PACNET

MULTILATERALISM KEY FOR DE-RISKING INDO-PACIFIC SUBSEA CABLES

PRATNASHREE BASU

Pratnashree Basu (pratnashree@orfonline.org) *is an Associate Fellow with the Strategic Studies Program and Centre for New Economic Diplomacy, Observer Research Foundation, India.*

Amid increasing concerns over espionage and geopolitical control, many countries are strategically bypassing Chinese subsea cables in the Indo-Pacific. Complexities surrounding subsea cables—fiber optic cables laid on the ocean floor, used for transmitting data across continents in the Indo-Pacific—are deeply entangled with geopolitical, technological, and security issues. Subsea cables are indispensable for global communications, transmitting over 97% of international data, including internet traffic, financial transactions, and government communications. This critical infrastructure forms the backbone of the digital economy, making it a critical asset and a point of contention. Disruptions, strategic or natural, impact regional economies heavily reliant on fast and stable internet connectivity, especially post-pandemic, and underscore the significant geopolitical and logistical hurdles faced by the global subsea cable industry.

Geopolitical implications

While natural disasters such as earthquakes, undersea landslides, and tsunamis can cause extensive damage to subsea cable networks by shifting the seabed, and in turn snapping or displacing cables, intentional sabotage represents a more pressing concern. Strategic disruptions, such as the deliberate cutting of cables, can isolate countries or regions and have severe repercussions affecting global trade, financial markets, and critical military and economic data flows. Data interception and espionage are other ways in which strategic leverage can be obtained without disrupting cables. Recent reports indicate that Chinese cable maintenance ships may be involved in tampering with international cables. It is estimated that subsea cables carry close to $10 trillion in financial transactions every day. Similarly, strategic control over these cables is essential, with disruptions potentially impacting fuel, power, and data significantly.

The deliberate targeting of subsea cables can serve as a form of hybrid warfare, wherein state and non-state actors use non-traditional means to achieve strategic objectives. For example, the intentional cutting of cables can be employed as a coercive measure in geopolitical conflicts, exerting pressure without overt military action. This approach can disrupt economic stability and operational capabilities, demonstrating the intersection of technology and geopolitics in modern conflicts. In April 2024, for instance, cables connecting Taiwan's Matsu Island were cut, allegedly by Chinese vessels. The disruption had immediate effects on the local population, cutting off internet and phone services, illustrating the potential for strategic isolation of regions through such acts.

The broader implication is the vulnerability of Taiwan's communications infrastructure, which could be a precursor to more extensive strategies to undermine Taiwan's stability. As Taiwan is a major player in the global semiconductor industry, disrupting its communication infrastructure could have a ripple effect on global supply chains, affecting industries worldwide, and potentially leading to a backlash from global markets and multinational corporations toward China. If the cutting of cables is seen as a precursor to or part of a military operation, it could lead to a severe escalation of tensions and potential military conflict, particularly with countries that have security commitments to Taiwan.

Circumventing China's subsea networks

Even as efforts to reduce dependencies on Chinese subsea networks continue, more than 20 cables connected to Chinese companies have either gone live or are planned to become operational in the Indo-Pacific region between 2021 and 2026. Unlike the semiconductor industry, where export controls led by the US have set back Chinese manufacturing and development by years, there are limitations to the restrictions that can be imposed when it comes to subsea cables, an area where Chinese firms already dominate. Moreover, while China's subsea cables share similar

vulnerabilities, the risk of deliberate disruption or espionage originating from China toward other countries is higher.

In recent years, subsea cables have played a crucial role in the technology competition between the US and China. Washington has established measures such as Team Telecom—to ensure that Chinese companies do not dominate the subsea cable industry—and intervened in several projects, such as the Southeast Asia-Middle East-Western Europe 6 cable, to prevent Chinese firms from securing contracts. These efforts include offering financial incentives for choosing US-aligned companies for their cable projects and imposing sanctions on Chinese firms underscoring fears of potential espionage and security risks associated with Chinese-controlled infrastructure. These moves have invited retaliatory measures from Beijing such as delays in cable approvals. For example, the Southeast Asia-Japan 2 cable project, involving Singtel, Meta, and Japan's KDDI, has been delayed due to slow permit approvals from Chinese authorities, citing national security concerns. Projects like the Apricot and Echo cables, for instance, are being developed to connect key regions while avoiding the South China Sea, albeit at higher costs due to longer and more complex routes.

Countries like Japan, Australia, and the US enhance subsea cable security through partnerships, regulatory measures, and strategic investments. Japan has proactively secured its subsea cable infrastructure through partnerships with the US, Australia, and Canada. Japanese companies are significant players in the industry, and the country supports international regulations to protect these assets. Singapore has incorporated regulations governing subsea cables into its bilateral Digital Economy Agreements with Australia and the United Kingdom. These standards include criteria for screening and certifying cable vendors to ensure secure data flows and could potentially serve as a model for similar initiatives.

The Philippines is set to become a key data hub with several upcoming cable projects, such as Apricot, Bifrost, PLCN, and CAP-1, featuring landing points in the country. These new connections will enhance route diversity and reduce latency for data traffic between Southeast Asia, North Asia, and the United States. Indonesia and Malaysia are expanding their subsea cable infrastructure to support economic growth and improve connectivity. These countries navigate geopolitical sensitivities by balancing relations with China and other global powers while participating in regional forums on cable security. Australia has taken steps to secure subsea cables through joint investments and strategic partnerships, emphasizing cybersecurity and developing contingency plans. To leverage its tech industry, South Korea, a key player in the global telecommunications network, has addressed the growing demand for high-speed and reliable internet connectivity. For example, KT Corporation is developing a 5.6k-mile subsea cable across the Indo-Pacific region with Savills Korea, connecting to countries like Japan, Taiwan, Indonesia, the Philippines, and Singapore.

Multilateral cooperation plays a crucial role in addressing these challenges. Regional partnerships like the Quadrilateral Security Dialogue are focusing on securing these critical infrastructures to counterbalance China's influence in the Indo-Pacific through joint investments, sharing best practices for cybersecurity, and developing contingency plans for disruptions. Additionally, organizations like the International Cable Protection Committee offer platforms for stakeholders to discuss security issues and enhance accountability mechanisms.

There is also a need for robust security measures through international cooperation. This includes deploying advanced monitoring systems to detect and respond to cable damages quickly, fortifying cables with protective sheathing, and establishing protocols for rapid repairs. Additionally, strategic redundancy, where multiple cables provide alternative routes for data transmission, is crucial to ensure continuity in case of disruptions. Countries and corporations therefore broadly adopt four types of responses to these disruptions—diversification of routes; strengthening international cooperation and coordinated response strategies; advanced monitoring systems and establishing protocols for rapid repairs; and devising stringent regulations to ensure secure data flows. As the demand for high-speed internet and digital connectivity continues to grow, addressing these challenges will be vital for the future of the region.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged.