RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 113 – 21 August 2023

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Enhancing the Resilience of Undersea Cables in the Indo-Pacific

By Elsa B. Kania

SYNOPSIS

Reducing the risks of damage to or sabotage of undersea cables is vital for maintaining communication and connectivity among countries around the world. However, mechanisms for effective coordination in securing such indispensable information infrastructure is limited. Indo-Pacific countries should give priority to building capacity for protection and repair of undersea cables and enhancing their long-term resilience.

COMMENTARY

In a world that is dependent on communication, deep-sea cables remain the traditional transmission means to stay connected regionally and globally. Yet, the world's heavy dependence on undersea cables can create systemic vulnerabilities with far-reaching consequences. Despite increased awareness about threats to such vital links, policy action is not commensurate with security challenges. Looking forward, prioritising the long-term resilience of this undersea information infrastructure will be critical for the interests of all nations.

Submerged but Significant

While the Internet can create the illusion of virtual and seamless connectivity, about 95-99 per cent of transoceanic digital communication is transmitted through undersea cables by most estimates. Despite parallel developments, such as satellite communications, deep-sea cables remain salient because of their high capacity, low latency, and reliable performance.

Internationally, the overall market for submarine cables is expected to continue growing, to reach over US$41 billion by 2032. Private companies have been at the forefront of the development of undersea cables, with network operators often

collaborating in consortiums – including technology companies such as Meta and Google.

At the same time, certain governments, such as the People's Republic of China (PRC), have prioritised investments in this critical information infrastructure. Beijing, in particular, has looked to support the participation of Chinese companies in undersea cable projects as an element of its "Digital Silk Road". Increasingly, the US government has become concerned about the risks of PRC influence in undersea cable networks and started actively pushing back against the involvement of Chinese companies in certain projects.

Concerns about such risks are not new. In fact, there is a long history of deep-sea cables becoming a mechanism for projection of power and influence or a focus for sabotage in conflict situations, including in World War I. This fraught geopolitics is likely to persist and can result in rerouting that could be disruptive, but they also provide opportunities for countries in the Indo-Pacific to shape future networks.

Risks of Damage

Undersea cables have been damaged on multiple occasions, whether accidentally, such as by anchors or fishing nets, or deliberately. For regulatory and financial reasons, a relatively common practice is to layer new cables upon existing pathways, which can create chokepoints where damage or disruption causes cascading vulnerabilities.

Indeed, today's highly interconnected network designs can lead to unforeseen consequences. For instance, the AAE-1 (Asia-Africa-Europe-1) cable, which extends 15,000 miles and has landing points in Hong Kong and Paris, left millions across multiple countries adversely impacted when a section of it that passed on land in Egypt was cut in June 2022. In fact, the impacts of the disruption apparently extended beyond AAE; concurrent disruptions to the SeaMeWe5 (Southeast Asia–Middle East–Western Europe 5) cable system that carries telecommunications between Singapore and France, occurred due to potential and previously unknown dependencies.

Within the Asia-Pacific, there are no regional policies or consistent requirements as yet to incentivise companies to diversify routes or improve security for existing deep-sea cables.

Several recent issues with undersea cables have also demonstrated the difficulty of repair. In late 2022 and through early 2023, Vietnam suffered damages to and the simultaneous malfunction of four of the five major cables the country depends on, which were "unprecedented occurrences" that caused severe internet slowdowns. Ultimately, the fifth cable was also damaged. The repairs were only fully completed around May and June 2023.

Dangers of Sabotage

Since the Russian invasion of Ukraine, concerns about the potential for undersea sabotage have increased. On 26 September 2022, the Nord Stream gas pipelines were attacked, in incidents of suspected sabotage. After reports and warnings of

Russian ships mapping sensitive undersea infrastructure, NATO has become increasingly concerned with these issues, launching a new centre dedicated to the protection of undersea cables and pipelines. The EU is also starting a collaborative programme, Critical Seabed Infrastructure Protection, which is exploring concepts including the use of undersea drones for security patrols around pipelines.

There have been longstanding concerns that undersea cables could also be an Achilles' heel for Taiwan. In February 2023, damage to undersea cables near Taiwan's Matsu Islands, attributed to the actions of Chinese vessels, provoked suspicions about sabotage. As a result, the Matsu Islands suffered a 50-day internet outage with major economic impacts. Over five years, these cables have been cut repeatedly, reportedly over twenty times.

In a conflict scenario, the PLA would likely enact an information blockade against Taiwan to achieve advantage in the cognitive domain. The PRC's calculations to sever the limited number of undersea cables Taiwan depends upon would almost certainly be a component of that campaign, which also could involve cyberattacks or targeting of cable landing stations. Such a move would have severe consequences for regional connectivity.

Gaps in Policy and Security

Although all countries remain highly dependent on undersea cables, not many governments have implemented policies to enhance security, resilience, and risk mitigation. In fact, for many states, it is often unclear which agencies of government have primary responsibility to protect such critical infrastructure. Moreover, there is often a disconnect between industry and government with regard to competing concerns or conflicting interests that arise at the intersection of national security and commercial considerations.

Inherently, such issues of critical infrastructure require not only coordination across multiple agencies of governance but also public-private partnership across national boundaries. The International Cable Protection Committee (ICPC), a non-profit consortium based in the UK, has promoted cooperation among commercial and governmental stakeholders on these issues. While ICPC is a critical contributor, its mandate is inherently limited. Ultimately, action from governments and improved mechanisms for international collaboration will be required to enable robust responses.

When cables require routine maintenance or urgent repairs, the process tends to be complex, expensive, and technically demanding. However, there has been persistent under-investment in repair capacity. This process requires cable repair ships, staffed by specialised crews and engineers and sometimes equipped with remotely-operated vehicles. Only a limited number of ships – estimated at fewer than 60 worldwide – are fully capable of repairing undersea cables. The workforce available is also limited. As such, repairs can take months to schedule, leaving affected communities without the information connectivity.

When undersea cables extend across different territorial waters and are subject to different national policies or regulations, repairs can be delayed or impeded. In 2019,

ASEAN released the "ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables", which sought to address these issues, including through articulating ASEAN states' commitment to "streamline and simplify" the process of applying for permits for cable repair. However, ASEAN has yet to announce more robust initiatives.

Implications and Opportunities

Going forward, to respond proactively to these challenges, there are actions that governments and regional or international organisations can take, including:

i. *Improve government policymaking and coordination on undersea cable protection*. Governments should clearly identify which agencies or inter-agency mechanisms are responsible for oversight, management, and protection of undersea cables. States also should introduce or update policies to improve the physical defence and cybersecurity of cable landing stations and streamline procedures for repairs at sea.

ii. *Invest in expansion and incentivise diversification of undersea cable networks in the Indo-Pacific*. More extensive investment in expanding and diversifying undersea cable networks can yield important returns. For instance, ASEAN could conduct a study to identify the risks associated with critical chokepoints for undersea cables in the region, such as the Straits of Malacca, and identify options for incentives to promote greater diversification of routes.

iii. *Promote partnership among regional governments and commercial stakeholders*. The "Quad Partnership on Cable Connectivity and Resilience" was announced in May 2023; such collaboration could be expanded beyond Quad partners to other Indo-Pacific countries for sharing of best practices and technical expertise. ASEAN could convene a working group and invite participation from companies involved in major undersea cable projects in the region to discuss security issues and coordinate repair capacity and practices.

iv. *Improve domain awareness and information-sharing on threats to undersea cables*. Indo-Pacific countries and industry stakeholders should explore ways to improve sharing of information and intelligence on threats, whether cyber or physical, to such cables.

v. *Build up regional capacity for cable repair*. Indo-Pacific governments could explore options to create a regional cable security fleet; invest in technical solutions, such as specialised unmanned systems; and/or collaborate on training and human capital development for cable repair. For instance, ASEAN could promote capacity-building by sponsoring specialised training for regional coast guards.

Elsa B. Kania was a visiting fellow at the Military Transformations Programme of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore, in 2022. Her research focuses on US-China relations, defence innovation, and emerging capabilities. She is a PhD candidate in Harvard University's Department of Government. Her views expressed here are her own.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg