cease, or cargo handling halts - rather than through early warning that could enable pre-emptive or intercept action.

30. The response gap follows directly. Joint response to infrastructure incidents requires, at minimum, rapid legal authorisation for vessel boarding, pre-agreed cross-border support arrangements, coordinated deployment of repair assets, and the kind of technical intelligence sharing that allows responders to understand the nature and extent of damage in real time. None of these currently exist in structured form across the Indo-Pacific. The Baltic Sea experience is instructive: the Newnew Polar Bear case in October 2023 demonstrated that even in a relatively institutionalised regional setting, the absence of NATO-wide infrastructure incident protocols meant the window for effective interception closed before coordination was achieved.[28] The Indo-Pacific, with its far greater jurisdictional diversity and the absence of an equivalent alliance framework, faces these challenges at substantially greater scale.

31. The implications are concrete and consequential: significant delays in the restoration of critical infrastructure following incidents, limited redundancy to absorb disruption while repairs are conducted, and virtually no surge capacity to handle simultaneous or cascading failures across multiple systems. These are not merely operational inconveniences - in a conflict-adjacent scenario, they represent strategic vulnerabilities of the first order.

The Public-Private Disconnect

32. The fifth gap, and one that is frequently overlooked, is the public-private disconnect. A structural feature of maritime infrastructure that complicates protection is the diffused ownership landscape. The majority of submarine cables are owned or operated by private entities - increasingly, the large hyperscale technology firms (Amazon, Google, Meta, and Microsoft now own or lease

[27] Indian Navy, "About Us — IFC-IOR". https://ifcior.indiannavy.gov.in/about_us
[28] Divya Rai, "Safeguarding India's Submarine Cables"

more than 50 per cent of global undersea bandwidth[29]), as well as telecommunications consortia and national operators. Offshore energy infrastructure involves overlapping private ownership, national licensing, and foreign investment. Port operations are frequently concessioned to international terminal operators.

33. Security responsibilities, however, remain predominantly state-centric. The mechanisms for integrating private infrastructure operators into national and regional security frameworks - for real-time incident reporting, information sharing, and coordinated response - remain underdeveloped. This disconnect creates a situation in which private operators hold the most granular knowledge of infrastructure vulnerabilities, while states hold the legal authority and enforcement capacity to act on them. Bridging this gap is a prerequisite for effective protection.

A FIVE-PILLAR COLLABORATIVE ARCHITECTURE

34. The foregoing analysis points toward the requirement of a coherent strategic response: the construction of a collaborative maritime infrastructure protection architecture that is systemic rather than sectoral, persistent rather than reactive, and functionally operationalised rather than merely declaratory. This architecture rests on five mutually reinforcing pillars depicted in Figure 2.

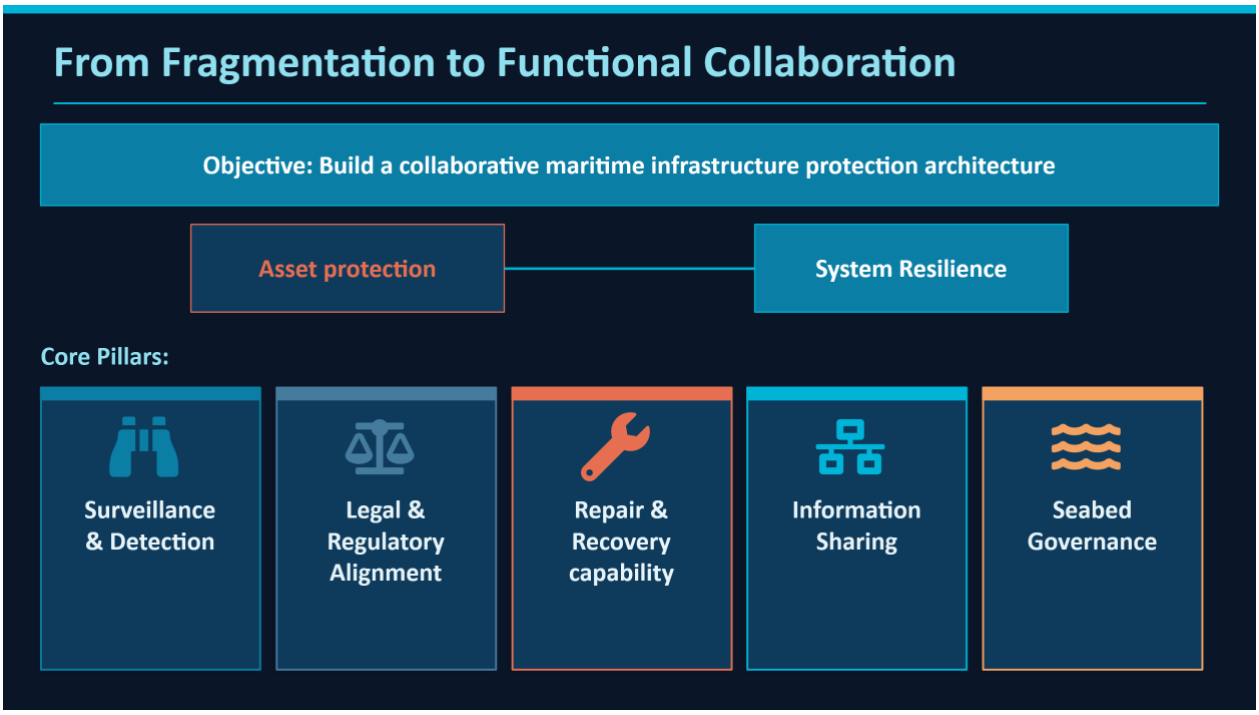

Figure 2: Five Pillar Collaborative Architecture
(Source: Author's own)

Pillar I: Enhanced Surveillance and Domain Awareness

[29] Daniel Runde, Erin Murphy, and Thomas Bryja, "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition", CSIS, August 2024. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240816_Runde_Subsea_Cables.pdf

35. Effective protection begins with knowledge - persistent, multi-layer awareness of the infrastructure environment and anomalous activities within it. The surveillance architecture required spans four domains: surface monitoring (extending existing AIS and radar networks with a specific infrastructure-centric information layer); subsurface sensing (deploying distributed acoustic sensing systems, seabed sensor networks, and UUV-enabled inspection regimes along critical cable and pipeline routes); space-based inputs (integrating commercial and government satellite imagery, synthetic aperture radar inputs, and other optical and electronic signature detection systems for wide-area monitoring of vessel behaviour near critical infrastructure); and cyber-domain monitoring (real-time tracking of anomalous activity in the digital systems that govern maritime operations).

36. Emerging technologies - particularly distributed fibre-optic sensing, which can detect acoustic anomalies along cable lengths, and AI-supported pattern recognition for vessel behaviour analysis - offer promising capabilities that should be integrated into a regional monitoring architecture.[30] The key governance challenge is not technical but institutional: establishing agreed protocols for data sharing across national boundaries, managing the *dual-use nature* of sensing technologies, and integrating private-sector infrastructure operators into the monitoring network.

Pillar II: Legal and Regulatory Alignment

37. The legal architecture must evolve alongside the operational and technological realities it governs. Several specific measures are warranted. First, Indo-Pacific states should undertake coordinated domestic implementation of UNCLOS Article 113, establishing clear criminal liability for infrastructure damage and agreed evidentiary standards for attribution in hybrid-threat scenarios. Second, bilateral and multilateral agreements should establish clear legal pathways for cross-border response - including incident reporting norms, boarding authority, hot pursuit provisions calibrated to infrastructure protection scenarios, streamlined clearance processes for repair vessels, and clarification of responsibilities in multi-actor scenarios. Third, safety zones around offshore infrastructure should be reviewed and, where warranted, extended, with enforcement mechanisms matched to the actual threat profile.

38. A longer-term priority is the development of a voluntary multilateral framework for seabed governance in the Indo-Pacific - addressing the transparency of seabed mapping activities, notification norms for vessels operating near critical infrastructure, and cooperative approaches to seabed resource access that reduce incentives for unilateral action. This framework should be developed through inclusive regional dialogue rather than imposed by any single state, reflecting the political diversity of the Indo-Pacific and the need for genuine buy-in from a wide range of stakeholders. This should aim to go beyond the UNCLOS and the BBNJ Treaty (Agreement on Marine Biodiversity of Areas Beyond National Jurisdiction),[31] and address lacunae that accentuate vulnerabilities.

Pillar III: Regional Repair Capacity and Recovery Architecture

39. **The General Problem (all infrastructure)**. The third pillar addresses a structural asymmetry that runs across all categories of critical maritime infrastructure: the gap between strategic importance and recovery capacity. Ports, offshore platforms, energy pipelines, and undersea cable

[30] Brendon J Cannon, "Undersea Cable Security in the Indo-Pacific: Enhancing the Quad's Collaborative Approach"
[31] IMO, "IMO welcomes entry into force of the BBNJ Agreement", 16 January 2026. https://www.imo.org/en/mediacentre/pressbriefings/pages/imo-welcomes-entry-into-force-bbnj.aspx

systems are each designed and operated to maximise efficiency and throughput - not to absorb disruption. When they fail, whether through deliberate attack, grey-zone interference, or cascading accident, the architecture for restoration is typically fragmented, nationally siloed, and reactive. No regional framework currently exists for the pooling of repair assets, the pre-positioning of critical spares, or the coordinated mobilisation of technical expertise across borders in response to infrastructure emergencies.

40. **National and Regional Action Framework**. Addressing this requires action at two levels. At the national level, states with significant infrastructure exposure - India prominently among them - should conduct systematic recovery gap analyses across each infrastructure category, identifying single points of failure, minimum redundancy thresholds, and the technical capabilities required for rapid restoration. These assessments should feed into national infrastructure resilience plans with explicit timelines, funding commitments, and inter-agency ownership. At the regional level, a cooperative recovery architecture should be established: a framework of pre-identified and mutually accessible repair assets, pre-positioned spares and inventory, streamlined cross-border access agreements, and standing technical teams that can be mobilised within days rather than weeks of an incident.

41. **Cables as the Priority Case**. Undersea cable systems represent the most urgent priority within this broader framework and illustrate with particular clarity both the scale of the gap and the feasibility of closing it. The asymmetry between the strategic importance of submarine cables and the availability of repair capacity is stark: India, for instance, relies entirely on two foreign-based consortia - in Singapore and Dubai - for cable repair services, with restoration timelines extending to 50 days or more.[32] States with significant cable dependence should prioritise the development of indigenous repair vessels and pre-positioned spare cable inventories as a near-term national capability investment.

42. **From National Capability to a Regional Pool**. At the regional level, however, national capabilities - however well developed - must be further amalgamated into a collective capacity pool that goes substantially beyond the current commercial arrangements in Singapore and the UAE. What is required is a structured regional recovery architecture: a framework in which nationally held repair vessels, technical teams, spare inventories, and access agreements are formally registered, mutually accessible under pre-agreed protocols, and deployable on a regional basis in response to any participating state's infrastructure emergency. The Quad's Cable Connectivity and Resilience Centre (CCRC) in Australia presents the most promising institutional anchor for such a pool.[33] Its existing mandate, multilateral legitimacy, and Indo-Pacific membership base make it well-positioned to evolve from a capacity-building hub into an operational coordination centre - maintaining the regional asset register, managing access protocols, facilitating joint exercises, and coordinating surge response when incidents occur. Formalising this expanded mandate, with dedicated resourcing and participation open to Indo-Pacific partners beyond the Quad itself, would represent a significant and concrete step toward genuine regional infrastructure resilience.

Pillar IV: Structured Information Sharing

43. Timely, accurate, and actionable information exchange is the connective tissue of any collaborative protection architecture. The current information landscape is characterised by bilateral

---

[32] Soham Agarwal, "Enhancing Capacity-of and Capabilities-in Repair of Submarine Communication Cables through International Cooperation"

[33] Australian Department of Foreign Affairs and Trade, "Cable Connectivity and Resilience Centre." https://www.dfat.gov.au/international-relations/regional-architecture/quad/cable-connectivity-and-resilience-centre

arrangements of varying quality, limited real-time capability, and almost no infrastructure-specific information channels. What is required is a dedicated infrastructure disruption reporting network - distinct from existing maritime domain awareness channels but linked to them - that enables rapid sharing of incident information, anomalous behaviour alerts, and infrastructure vulnerability assessments across regional partners.

44. The IFC-IOR represents the most developed regional information fusion capability and a logical anchor for this network. IFC Singapore provides a complementary hub for the Southeast Asian dimension. The critical enhancement required is an infrastructure-centric information layer - connecting these hubs to private infrastructure operators, national maritime information collation centres, and the capability development institutions described in Pillar V - and developing the common operational protocols necessary for information to flow rapidly enough to support time-sensitive response decisions.

Pillar V: Seabed Governance

45. The seabed is the most critical and least governed frontier of maritime infrastructure protection - and the one where the gap between strategic reality and legal framework is widest. Three international instruments nominally address this domain. UNCLOS establishes the seabed and its resources as the "common heritage of mankind" but provides no effective governance mechanism for the protection of the infrastructure that operates upon it.[34] The 2023 BBNJ Treaty advances the governance of marine biodiversity in the high seas but does not address the security of seabed infrastructure.[35] The International Seabed Authority, established under UNCLOS to regulate deep-seabed mineral resource extraction, has jurisdiction over resource exploitation but not over the cables, pipelines, and sensor systems that traverse the same seabed environment.[36] The result is a governance lacuna of considerable strategic consequence: commercial and military actors can map, approach, and interfere with seabed infrastructure in waters beyond national jurisdiction with minimal legal constraint, limited transparency obligations, and no regional enforcement architecture.

46. What the Indo-Pacific requires is a purpose-built regional governance edifice that goes beyond the lacunae in these existing instruments - not by replacing them, but by building a functional layer above them that is specific to the region's infrastructure protection needs. This edifice should rest on four normative pillars: first, mandatory transparency norms for seabed mapping and surveying activities conducted near critical infrastructure corridors, with notification requirements applicable to both commercial and government vessels; second, a regional infrastructure corridor protection regime, designating agreed exclusion or heightened-monitoring zones around critical cable and pipeline routes, analogous to - but extending beyond - the safety zones currently provided under UNCLOS; third, cooperative frameworks for the shared custody and management of seabed monitoring data, ensuring that information generated by national sensing systems is available to regional partners under agreed protocols; and fourth, a standing dispute resolution and incident attribution mechanism for infrastructure damage occurring beyond territorial waters, filling the enforcement void that the Yi Peng 3 and Xingshun 39 cases so clearly exposed.

---

[34] United Nations Convention on the Law of the Sea (UNCLOS), Article 136. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

[35] Hema Nadarajah, "The High Seas Treaty and the South China Sea: Canada's Role in a Contested Maritime Order", Asia Pacific Foundation of Canada, 14 May 2026. https://www.asiapacific.ca/publication/high-seas-treaty-and-south-china-sea-canadas-role-contested-martime-order

[36] International Seabed Authority. https://isa.org.jm/about-isa/

47. This is admittedly a long-term normative agenda. But it requires an institutional home and a political constituency to begin. The ARF, as the Indo-Pacific's primary inclusive multilateral security dialogue, is well-placed to serve as the normative platform for initiating this process - hosting the working group, building the consensus, and providing the political legitimacy that a purely technical or alliance-based framework could not command. The goal is not a new treaty, which the current geopolitical environment makes impractical, but a regional code of conduct for seabed infrastructure - voluntary, iterative, and inclusive - that establishes behavioural norms, builds transparency habits, and creates the political foundation for more binding arrangements over time.

OPERATIONALISING THE ARCHITECTURE: A LAYERED IMPLEMENTATION MODEL

48. The five pillars outlined above require institutional homes and political authority to function. The Indo-Pacific is fortunate in possessing a range of multilateral platforms that, taken together, can provide a layered implementation model matched to the different dimensions of the collaborative architecture. Rather than requiring new institutions, the model works with and through existing frameworks, cascading from political authorisation and normative consensus at the top to operational execution and technical capability at the base *(Figure 3 refers).*

49. At the ***normative and political layer***, the ASEAN Regional Forum, the East Asia Summit, and BIMSTEC each offer platforms for norm-building and confidence-building on infrastructure protection. The ARF's Inter-Sessional Meeting on Maritime Security[37] is particularly well-suited to advancing shared understandings of infrastructure vulnerability, agreeing on reporting norms, and building the political consensus needed to support more operationally specific arrangements - including, over the longer term, the regional code of conduct for seabed governance proposed under Pillar V. These forums cannot substitute for operational capacity, but they generate the political authorisation and normative legitimacy that operational capacity requires to function across diverse national legal systems and diplomatic relationships.

50. At the ***implementation layer***, the Indo-Pacific Oceans Initiative serves as the critical bridge between political intent and operational execution. Co-led by India and the United Kingdom on the Maritime Security pillar, the IPOI's seven-pillar thematic structure - spanning maritime security, trade and connectivity, disaster risk reduction, marine resources, marine ecology, science and technology, and capacity building - maps comprehensively onto the collaborative architecture proposed here.[38] No other regional framework combines this breadth of thematic coverage with the institutional depth and political buy-in that effective implementation requires. Leveraging synergies between the IPOI and the ASEAN Outlook on the Indo-Pacific (AOIP)[39] can further broaden the coalition of engagement, particularly with ASEAN member states that are simultaneously major cable hosts, significant energy transit points, and significant points of vulnerability.

51. At the ***operational layer***, infrastructure-centric monitoring through the IFC-IOR, IFC Singapore, and the emerging network of National Maritime Information Centres generates the common operational picture on which all response depends. The IFC-IOR, at Gurugram with over

---

[37] ASEAN Regional Forum, "Work-Plan for Maritime Security: 2022-2026". https://aseanregionalforum.asean.org/wp-content/uploads/2022/08/3.-ARF-Workplan-on-Maritime-Security.pdf

[38] 2025 Edition of the Indo-Pacific Regional Dialogue (IPRD-2025), "Concept Note", NMF. https://maritimeindia.org/indo-pacific-regional-dialogue-2025/

[39] "ASEAN Outlook on the Indo-Pacific". https://asean.org/wp-content/uploads/2021/01/ASEAN-Outlook-on-the-Indo-Pacific_FINAL_22062019.pdf

75 international linkages, is the most developed regional information fusion capability and the natural anchor for an infrastructure-specific information layer.[40] The critical enhancement required is the development of dedicated infrastructure disruption reporting protocols within these existing frameworks - connecting them to private infrastructure operators and enabling the time-sensitive information flows that coordinated response requires. NISHAR in Figure 3 stands for the Network for Information Sharing. This will be elaborated upon subsequently.

52. At the ***capability development layer***, two institutions merit particular emphasis. The proposed Regional Maritime Security Centre of Excellence (being established by the NMF in conjunction with Kings College London)[41] - focused on research, advocacy, and training on holistic maritime security - would provide the long-term intellectual and doctrinal infrastructure that the architecture requires: developing common frameworks for infrastructure threat assessment, training practitioners in cross-domain coordination, and generating the shared situational awareness concepts that underpin effective joint response. Complementarily, the Quad's Cable Connectivity and Resilience Centre in Australia, as argued under Pillar III, should evolve beyond its current capacity-building mandate into an operational coordination hub - anchoring the regional asset pool, managing cross-border access protocols, and coordinating surge response when incidents occur.[42]

53. From **detection to recovery**, the integrated execution model functions as a continuous cycle across all four layers. The normative layer provides the legal and political authorisation framework within which responses are legitimised. The implementation layer activates the thematic cooperation mechanisms through which resources and expertise are mobilised. The operational layer generates the situational picture, triggers information fusion protocols drawing on maritime, cyber, and space-based inputs, and deploys specialised assets - repair vessels, cyber response teams, and patrol assets - under pre-agreed cross-border frameworks. The capability development layer sustains all three layers above it through training, doctrine, and the regional asset pool. Recovery and continuity draw on pre-positioned assets and the regional repair architecture to restore critical services with minimum delay - and to feed lessons learned back into all four layers for continuous improvement - refining norms, recalibrating implementation mechanisms, improving operational protocols, and updating doctrine and capability requirements.

---

[40] IFC-IOR," https://ifcior.indiannavy.gov.in/about_us

[41] Siddhant Sibbal, "India pushes trust as anchor for Indo-Pacific security at key New Delhi forum", WION, 28 October 2025. https://www.wionews.com/india-news/india-pushes-trust-as-anchor-for-indo-pacific-security-at-key-new-delhi-forum-1761673847430

[42] Brendon J Cannon, Pooja Bhatt, "PacNet#8 - Policy Recommendations for Quad Cooperation on Submarine Cable Protection in the Indo-Pacific," Pacific Forum, 08 February 2024. https://pacforum.org/publications/pacnet-8-policy-recommendations-for-quad-cooperation-on-submarine-cable-protection-in-the-indo-pacific/
Also see: Asha Hemrajani, "The Quad Partnership for Cable Connectivity and Resilience", RSiS, 17 November 2023. https://rsis.edu.sg/rsis-publication/rsis/the-quad-partnership-for-cable-connectivity-and-resilience/

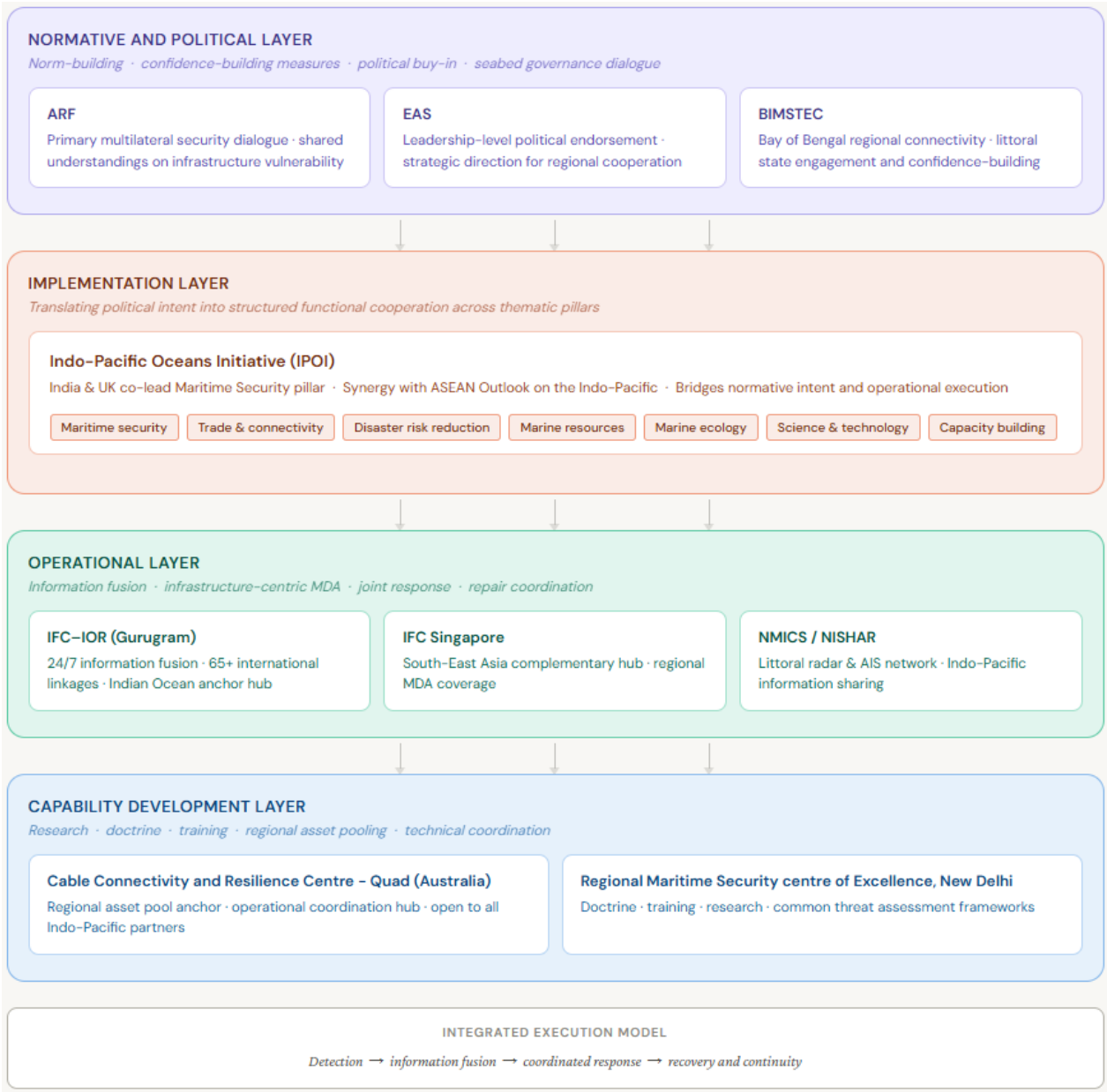

Figure 3: Implementation Mechanism
(Source: Author's own)

54. **India's regional Engagements**. India's existing regional engagements demonstrate that the building blocks of this architecture are already in place. India undertakes coordinated patrols (CORPAT) with Indonesia, Thailand, Myanmar, and Bangladesh and combined EEZ patrols with Mauritius and Seychelles.[43] The Indian Navy, in 2025, conducted an exercise and patrolling therein with the Philippine Navy also.[44] The Indian Navy recently designated an Offshore Patrol Vessel (OPV) as Indian Ocean Ship (IOS) Sagar, which sailed with a multinational crew from nine Indian Ocean island and coastal states. 44 personnel replaced the Indian crew in this endeavour.[45] The deployment of the ship also comprised the first Africa – India Key Maritime Engagement

[43] Rear Admiral Sushil Ramsay, retd, "Indian Navy Mission Deployed and Combat Ready", SP's Naval Forces, Issue: 06-2018 . https://www.spsnavalforces.com/story/?id=595&h=Indian-Navy-Mission-Deployed-and-Combat-Ready
[44] MoD, "INS Sahyadri Makes Port Call at Manila, Philippines", PIB, 27 November 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2195133&reg=3&lang=2
[45] MoD, "PR-EVENT BRIEF: INS SUNAYNA - MISSION IOS SAGAR", PIB, 05 April 2025. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2119169&reg=3&lang=2

(AIKEYME) which was co-hosted by India and Tanzania and focused on maritime security and information sharing.[46] Incidentally, this model is being repeated in 2026 with countries of South-East Asia.[47] India is reaching out to its partners to establish National Maritime Information Centres (NMICs) through the provision and setting up of cheap radar and AIS chains. India is also offering what the Indian Navy has coined NISHAR – the Network for Information Sharing, is a very cheap and easy to put in place connectivity tool that uses terrestrial networks and the INMARSAT to get into the fold shore-based centres, ships and aircraft. All these endeavours demonstrate that capacity building and institutional integration can advance in parallel.

INDIA AS AN ARCHITECTURE BUILDER

55. The architecture proposed in this paper is not a distant aspiration - several of its most consequential elements are achievable within the current policy cycle. What follows is a *phased plan of action* from India's perspective, organised across three time horizons. It is not a comprehensive to-do list but a sequenced prioritisation: actions chosen because they are specific, assignable, and build deliberately upon each other. India's role throughout is that of a persistent convener and architecture builder - not a unilateral actor, but the state with the strategic interest, institutional relationships, and regional credibility to initiate, sustain, and expand the collaborative framework that Indo-Pacific CMI protection requires. Each phase consolidates the gains of the preceding one before building the next layer, ensuring that the architecture deepens in capability and broadens in membership as it matures.

Short Term (0–18 months)

56. **Launch**.

(a) **Establish the RMSCE**. India to finalise host arrangements, mandate, and founding membership. The Centre's first work programme should focus specifically on critical maritime infrastructure threat assessment frameworks and a cross-domain coordination doctrine.

(b) **Table an infrastructure-specific agenda at the ARF ISM on Maritime Security**. India to propose a dedicated working group on CMI protection, with a mandate to develop agreed reporting norms and incident notification protocols among member states.

(c) **Commission a National CMI Recovery Gap Analysis** covering cables, offshore platforms, ports, and energy pipelines. Identify single points of failure, minimum redundancy thresholds, and indigenous capability shortfalls. Results to drive the medium-term investment plan.

(d) **Negotiate Bilateral Infrastructure Incident Response Agreements** prioritising Indonesia, Australia, Singapore, France (Réunion), and Mauritius. Focus on vessel boarding authority, repair ship access, and real-time information sharing on infrastructure anomalies.

---

[46] Indian Navy, "AFRICA INDIA KEY MARITIME ENGAGEMENT 2025". https://indiannavy.gov.in/content/africa-india-key-maritime-engagement-2025

[47] MoD, "Raksha Rajya Mantri Flags Off IOS SAGAR from Mumbai", PIB, 02 April 2026. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2248586&reg=3&lang=1

These early bilateral agreements are operational precursors to the model legal framework to be developed in the medium term - they establish working relationships and identify practical constraints that will directly inform that framework's drafting.

(e) **Initiate Expansion of the IFC-IOR Mandate**. Formally begin the inter-agency and diplomatic consultations required to add an infrastructure-centric monitoring layer to the IFC-IOR's mandate. Initiate establishment of direct data-sharing links with private cable and offshore platform operators and the development of an infrastructure disruption reporting protocol distinct from existing maritime incident channels. This protocol is conceived as the primary information intake mechanism for the future Indo-Pacific Maritime Infrastructure Centre (IPMIC) once established.

(f) **Initiate Procurement of an Indigenous Cable Repair Vessel**. Commission a feasibility study, identify build or lease pathway, and establish interim access agreements with Singapore and UAE consortia with guaranteed response timelines.

(g) **CMI Legal Alignment Study**. Commission a comparative analysis of domestic implementing legislation for the relevant UNCLOS articles across Indo-Pacific states, identifying which states have enacted legislation, what enforcement gaps exist, and what a model implementing statute would look like. India and Indonesia to lead the study in partnership with a regional legal institution such as the Asian-African Legal Consultative Organisation (AALCO)[48] or the National University of Singapore (NUS) - Centre for Maritime Law.[49] Findings to be circulated through the ARF working group proposed under para 56(b) and used to frame the medium-term bilateral negotiation agenda. In parallel, India to use the study as the basis for advocating domestic legislative reform in partner states, including through the RMSCE's training programme once operational.

57. **Prepare for the Medium Term**.

(a) Begin consultations with Quad partners on expanding CCRC mandate towards an operational coordination hub.

(b) Initiate drafting of a model bilateral seabed infrastructure notification protocol for tabling at the ARF.

(c) **Initiate exploratory consultations with Vietnam and Singapore** on the concept of a jointly established Indo-Pacific CMI coordination centre, co-led by India and Indonesia, anchored in ASEAN's existing cooperative frameworks. These consultations should gauge appetite for ASEAN co-ownership of such a centre and for a third ASEAN founding partner at the governance level. In parallel, India and Indonesia to jointly initiate informal outreach to all ten ASEAN member states on the concept of a nationally designated CMI coordination touchpoint - an existing national maritime authority tasked with aggregating domestic infrastructure incident data and maintaining liaison with private infrastructure operators. This outreach is deliberately preparatory: its purpose is to build familiarity with the concept, identify practical constraints in individual member states, and generate the political groundwork needed for a formal proposal at the medium-term stage. No institutional commitments would be sought at this stage.

[48] Asian African Legal Consultative Organisation. https://aalco.int/
[49] NUS, Centre for Maritime Law. https://law.nus.edu.sg/cml/

Medium Term (18 months – 04 years)

58. **Consolidate**.

(a) Formalise the bilateral incident response agreements negotiated in the short term into a broader multilateral framework through the IPOI Maritime Security pillar. These agreements address operational coordination arrangements. The legal instruments covering boarding authority and attribution standards would be developed concurrently under 59(j).

(b) Operationalise the RMSCE's first training cohort - drawing practitioners from ARF, BIMSTEC, and IPOI partner states. Feed outputs directly into IFC-IOR operational protocols. Include a dedicated module on domestic legislative implementation of UNCLOS, supporting the legal reform advocacy initiated under 56(g).

(c) Review and deepen IFC-IOR's infrastructure monitoring layer based on the first 18 months of operation - expand private sector integration and extend coverage to Southeast Asian cable corridors in coordination with IFC Singapore. Formally launch the infrastructure disruption reporting protocol initiated in 56(e) as the IFC-IOR's dedicated CMI information intake channel, designed to transition seamlessly into the IPMIC framework on its establishment.

59. **Build**.

(a) **Indo-Pacific Maritime Infrastructure Centre (IPMIC)**. Establish the *Indo-Pacific Maritime Infrastructure Centre (IPMIC)* - a dedicated CMI coordination authority jointly established and run by India and Indonesia, distinct from but operating in close institutional consonance with the IFC-IOR. The IPMIC should be proposed and established primarily through the ASEAN Outlook on the Indo-Pacific (AOIP), giving it genuine ASEAN institutional provenance rather than the character of an externally proposed initiative offered for ASEAN participation. A third ASEAN founding co-chair - Vietnam, given its strategic posture and cable infrastructure significance, or Singapore, given its operational capability and hosting of IFC Singapore - should be invited to join India and Indonesia as a core governance partner from the outset. Within the IPMIC framework, responsibilities would be distributed across four sub-regional nodes: India for the Indian Ocean Region; Indonesia for Southeast Asia; Japan for East Asia and the Western Pacific; and Australia for Oceania and the Southern Pacific. Each node would aggregate infrastructure incident data, coordinate local response assets, and maintain liaison with private infrastructure operators within its sub-region, feeding into the IPMIC through a common information framework. Critically, an **ASEAN CMI Focal Point** (described subsequently) should be designated in each of the ten ASEAN member states, feeding into the Indonesian node - giving every ASEAN member a defined role and institutional stake in the architecture, mirroring the ReCAAP national focal point model that has demonstrated the effectiveness of distributed ownership in regional maritime security cooperation. While the IFC-IOR retains its mandate for information fusion, maritime domain awareness, and operational coordination, the IPMIC would carry the regional CMI protection mandate specifically: managing the cross-border asset pool, coordinating recovery operations, integrating private sector infrastructure operators into a structured reporting and response framework, liaising with the CCRC on cable-specific technical dimensions, and driving implementation of the legal and governance frameworks developed under Pillars II and V. The two centres - the IPMIC and the IFC-IOR - would share a common information architecture, avoiding duplication while achieving the functional separation that effective CMI protection requires. The IPMIC should initially

function as a separate vertical within the IFC-IOR until it attains the consolidation and critical mass to commence operations as a distinct entity. Towards this, Indonesia must depute a Liaison Officer to the IFC-IOR who would also be the governing touchpoint for the IPMIC.

(b) **Propose a Regional CMI Asset Pool through the IPMIC and the Quad CCRC jointly**. The IPMIC to manage the broader infrastructure asset register covering ports, offshore platforms, and energy pipelines across all four sub-regional nodes; the CCRC, operating as the technical coordination arm of the Australian node, to retain lead responsibility for cable-specific repair assets and technical coordination. India and Indonesia to jointly lead the drafting of unified access protocols and surge deployment procedures. Membership would be open to all Indo-Pacific partners.

(c) **Deploy an indigenous cable repair vessel** and integrate it into the regional asset pool under agreed access protocols.

(d) **Launch NISHAR Network Expansion**. Connect National Maritime Information Centres across at least twelve Indo-Pacific littoral states with the IFC-IOR, with an infrastructure-specific data layer built in from the outset. Integrate commercial and government satellite imagery inputs into the network to provide wide-area monitoring of vessel behaviour near critical infrastructure corridors, addressing the space-based surveillance dimension of Pillar I.

(e) **Table a draft Indo-Pacific Infrastructure Corridor Protection Regime at the ARF** designating heightened-monitoring zones around critical cable and pipeline routes, with agreed vessel notification requirements. This is distinct from and complementary to the Safety Zone Enhancement Protocol at 59(k), which addresses point infrastructure. Both are voluntary and iterative in the first instance.

(f) **Establish a public-private infrastructure security council under the IPMIC** convening cable operators, port authorities, offshore energy companies, and national security agencies under a structured information-sharing and incident-reporting framework. India to host the inaugural meeting. This would be amongst the deliverables of the IPMIC's second year of operation, once the centre has achieved sufficient institutional consolidation to host and convene effectively.

(g) Negotiate expanded safety zones around India's offshore platforms and cable landing stations - seek bilateral reciprocity with key partners.

(h) Initiate a jointly operated seabed monitoring pilot along two critical Indo-Pacific corridors - provisionally the India-Singapore cable corridor and the India-Mauritius-South Africa corridor - combining distributed acoustic sensing, UUV-enabled inspection, and satellite integration. India to lead the technical framework and invite corridor partners to contribute sensing assets and data-sharing arrangements. Pilot findings to feed directly into IPMIC operational protocols and inform the design of the full regional monitoring architecture.

(j) **Negotiate a Model Bilateral Infrastructure Incident Response Legal Framework** covering boarding authority in relevant scenarios, hot pursuit provisions calibrated specifically to CMI incidents, streamlined repair vessel access protocols, and agreed evidentiary standards for attribution of hybrid and grey-zone attacks. India to

formulate the model framework bilaterally with Indonesia in the first instance, then circulate through the IPOI Maritime Security pillar and the ASEAN Outlook on the Indo-Pacific for broader Indo-Pacific adoption. The framework to draw directly on the findings of the CMI Legal Alignment Study commissioned in the short term and the operational experience generated by the bilateral agreements concluded under 56(d).

(k) **Table a draft Safety Zone Enhancement Protocol at the ARF** - proposing expanded protection zones around critical offshore infrastructure and cable landing stations, with enforcement provisions calibrated to current threat profiles including anchor drag, UUV operations, and precision targeting.
This addresses point infrastructure and is distinct from and complementary to the Infrastructure Corridor Protection Regime at 59(e), which addresses routes and corridors. This would be voluntary in the first instance, with a roadmap toward binding bilateral adoption.

(l) **Convene an ASEAN CMI Focal Points Network** under Indonesian leadership and within the IPMIC framework. Establish a structured network of nationally designated CMI focal points across all ten ASEAN member states. Each focal point to be responsible for aggregating national infrastructure incident data, liaising with private operators, and feeding information into the Indonesian node. India and Indonesia to jointly fund a capacity and capability building programme for focal point states with limited technical capability, administered through the IPOI Capacity Building pillar. The network to be formally launched at an ASEAN-hosted event, reinforcing ASEAN ownership of the architecture.

60. **Prepare for the Long Term**.

(a) Commission legal drafting of a regional seabed governance code of conduct for tabling at the EAS.

(b) Initiate discussions with the ISA and UN bodies on an Indo-Pacific addendum to the BBNJ Treaty addressing infrastructure protection.

(c) Commission a feasibility study on a regional infrastructure redundancy standard - examining minimum redundancy thresholds across cable, energy, and port systems for Indo-Pacific states; mapping the financing gap between current national capabilities and agreed thresholds; and exploring models for a cooperative financing mechanism drawing on precedents from existing multilateral infrastructure funds. Findings to be tabled through the IPMIC and the IPOI Capacity Building spoke as the basis for long-term standard-setting negotiations.

Long Term (4–10 years)

61. **Consolidate**.

(a) Formalise the Regional CMI Asset Pool under a legally grounded but non-treaty framework - analogous to the arrangements governing organisations like the ReCAAP Information Sharing Centre, which operates under a binding agreement but through an opt-in model that accommodates non-signatories.[50]

[50] ReCAAP Information Sharing Centre, "About ReCAAP ISC." https://www.recaap.org/about_ReCAAP-ISC

(b) Expand the RMSCE into a fully accredited regional training and certification institution - with standardised CMI protection curricula adopted across IPOI and ARF member states.

(c) Embed the infrastructure corridor protection regime into bilateral and multilateral maritime agreements across the Indo-Pacific - moving from voluntary notification norms toward enforceable standards. The accession experience of states committing to the corridor regime should be leveraged directly in the negotiations under 61(d).

(d) **Formalise the Model Bilateral Infrastructure Incident Response Legal Framework into a Multilateral Instrument**. Building on the bilateral agreements concluded in the medium term, India and Indonesia to jointly sponsor a multilateral CMI Incident Response Protocol through the ARF, open for accession by all Indo-Pacific states. The protocol to address boarding authority, hot pursuit, repair vessel access, and attribution standards in a single legally coherent instrument, filling the enforcement void that UNCLOS and the 1884 Convention have left unaddressed.

62. **Build**.

(a) **Conclude a Regional Seabed Governance Code of Conduct** negotiated through the ARF, anchored in UNCLOS and the BBNJ Treaty, addressing transparency of seabed mapping, vessel notification near critical corridors, shared custody of monitoring data, and a standing dispute resolution and incident attribution mechanism for infrastructure damage occurring beyond territorial waters.

(b) **Establish a Regional Infrastructure Redundancy Standard**. Agreed minimum levels of cable, energy, and port redundancy for Indo-Pacific states, with a cooperative financing mechanism for states lacking the resources to meet them independently.

(c) **Integrate CMI protection into the Indo-Pacific's broader security architecture** ensuring that infrastructure resilience is a standing agenda item at all the multilateral fora in the Indo-Pacific, a funded pillar of the IPOI beyond what the asset pool and IPMIC already provide, and a defined operational commitment within India's bilateral security partnerships.

(d) **Full-Spectrum Persistent Seabed Monitoring**. Expand the seabed monitoring pilot into full-spectrum persistent coverage across identified critical Indo-Pacific corridors towards obtaining a jointly operated regional picture accessible to all architecture partners through the IPMIC.

CONCLUSION: FROM PROTECTION TO SYSTEMIC RESILIENCE

63. Critical maritime infrastructure occupies a paradoxical position in the Indo-Pacific strategic order. It is simultaneously the region's most consequential vulnerability and its most significant strategic opportunity. The same cables, shipping lanes, offshore platforms, and port networks that adversaries are increasingly targeting as instruments of grey-zone coercion are also the foundations on which a collaborative regional security architecture can be built - and through which India and its partners can demonstrate that the Indo-Pacific's institutional density is equal to the sophistication of the threats it faces.

64. The challenge is not creation. The building blocks of an effective collaborative architecture are present. What these foundations currently lack is integration, coordination, and functional alignment - the connective tissue that transforms a collection of capable but loosely coupled institutions into a coherent, system-wide protection architecture.

65. Meeting that challenge requires protection to evolve along three axes simultaneously. First, from *reactive to anticipatory*: the current architecture responds to disruption after it occurs; the architecture required detects, deters, and where necessary intercepts before critical systems fail. Second, from *sectoral to system-wide*: infrastructure protection can no longer be addressed cable by cable, port by port, or platform by platform - it must be governed as an interdependent system in which disruption in one layer cascades rapidly across all others. Third, from *national to collaborative*: no Indo-Pacific state, however capable, possesses the surveillance reach, legal authority, repair capacity, and institutional leverage to protect critical infrastructure unilaterally - collective action is not merely preferable, it is structurally necessary.

66. These three evolutions, taken together, define what it means to move from protection to systemic resilience. The infrastructure is in place. The partnerships exist. The threat is present and growing. The architecture proposed in this paper - five pillars, four implementation layers, anchored in existing institutions and open to the full breadth of Indo-Pacific partnership - offers a practical pathway from where the region is to where strategic prudence requires it to be. The question is not whether the Indo-Pacific can build this architecture. It is whether it will do so before the next major infrastructure incident makes the cost of delay impossible to ignore.

Disclaimer: This paper reflects the personal views of the author and not those of either the Government of India, or, of the Indian Navy.