MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Red Sea Cable Cuts: Envisaging Operational Framework for Securing Critical Undersea Infrastructure

R. Vignesh

October 07, 2025

Summary

India has vital stakes in ensuring the safety of the rapidly expanding Critical Undersea Infrastructure (CUI) networks across the Indian Ocean Region. To safeguard its CUI in future years, India must lead in establishing strategic and operational frameworks complemented by developing robust domestic capabilities.

In the first week of September 2025, several nations across West and South Asia, including India, experienced significant internet outages caused by severing multiple undersea cables in the Red Sea. Initial suspicions quickly turned towards Yemen's Houthis rebels, who have been waging a sustained campaign of attacking commercial ships transiting the Red Sea. However, the International Cable Protection Committee (ICPC) suggested that the likely cause was accidental damage caused by commercial shipping activity.[1] The September incident, though, marked the seventh instance of undersea cable damage in the region since the Houthis launched their campaign in December 2023.[2] Even in their early stages of their campaign, the Houthis explicitly threatened to cut undersea cables in the Red Sea through social media channels.[3] Yemen's internationally recognised government has also repeatedly warned that the Houthis may attempt to damage undersea cables.[4]

In light of these facts, the potential involvement of the Houthis in past or future attacks on Critical Undersea Infrastructure (CUI) in the Red Sea cannot be ruled out. The incessant attack of the Houthis on commercial shipping has already led to the identification of the Red Sea as a High Risk Area (HRA) by various seafaring organisations. In this context, the growing threat to CUI, like internet cables, further undermines maritime security in a region that serves as a gateway to the Indian Ocean Region (IOR) and will have implications for India's strategic interests.

Presently, the Red Sea, the Baltic Sea and the Taiwan Straits have emerged as global hotspots where severe damage to CUI has considerably increased, raising suspicions of possible subversive malicious activity. In January 2025, NATO launched a new multinational naval mission in the Baltic Sea, known as 'Baltic Sentry', to protect CUI from intentional sabotage.[5] Assessing this mission can provide crucial insights into developing an operational framework for securing CUI in India's maritime areas of interest.

Critical Undersea Infrastructure in the Crosshairs

CUI generally refers to the network of undersea cables and pipelines laid across the vast seabed, through which data and energy resources are transmitted. Since the first submarine cable was laid across the English Channel in 1850 to connect Britain

[1] Jon Cambrell, **"Commercial Shipping Likely Cut Red Sea Cables That Disrupted Internet Access, Experts Say"**, Associated Press, 9 September 2025.

[2] Jay Hilotin, **"Red Sea Cable Chaos: Why the Internet Didn't Go Dark"**, *Gulf News*, 10 September 2025.

[3] Emily Milliken, **"The Next Casualty of the Red Sea Attacks: Undersea Cables"**, Gulf International Forum, 29 January 2024.

[4] Frank Gardner, **"Could the Houthis Sabotage Undersea Cables?"**, *BBC*, 7 February 2024.

[5] **"NATO Launches 'Baltic Sentry' to Increase Critical Infrastructure Security"**, NATO, 14 January 2025.

and France via telegraph, undersea cable networks have become the nerve centre of today's global world order. As of 2025, over 500 operational submarine telecommunications cables spanning over 1.7 million square kilometres worldwide, through which nearly 99 per cent of digital communications, including internet, telecom and financial transactions, are transmitted.[6]

These vast global networks of undersea cables are highly susceptible to damage by human activities in the underwater environment, such as deep-seabed mining and bottom trawling. Accidentally damaging these cables can lead to significant global or regional communication grid disruptions, affecting economic activities and national security. Besides cables, underwater oil and gas pipelines are also emerging as major arteries of global energy connectivity. They enable cost-effective transportation of large volumes of crude oil and natural gas across vast geographic distances.

The sabotage of the Nord Stream pipeline in the Baltic Sea in 2022 highlighted the threat posed to these underwater cables and pipelines from deliberate attacks by subversive state or non-state actors. Developing highly advanced deep-sea cable-cutting technologies by nations like China[7] underscores the growing likelihood of CUI being targeted as a military tactic by state or non-state actors for waging grey-zone warfare.

Three factors make CUI a convenient target for subversive attacks, whether by state or non-state actors.

1. **Unprotected Nature of the High Seas**: The vastness and ungoverned nature of the high seas in which these critical underwater infrastructures are located make them inherently vulnerable to subversion and sabotage.

2. **Ease of Execution**: These submarine cables and pipelines can be damaged by employing the most rudimentary methods. For instance, a perpetrator can use a commercial ship to deliberately drag its anchors over known submarine cable locations, thereby damaging them with minimal effort or risk.

3. **Anonymity & Deniability**: The vast expanse and remote locations of these critical undersea infrastructure allow the perpetrators to attack them with a high degree of anonymity. Also, a combination of factors, including the lack of governance of the high seas and the susceptibility of these installations to accidental damage by commercial shipping activity, provides plausible deniability to the perpetrators.

---

6 **"International Summit Outlines Steps to Improve Resilience of Submarines Telecommunications Cables Worldwide"**, International Telecommunications Union, 17 February 2025.

7 Stephen Chen, **"China Unveils a Powerful Deep-Sea Cable Cutter that Could Reset the World Order"**, *South China Morning Post*, 22 March 2005.

As a result of these factors, over the past few years, there have been increasing instances of CUI being targeted and damaged by unidentified actors. This trend is particularly evident in maritime spaces near littoral regions experiencing conflict or geopolitical tensions, such as the Baltic Sea, the Taiwan Straits and the Red Sea. Since October 2023, there have been at least 11 reported instances of damage to submarine cables in the Baltic Sea.[8]

Taiwan, for instance, has been grappling with the issue of frequent undersea cable disruption, possibly caused by sabotage. Between 2019 and 2023, Taiwanese authorities reported 36 cases of submarine cables being damaged by suspicious foreign vessels.[9] As of 2025, two incidents of undersea cable damage have already been reported, with indications suggesting possible intentional sabotage.[10] In June 2025, Taiwan sentenced a Chinese national to three years in prison for intentionally damaging its undersea cable. This persistent threat has prompted the Taiwanese Navy and Coast Guard to launch 24-hour patrols on 11 September 2025 to continuously monitor the 24 undersea cables critical to Taiwan's internet connectivity.[11]

NATO's Baltic Sentry

The Baltic Sea is a large semi-enclosed maritime space spanning nearly 3,77,000 square kilometres and is accessible through three narrow chokepoints. The ten littoral states of the Baltic Sea include Russia, Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Norway, Poland and Sweden.[12] The Baltic Sea is a crucial corridor for global maritime trade as nearly 15 per cent of international container shipping transits through this region, which accounts for approximately 2,500 vessels daily.[13] Additionally, the area hosts a vast network of CUI, including undersea cables and pipelines crucial for communication and energy connectivity between the Baltic region and Western Europe.

Over the past few years, the Baltic Sea has emerged as a flashpoint of strategic tensions between NATO and Russia, especially after the latter's actions in Crimea in

[8] John Leicester and Emma Burrows, **"At Least 11 Baltic Cables have Been Damaged in 15 Months, Prompting NATO to up its Guard"**, Associated Press, 28 January 2025.

[9] Koh Ewe and I-ting Chiang, **"Taiwan Jails China Captain for Undersea Cable Sabotage in Landmark Case"**, *BBC*, 12 June 2025.

[10] Gahon Chia-Hung Chiang, **"Countering China's Subsea Cable Sabotage"**, Global Taiwan Institute, 19 March 2025.

[11] Yimou Lee, Fabian Hamacher and Ann Wang, **"Exclusive New China 'Grey-Zone' Threat, Taiwan Steps Up Sea Cable Patrols"**, *Reuters*, 11 September 2025.

[12] Enrico D'Ambrogio, **"Baltic Sea Region"**, Baltic Sea States Subregional Co-operation (BSSSC), October 2022.

[13] Julian Pawlak, **"Charting the Challenges in the Baltic Sea"**, *War on the Rocks*, 21 May 2024.

2014. Subsequently, these tensions have further escalated since the outbreak of the Ukraine War in February 2022. Since then, there has been a notable increase in damage to the undersea cables and pipelines in the region, raising suspicion of intentional sabotage. NATO has attributed these incidents to the activities of Russia's so-called 'Shadow Fleet' operating in the Baltic Sea, thereby accusing Moscow of waging grey zone warfare by targeting CUI in the region.

The term 'shadow fleet' has been used by NATO and the European Union (EU) to refer to Russia's alleged use of commercial vessels to conduct shipping operations aimed at circumventing Western sanctions imposed after the outbreak of the War in Ukraine. The shadow fleet primarily comprises ageing commercial ships that operate on the high seas under the Flag of Convenience (FOC). This is a practice where vessels sail under a country's flag other than their own.[14] Additionally, these vessels are deliberately registered in a manner that presents dubious information regarding their ownership and operators. This makes tracing the origin and ownership of such vessels very challenging. Such vessels also have suspicious movements at sea, typically characterised by Automatic Identification System (AIS) blackouts, falsified positions, and transmission of false data and other deceptive techniques.[15]

These are the vessels that NATO has accused of indulging in the intentional sabotage of CUI in the Baltic Sea. NATO has substantiated this claim by citing the case of the oil tanker Eagle S seizure by Finnish Authorities in December 2024. While transporting oil from Russia across the Gulf of Finland, this vessel dragged its anchor along the seabed for approximately 90 kilometres. According to Finnish authorities, this caused damage to five undersea cables near Finland.[16]

To address this security challenge, NATO launched a coordinated naval operation, Baltic Sentry, on 14 January 2025, involving the navies of Germany, Sweden, Finland, Latvia, Lithuania, Estonia and Poland. This multinational operation aims to secure the CUI in the Baltic region by focusing on three key vectors, which are as follows:

1. **Establishing Deterrence through Conspicuous Naval Presence**: NATO aims to establish a sustained naval presence along key Sea Lanes of Communication (SLOC) in the Baltic Sea to deter suspicious actors from sabotaging CUI in the area. Operation Baltic Sentry essentially encapsulates a 'deterrence by denial' strategy. The forward deployment of NATO's naval

[14] **"Flags of Convenience"**, International Transport Workers Federation.

[15] **"Russia's 'Shadow Fleet': Bringing the Threat to Light"**, European Parliamentary Research Service (EPRS), November 2024.

[16] Miranda Bryant, **"Finland Charges Tanker Crew Members with Sabotage of Undersea Cables"**, *The Guardian*, 11 August 2025.

platforms is intended to create a posture capable of mounting a swift and robust response to any attempts to sabotage CUI in the Baltic Sea. [17]

2. **Sustained Monitoring through Multi-Layered Surveillance**: In this operation, NATO has deployed various naval assets to enhance maritime situational awareness through multi-domain vigilance activity.[18] The assets employed include surface ships, maritime reconnaissance aircraft, submarines and naval drones. Integrating aerial, surface and sub-surface surveillance enables NATO's operational command centre to efficiently monitor critical SLOCs and vital areas of interest to detect suspicious activity.

   In July 2025, to further augment surveillance in this operation, NATO deployed several experimental unmanned systems in the Baltic Sea. These systems include Unmanned Aerial Vehicles (UAVs), Unmanned Surface Vessels (USVs), and Unmanned Underwater Vehicles (UUVs), which have been deployed under Task Force X. Through these initiatives, NATO seeks to reduce operating costs for sustained operation effectively, bridge surveillance gaps, and aid critical decision-making, thereby minimising response time.[19]

3. **Optimising Data Collation and Information Sharing**: The navies participating in Operation Baltic Sentry aim to streamline the collation of the vast amounts of data gathered from the diverse array of platforms deployed across the region. Integrating this data will significantly enhance their collective maritime domain awareness (MDA) and Underwater Domain Awareness (UDA) capabilities. This will enable them to accurately identify key zones of interest, including major shipping routes, critical maritime traffic junctions and the locations of CUI.

   Furthermore, NATO shares this information with other key stakeholders, such as allied navies, commercial shipping companies and regional port authorities. This is being done to facilitate the flow of intelligence inputs and improve overall maritime security coordination.[20] This will significantly enhance the situational awareness of participating navies, enabling them to detect and respond swiftly to any anomalies or suspicious activities.

---

[17] Klaudia Maciata, **"Fortifying the Baltic Sea – NATO's Defence and Deterrence Strategy for Hybrid Threats"**, *NATO Review*, 5 May 2025.

[18] **"NATO's Baltic Sentry Steps Up Patrols in the Baltic Sea to Safeguard Critical Undersea Infrastructure"**, NATO, 14 January 2025.

[19] **"NATO ACT Deploys Unmanned Vehicles for Surveillance in the Baltic Sea"**, *Naval News*, 8 July 2025.

[20] Klaudia Maciata, **"Fortifying the Baltic Sea – NATO's Defence and Deterrence Strategy for Hybrid Threats"**, *NATO Review*, 5 May 2025.

In the nearly ten months since Operation Baltic Sentry was launched, there has been no notable instance of sabotage of CUI in the Baltic Sea. NATO Commanders have highlighted this as a testament to the operation's success in securing CUI and deterring grey-zone warfare.[21] In light of this, the potential of adopting a similar operational framework to safeguard CUI in the IOR must be explored, should the need arise.

Envisioning an Operational Framework for the Indian Ocean Region

The assessment of NATO's Baltic Sentry prominently highlights that securing the vast maritime commons is beyond the means and capabilities of any single nation. Security on the high seas can only be achieved through collective efforts, as it enables resource pooling and ensures operations' long-term sustainability. Such collaborative maritime security efforts are not entirely new to the IOR. Over the past two decades, the IOR has witnessed the deployment of several multinational naval task forces to combat security threats, piracy and terrorism, particularly in the Western Indian Ocean. Like NATO's Baltic Sentry, the operational framework of these initiatives has been built on the fundamental pillars of presence, sustained monitoring and information-sharing. Several past and ongoing multinational naval operations in the IOR, such as Operation Ocean Shield and Operational Atlanta, have been based on an operational framework built around these three pillars.

However, securing the CUI would additionally require the incorporation of an underwater element to any collective maritime security effort. This has been made evident through the assessment of Baltic Sentry, in which UDA has been a key element of its operational framework. Maintaining sustained underwater surveillance is a highly resource-intensive operation that involves the deployment of several aerial, surface and sub-surface platforms. To this end, the employment of UAV, USV and UUV in Operation Baltic Sentry presents a viable solution. Given the resource constraints regional navies face in the IOR, incorporating these emerging technologies to bridge capability gaps becomes essential to any potential regional effort to secure CUI.

While the above measures play a crucial role in deterring and detecting acts of sabotage against CUI, it is also essential to establish clear rules of engagement. These rules, laid out as an operational framework, are necessary for guiding the interdiction and apprehension of vessels caught sabotaging CUI on the high seas. However, NATO's Operation Baltic Sentry lacks such a framework, limiting the scope of its

[21] Clement Ngu, **"NATO Effective in Patrolling Baltic Undersea Cables, Says Commander"**, *Nikkei Asia*, 25 August 2025.

operations to deterrence and monitoring. In the absence of a defined operational mandate, the ability of any multinational effort to secure CUI remains inadequate, as challenges will rise in responding to sabotage in progress on the high seas. Additionally, Elisabeth Braw points out the inherent operational constraints of NATO's Baltic Sentry arising from its reliance on purely military platforms. As a result, complexities are likely to arise when interdicting civilian vessels that may be used to sabotage CUI.[22]

In the IOR, this challenge can be addressed by incorporating enforcement strategies derived from existing operational frameworks, such as the Djibouti Code of Conduct (DCoC), which has been effectively used to combat piracy. Further, a robust enforcement mechanism in the high seas can only be achieved through integrating naval presence and surveillance with the elements of maritime law enforcement agencies, such as coast guards. A practical operational framework for protecting CUI in the IOR must rest on four key pillars: establishing deterrence through a credible naval presence. Second, sustained surveillance incorporating UDA is enabled by advanced technologies. Third, the facilitation of comprehensive information-sharing among key regional stakeholders. Finally, the development of robust enforcement protocols to guide the interdiction of vessels engaged in sabotaging CUI.

Securing the CUI in the IOR: India's Stakes

It must be noted that India was among the many nations that faced increased internet traffic latency due to the recent Red Sea Cable cuts. This was because the two cable networks cut in this incident include the SEA-ME-WE 4 and IMEWE, which connect India to West Asia and Europe. Several of India's leading Internet Service Providers (ISPs), including Airtel, Reliance Jio and Tata Communications, use these cable systems for internet distribution nationwide.[23] Although these cuts did not cause widespread disruption, they serve as a stark reminder that the resilience of India's communication networks is closely tied to the safety of undersea cables across the IOR. Also, this incident occurred when India was looking to expand its subsea cable infrastructure rapidly in the coming years.

This was highlighted by the Chairman of the Telecom Regulatory Authority of India (TRAI), Anil Kumar Lahoti, in his speech during the Subsea Cable Systems Conference held in New Delhi in March 2025. He stated that India urgently needs to rapidly expand its cable landing stations (CLS) to meet its growing data demands

[22] Elisabeth Braw, **"Can a Few Surveillance Ships Protect Cables and Pipelines from Sabotage in the Baltic Sea?"**, *DW News*, 6 February 2025.

[23] Aroon Deep, **"Indian Networks Face Higher 'Latency' to Europe Following Red Sea Cable Cuts"**, *The Hindu*, 8 September 2025.

and achieve its goal of becoming a global digital hub. CLS essentially serves as the gateway for data flow into the country, located on India's coasts, where undersea cables are linked to terrestrial networks. Lahoti pointed out that India currently accounts for just one per cent of global CLS and emphasised that it must be expanded tenfold to meet its growing data demands.[24]

Apart from cables, India has been exploring options of establishing undersea gas pipelines for energy connectivity with West Asia for several years. As of 2024, a feasibility study was being carried out to establish an underground gas pipeline of around 1,200 kilometres between India and Oman at an estimated US$ 5 billion for directly importing gas supplies from West Asia.[25] These developments clearly highlight how the security of CUI in the IOR is intricately linked to India's national interest in the near future.

Given these factors, India has vital stakes in ensuring the safety of the rapidly expanding CUI networks across the IOR. In a scenario where the safety of these CUI is endangered by intentional sabotage, India, as a key stakeholder in the IOR, has an inherent responsibility to lead regional efforts to safeguard them. To this end, India's efforts to protect CUI must be built around two key areas: fostering regional cooperation and enhancing capability development. As brought out earlier, securing the vast networks of CUI across the high seas requires the pooling of resources and information sharing among the key stakeholders of a region.

Therefore, in the future, India must focus on incorporating the operational components of CUI protection into its joint military exercises and coordinated maritime patrols with friendly foreign navies. Secondly, because safeguarding CUI is a tech-intensive process, India must prioritise investment in developing and acquiring indigenous UUVs and Underwater Remotely Operated Vehicles (UWROVs), which are critical for enhancing the Indian Navy's UDA capabilities. The Indian Navy's recent contract with an Odisha-based deep-tech start-up for developing indigenous UWROVs indicates that India has already initiated efforts in this direction.[26]

Beyond strategic and operational frameworks, ensuring the resilience of India's CUI networks requires building domestic capabilities, increasing private sector participation and formulating robust policy guidelines, particularly regarding undersea cables. These measures are necessary to create the necessary material

[24] Shruti Tripathi, **"India Must Build 10X More Cable Landing Stations to Compete in Global Data Race: TRAI Chief"**, Outlook Start-Up, 25 March 2025.

[25] Sowmya Sundar, **"$5bln India-Gulf Region Gas Pipeline Project Expected to Move to FEED Stage by Year End – Company Executive"**, *Zawya.com*, 21 March 2024.

[26] Mayank Singh, **"Indian Navy to Buy Underwater Remotely Operated Vehicles from Odisha-Based Startup"**, *The New Indian Express*, 18 September 2025.

capacities for undersea cable repairs in case of damage. This issue was prominently highlighted in India's first International Subsea Cable Systems Conference.[27] It must be noted that India does not possess cable-laying and repair ships. As a result, Indian network operators are forced to rely on foreign companies that own such specialised vessels to repair damaged cables in the undersea.

The situation is further complicated by the complex bureaucratic process involving multiple ministries to permit these foreign vessels to operate in Indian waters.[28] Hence, India must develop indigenous infrastructure, cable construction and repair expertise. This includes the acquisition of specialised cable-laying and repair vessels along with other related technologies. Also, to facilitate greater private sector involvement in this process, it is essential to offer targeted incentives and simplify complex policy guidelines.

Overall, the recent incidents of cable cuts in the Red Sea serve as a wake-up call, highlighting the urgent need to develop operational strategies in the IOR to secure CUI against threats of grey-zone warfare in the underwater domain. India must lead in establishing strategic and operational frameworks complemented by developing robust domestic capabilities to safeguard its CUI in future years.

[27] **"Key Takeaways from India's 1st International Subsea Cable Systems Conference"**, Broadband India Forum, 25 March 2025.

[28] Ibid.

About the Author

Dr. R. Vignesh is Associate Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses