

Tab 1

Invisible Arteries of Global Security: The Strategic Role of Submarine Cables

- By Panishthi Mishra & Riddhi Singh

Introduction

Undersea fibre-optic cables comprise the invisible backbone of the global digital economy. They transport 99% of transoceanic digital communications, including phone calls, texts, E-Mails, etc. These cables drive international business by facilitating the expansion of MNCs, outsourcing operations, and transmitting high-speed financial transactions connecting the globe. Stephen Malphrus, staff director at the U.S. The Federal Reserve Board, once stated that if the cable networks are disrupted, “the financial services sector does not ‘grind to a halt,’ rather it snaps to a halt.” Consequently, the reliability of undersea cables has been deemed “absolutely essential” for the functioning of governments and the enforcement of national security.

Worldwide, around 150-200 accidental or unintentional cable damages happen annually. Generally, cable damage is caused by human activities like, damages caused by fishing vessels and geological occurrences — earthquakes or ageing infrastructure. But over the years, increasing incidents of cable damages in sensitive and strategic chokepoints have raised concerns about the deliberate damages caused by foreign actors, revealing its vulnerabilities in terms of global security.

Internationally, legal frameworks were established to ensure protection of submarine cables, starting with the adoption of the International Convention for the Protection of Submarine Telegraph Cables(1884) and later through the United Nations Convention on the Law of the Sea (UNCLOS). But, emerging challenges such as cyber threats and hybrid warfare have revealed limitations in the existing legal framework.

This article delves into the inter-relationship between undersea cables and global security through aspects like strategic importance, vulnerabilities, and the evolving policy responses to protect critical submarine infrastructure. It includes three case studies of the Baltic Sea, Bab el-Mandeb (Red Sea), and Taiwan's cable resilience. Lastly, the article concludes by proposing policy recommendations to strengthen the security, resilience, and governance of undersea cable networks in an interconnected and contested international environment.

Baltic Sea

The Baltic Sea carries approximately 18% of Europe’s short-sea shipping trade, connects to the Kiel Canal and North Sea, and hosts data pipelines and critical energy. Its exceptional usage has rendered its underwater infrastructure vulnerable to power equations. Instances of vulnerability include disruption of the Nord Stream pipelines

(September 2022) and the Gulf of Finland's Balticconnector gas pipelines (October 2023).

The global security angle to undersea cables in the Baltic area can be understood by the Russia-NATO involvement in the region. Going back to their historic ties, even presently the two factions keep increasing their relative power against the other. But, Russia stands at a particular disadvantage because its naval forces have been largely underfunded since the end of the Cold War. This underfunding has forced Russia into a paranoia that the Baltic Sea could potentially transform into a NATO dominated area, which may also explain its war with Ukraine. But, that has not stopped countries like Finland and Sweden from joining NATO. Their addition has turned the Baltic area into a NATO Lake. Initiating a hot war against any of these NATO membership acquired states is impossible because of the Article 5 doctrine of the treaty.

Thus, it has turned to alternatives like targeting and disrupting undersea energy linkages across the Baltic and North Seas. Russia's renewed 2022 maritime doctrine reflects principles of hybrid warfare, focusing on elevating energy infrastructure through naval operations. This has taken place by the protection and development of offshore pipeline systems and energy infrastructure. Without wanting to convert it into a hot war which could potentially trigger Article 5, the doctrine pushes for mobilization training and readiness on the maritime field, thus identifying Russia as a grey zone actor. Through this, civilian, scientific, specialized, commercial fleets are treated as a means to an end of state power.

Investigative journalists from Denmark, Norway, Finland, Sweden (all surrounding the Baltic), revealed Russia has been actively mapping the North & Baltic Seas by a series of large-scale programmes on critical underwater infrastructure. Experts believe that these Russian activities are a possibility for future obstruction. Russian ghost ships and vessels identified for research and military purposes with regard to undersea infrastructure are not recent developments. This practice has been in operation since the 1990s and 2000s and sees a much stronger future specially in the background of the Baltic turning into a NATO Lake.

Bab-el-Mandeb

Carrying more than 95% of international communication and data & financial flows worth approx. \$10 trillion, the Bab-el-Mandeb is a digital chokepoint connecting three continents; Asia, Europe, Africa. Located between Yemen (Arabian Peninsula) and Djibouti-Eritrea (Horn of Africa); it provides a crucial connection between the Red Sea and the Indian Ocean.

The circumstances with Bab-el-Mandeb are two-pronged. On one end, the strait is affected by the Iran backed Houthis (Yemen) operating aggressive military campaigns against vessels travelling in the Red Sea. It launched approximately 100 missiles and drones at vessels traversing through it, since October, 2023, later antagonised by the Israel-Gaza Conflict. An important shipping company, Maersk, even suspended its shipping activities through the Suez Canal and Red Sea. The Houthis threatened to

attack ships (owned by Israeli businessmen and firms), travelling to Israel, regardless of their nationality.

The Southern Red Sea has observed damage to four cables; TGN, AAE-1, Seacom, Europe India Gateway, has possibilities of Houthis' involvement. Despite the speculations being refuted later by the Houthis and other investigations, the mere fact that the incident was linked to the damage caused by the anchor of a merchant ship of the militia through one of its usual surface operations reflects a high probability of involvement.

The consequences have been all encompassing; Meta and Google, leading two significant subsea fiber-optic cable projects (2Africa & Blue-Raman), passing through the Red Sea and Bab-el-Mandeb strait corridor, have met with obstructions due to regional instability and security risks. The Red Sea is indispensable for global communication. It siphons one-fifth of the globe's internet traffic, provides cost-effective, direct connections between Europe, Africa, Asia. The disturbances in Bab-el-Mandeb, in the background of the Hormuz Strait blockage, have forced countries to detour their shipments to alternative sea routes of communication like *around Africa*, which have proven costly.

The second prong is directly related to the China-USA axis. USA's infrequent attention to the Red Sea is being capitalized by China. Instead of pushing for a hot war, China can be interpreted as using a strategy similar to the one initiated in the Baltic Sea (with regard to Article 5 doctrine of NATO).

While Yemen has become a seat of competition between the two, Djibouti is a significant agent in this power equation. Located at the door of the Bab-el-Mandeb, Djibouti is home to 8 foreign military bases; USA, Japan, France. China's military presence here has been expanding in the recent past with the establishment of its first overseas military base in Djibouti (2017). While China portrays itself as operating within these military bases only for logistics, many observers and strategists view this with scrutiny due to the Chinese base being located a slender 7 miles away from USA's Camp Lemonnier.

Additionally, the Djiboutian-Chinese militaries have participated in joint military exercises and China has also upstaked its operations at the Doraleh Multipurpose Port. Djibouti established a 690 hectare mega port aided by the China Merchant Group & ZPMC. China's influence is so dangerously powerful, that upon its request, the Djiboutian government even denied US planes from flying low over its naval base.

The USA-China axis is directly linked to the situation of undersea cable infrastructure in Bab-el-Mandeb. China becoming a leading figure as a subsea cable provider and owner, has been centric to its Digital Silk Road ambitions, launched in 2015. It is targeting the economies of Asia, Africa, Pacific, and Middle East, and capturing 60% of the globe's fibre-optic cable market. This is something similar the Chinese have been doing in the Democratic Republic of Congo, by capturing 50-70% of copper and cobalt's production-operations activities - different fields, similar approaches.

Counter-actively, America, suspicious of Chinese involvement in monitoring and severing cable-run data using coastal landing stations for cables or software programs, has blocked Chinese companies from subsea cable projects. This can be backed by delays by China in granting permits, cable repair issues, etc.

Therefore, Bab-el-Mandeb is at mercy of a power equation involving Yemen, Iran-backed Houthis, China, and the USA.

Taiwan

In contemporary times, islands remain important to Internet Communication, as more than half of the nodes in Undersea Cable networks are still located on islands. One of them is Taiwan, an important island in the geopolitics of UnderSea Cables. Taiwan being one of the chokepoints, becomes vulnerable to the grey-zone aggression by China, as claimed by Taiwan.

One of the major interruptions was the damage to Matsu Undersea Cables. The incident unfolded with disruptions and damages caused to two submarine communication cables connecting Taiwan and Matsu. INDSR claimed the attacks were by CCP fishing vessels and unidentified ships. This undermined Taiwan's cyber resilience. Several think tanks and strategic institutes sought the interruptions to be a grey war tactic employed by China. Some regional and maritime policy think tanks highlight the operational ambiguity surrounding these incidents. However, a definitive public attribution remains contested internationally.

In response to the growing threat to the submarine infrastructure, Taiwan has adopted a Whole-of-Society Resilience (WOSR) approach. In this approach, the WOSR framework tries to combine stakeholders like government agencies, the armed forces, private telecommunications companies, civil society organisations, and local communities to build national resilience. The framework also helps in recognising submarine cables as critical infrastructure, the strategy also highlights communication redundancy through satellite connectivity and advocates for cloud-based data backups, resilient digital networks and emergency communication systems to ensure the continuity of essential services during disruptions. Taiwan through this approach combines technological redundancy with institutional coordination and public preparedness and seeks to reduce the impact of cable damage, enhance its capacity to recover from disruptions and strengthen deterrence against grey-zone coercion targeting its undersea communication infrastructure.

Taiwan's case study, thus, demonstrates the strategic importance of undersea cables as it can become a grey-zone tactic without escalating it into open and armed conflict. The disruptions exposed the vulnerabilities of Taiwan's submarine infrastructure

which illustrated that damages to submarine cable not only cause disruption in internet connectivity, rather the repercussions are beyond that. In response, Taiwan shifted its focus from repairing to an approach that encompasses the whole of the society, in order to build a resilient framework to combat the challenges posed by the destruction of cables and to counter grey-zone operations against the undersea critical infrastructure.

Policy Recommendation

The increasing strategic importance of submarine cables and the vulnerabilities posed by natural and human-induced threats leads governments to adopt a comprehensive resilience strategy that combines different aspects like technological, legal and geopolitical measures. The International Telecommunication Union (ITU) recommends resilience through three board pillars – first is timely deployment of and repair, second, risk identification and mitigation, and third, enhanced geographic diversity of connectivity.

First, governments should strengthen maritime surveillance and monitoring around critical submarine cable routes. The incidents in the Baltic Sea and around Taiwan demonstrate that cable damage is strategically in nature. Therefore an integrated satellite surveillance, Automatic Identification System (AIS) tracking, and intelligence-sharing mechanisms to be used to detect suspicious vessel activity and to enable rapid responses to potential threats.

Second, international cooperation should be institutionalised to improve incident response and cable repair. The regional organisations like NATO and the EU in the Baltic Sea area, as well as Indo-Pacific partners in the Taiwan Strait and multinational maritime coalitions operating in the Red Sea and Bab-el-Mandeb, should together establish joint contingency plans, and coordinate emergency repair operations.

Third, countries should diversify their cable routes and develop redundant communication infrastructure. The heavy dependence on a limited number of submarine cable systems is increasing vulnerability, so governments should encourage the construction of geographically diverse cable routes, establish multiple landing stations, and integrate satellite communications as an emergency backup to ensure continuity of essential government, financial, and telecommunications services during disruptions.

Conclusion

In contemporary times, the global economy has grown more dependent upon digital connectivity, transforming submarine cables from an invisible mode of

communication to a critical infrastructure in pursuit of global security. The three case studies discussed in the article highlight the problems faced by submarine cables. It tells that the strategic importance of undersea cables, for coordinated action at all levels, regional, national and international. In response, governments adopt resilience strategies that include enhanced maritime surveillance, rapid repair capabilities, and strengthened international cooperation under existing laws like the UNCLOS. The digital interdependence grows so does the requirement of, safeguarding submarine cable infrastructure becomes essential for ensuring economic stability, securing global communications, and international security. Therefore, the focus should be on building a more resilient submarine cable system rather than restoring damaged infrastructure.

References

1. Africanews. (August 13, 2024). Djibouti opens \$590 million world class mega port co-funded by China. Africanews.
<https://www.africanews.com/2017/05/25/djibouti-opens-590m-world-class-mega-port-co-funded-by-china/>
2. Barnes, J. (April 19, 2023). Russian ‘spy ships’ threaten to sabotage UK energy supply. The Telegraph.
<https://www.telegraph.co.uk/world-news/2023/04/19/russia-ukraine-war-spy-ships-europe-energy-infrastructure/>
3. Bruns, S. (December 20, 2023). From “Flooded Meadow” to maritime hotspot: Keeping the Baltic Sea Free, Open, and Interconnected. Carnegie Endowment for International Peace.
<https://carnegieendowment.org/research/2023/12/from-flooded-meadow-to-maritime-hotspot-keeping-the-baltic-sea-free-open-and-interconnected>
4. Byman, D., Jones, S. G., & Blanchette, J. (2024, December 11). Strengthening resilience in Taiwan. Center for Strategic and International Studies.
<https://www.csis.org/analysis/strengthening-resilience-taiwan>
5. Calabrese, J. (January 29, 2020). The Bab-el-Mandeb Strait: Regional and great power rivalries on the shores of the Red Sea. Middle East Institute.
<https://mei.edu/publication/bab-el-mandeb-strait-regional-and-great-power-rivalries-shores-red-sea/>
6. Chiriac, O. R. (November 28, 2022). The 2022 maritime doctrine of the Russian Federation: Mobilization, Maritime Law, and Socio-Economic

Warfare. Center for International Maritime Security.

<https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/>

7. Cooper, C. (May 3, 2023). NATO warns Russia could target undersea pipelines and cables. Politico.
<https://www.politico.eu/article/nato-warns-russia-could-target-undersea-pipelines-and-cables/>
8. Deni, J. R. (December 18, 2023). Is the Baltic Sea a NATO Lake?. Carnegie Endowment for International Peace.
<https://carnegieendowment.org/research/2023/12/is-the-baltic-sea-a-nato-lake>
9. Djibouti: Doraleh Multipurpose Port: Phase 1. (March 12, 2022). Djibouti: Doraleh Multipurpose Port: Phase 1. Business and Human Rights Centre.
<https://www.business-humanrights.org/en/latest-news/djibouti-doraleh-multipurpose-port-phase-i/>
10. European Parliament. (2022). Security threats to undersea communications cables and infrastructure – Consequences for the EU.
[https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA\(2022\)702557?utm](https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557?utm)
11. Gallagher, J. C. (2022). Undersea telecommunication cables: Technology overview and issues for Congress (CRS Report No. R47237). Congressional Research Service.
<https://www.congress.gov/crs-product/R47237>
12. Himka, S. (July 9, 2025). Baltic Sea undersea cable security. The Henry M. Jackson School of International Studies.
<https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/>
13. International Telecommunication Union. (2026). International Advisory Body on Submarine Cable Resilience: Report of the Working Groups 2026. International Telecommunication Union.
<https://www.itu.int/en/publications/gs/pages/publications.aspx?media=electronic&parent=S-IAB-WG-2026>

14. Institute for National Defense and Security Research No. (28 July 2023) Reports.
15. Joint Research Centre. (2025, February 21). Subsea cables: How vulnerable are they and can we protect them? European Commission.
https://joint-research-centre.ec.europa.eu/jrc-explains/subsea-cables-how-vulnerable-are-they-and-can-we-protect-them_en
16. Kalm, H. (May 29, 2024). NATO's path to securing undersea infrastructure in the Baltic Sea. Carnegie Endowment for International Peace.
<https://carnegieendowment.org/research/2024/05/nato-baltic-sea-security-nord-stream-balticconnector>
17. Kramer, F. D., Liff, A. P., et al. (2024, July 2). *Strengthening Taiwan's Resiliency*. Atlantic Council.
<https://www.atlanticcouncil.org/in-depth-research-reports/report/strengthening-taiwans-resiliency/>
18. Lecesce, G. (December 13, 2025). Chokepoints above and below the surface: The Red Sea's emerging infrastructure challenge.
<https://www.iai.it/en/publications/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge>
19. Leon, J. (November 17, 2025) Red Sea conflict forces Google & Meta to delay undersea cable projects. Android Headlines.
<https://www.androidheadlines.com/2025/11/red-sea-conflict-google-meta-to-delay-undersea-cable-projects.html>
20. Liff, A. P. (2025, May 27). Whole-of-society resilience: A new deterrence concept in Taipei. Brookings Institution
<https://www.brookings.edu/articles/whole-of-society-resilience-a-new-deterrence-concept-in-taipei/?utm>
21. Lisinski, K.V. (August 13, 2025). The Silent Cartel: How Chinese companies came to dominate critical mineral markets. New Lines Institute For Strategy And Policy.
<https://newlinesinstitute.org/tech-econ-sov-sec/the-silent-cartel-how-chinese-companies-came-to-dominate-critical-mineral-markets/>

22. Milliken E. (July 31, 2025). Djibouti is the next arena for the US-China competition in the Red Sea. Atlantic Council.
<https://www.atlanticcouncil.org/blogs/menasource/djibouti-is-the-next-arena-for-us-china-competition-in-the-red-sea/>
23. Milliken E. (n.d). The next casualty of the Red Sea Attacks: Undersea cables. Gulf International Forum.
<https://gulrif.org/the-next-casualty-of-the-red-sea-attacks-undersea-cables/>
24. Runde, D. F., Murphy, E.L., Bryja, Thomas. (August 16, 2024). Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition. Center For Strategic & International Studies.
<https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>
25. Schaller, C. (May 21, 2024). Russia's mapping of critical infrastructure in the North and Baltic Seas - International law as an impediment to countering the threat of strategic sabotage. BRILL.
https://brill.com/view/journals/nord/93/2/article-p202_002.xml#:~:text=20,of%20the%20Russian%20Federation%20states%3A
26. Singh, A. (December 6, 2024). A reminder from the Baltic on securing undersea cables. Observer Research Foundation.
<https://www.orfonline.org/research/a-reminder-from-the-baltic-on-securing-undersea-cables>
27. STAROSIELSKI, N. (2015). *The Undersea Network*. Duke University Press.
<https://doi.org/10.2307/j.ctv11smhj2>
28. TOI Staff. (December 9, 2023). In escalation, Houthis vow to target all Israel-bound ships in Red Sea. The Times of Israel.
<https://www.timesofisrael.com/in-escalation-houthis-vow-to-target-all-israel-bound-ships-in-red-sea/>
29. United Nations. (1982). United Nations Convention on the Law of the Sea.
[United Nations Convention on the Law of the Sea](#)

Tab 2

