Securing the backbone: Security challenges to and governance of submarine cables in the Indo-Pacific

Submarine cables form the backbone of international communication, responsible for 99 percent of international data traffic. Submarine cables are more feasible than satellites in terms of data transmission due to their high-capacity and low-latency. This means that fibre-optic cables are able to transmit large data volumes more rapidly and at relatively low cost compared with satellites. In an era where digital connectivity is the lifeblood of economies and societies, submarine cables play a pivotal role in facilitating seamless communication, commerce, and collaboration on a global scale. This intricate web of fibre-optic cables on the ocean floor transports internet traffic essential for trade, defence, diplomacy, healthcare, and entertainment and underpins daily activities such as data transfers, emails, voice calls, video conferences, and financial transactions.

In the context of global supply chains, the importance of submarine cables cannot be overstated, particularly in the dynamic and economically vital region of the Indo-Pacific. The Indo-Pacific is a bustling hub of trade and economy, encompassing vast maritime territories and hosting some of the world's largest and fastest-growing economies with increased demand for higher bandwidth.

Despite the importance of submarine cables to the global supply chain and economy, this critical infrastructure is vulnerable to attack and damage, both intentional and unintentional. Attacks on submarine cables can be physical due to human activities at sea or cyberattacks which target cable landing stations and the network management systems used to monitor the cables remotely. There are also significant gaps in the governance of submarine cables, particularly in terms of international regulations. Therefore, in order to protect this important digital supply chain infrastructure, three main areas need to be addressed by national governments in collaboration with industry players: physical security risks, cybersecurity risks, and governance and legal gaps. This can offer more comprehensive protection of submarine cables from human activities at sea.

Physical security risks

Submarine cables are vulnerable to a range of physical security risks due to their underwater placement and extensive geographical coverage. These risks can include accidental damage from ship anchors or fishing activities, intentional sabotage, and natural disasters such as earthquakes or undersea landslides. According to the International Cable Protection Committee (ICPC), the majority of cable damage is caused by unintentional human activities at sea, with fishing accounting for almost half of the cable faults. ICPC estimates that there are approximately 100 to 200 faults each year on the global submarine telecommunications cable network.

In the Indo-Pacific, several notable cases of damage to submarine cables in 2023 were reported in the waters of Guam, Taiwan, Vietnam, and the Solomon Islands. In February 2023, all five submarine cables that connect Vietnam globally malfunctioned simultaneously, impacting data flow, internet speed, and business operations. All five cables were only fully repaired by November 2023, as during this period, a section of the Asia-Pacific Gateway (APG) cable and the Asia-Africa-Europe 1 (AAE-1) cable connecting to Singapore broke down again soon after the initial repair.

Due to the lack of advanced surveillance and monitoring systems for undersea infrastructure, it is difficult for maritime law enforcement agencies to prevent deliberate cable damage, especially when the Automatic Identification System (AIS) is turned off. The AIS is used by maritime law enforcement agencies to monitor and track vessel movements in territorial waters and Exclusive Economic Zones (EEZs) by providing real-time information about ship positions, course, speed, and other relevant data. Maritime law enforcement agencies often discover damage to submarine cables in their jurisdictional waters only after incidents occur, which are mostly unintentional. Reports of these incidents are then shared by organisations such as the Information Fusion Centre (IFC) which notifies regional countries. Given that these cables often connect multiple countries across the region, damage can impact internet connectivity for those states as well.

Submarine cables can also become a security target, during peacetime or armed conflict. Cable damage could sever a state’s critical internet supply and international communications and intimidate an adversary. In February 2023, two submarine cables in waters off the Taiwan-controlled Matsu Islands were damaged by a Chinese fishing boat and a Chinese cargo ship, respectively, leaving the 13,000 residents

with limited internet connection for 50 days. Although there was no evidence indicating they were deliberate actions, some analysts claimed that the damage was grey-zone aggression by China which could have been planning to disrupt Taiwan's internet access. An internet outage in Taiwan could severely disrupt the global supply chain, as the island produces over 60 percent of the world's semiconductors. These semiconductors are essential components in the production of nearly all electronic devices, such as laptops and mobile phones. Furthermore, Taiwan is responsible for manufacturing over 90 percent of the world's most advanced semiconductors. Thus, any disruption in semiconductor production due to an internet outage would significantly impact international supply chains, causing delays and shortages of electronic products worldwide.

The increased utilisation of grey-zone tactics, amidst the geopolitical headwinds in the Indo-Pacific, suggests that submarine cables could readily become targets of state and non-state actors. Such tactics, while not culminating in outright armed conflict, possess the potential to exert influence and undermine global supply chains, communication, and stability.

Furthermore, repairing submarine cables is usually time-consuming and costly. In 2023, the average time to repair a cable was 40 days, which was influenced by factors such as weather, crew availability, and the time to obtain the permit. The cost of repairs averages between USD 1-3 million. One of the factors exacerbating the situation is that there is a global shortage of cable laying and repair ships and many of them are aging.

Out of the 60 cable ships listed by the ICPC as of February 2022, there were 20 vessels registered and operated in the Indo-Pacific region under several zone and private cable maintenance agreements such as the South East Asia and Indian Ocean Cable Maintenance Agreement, the Yokohama Zone Agreement, the Asia Pacific Marine Maintenance Service Agreement, and the South Pacific Maintenance Agreement.

However, the majority of the 20 vessels are over 20 years old, with the most recent cable ship, KDDI Cable Infinity, which was built in 2019. Notably, it is also the only vessel constructed after 2010. At least five major submarine cable systems are slated for launch in the Indo-Pacific in 2024 and 2025, yet the number of cable ships available is not keeping pace with the rate of submarine cable construction.

Cybersecurity risks

Submarine cables are prone to cyberattacks or espionage by either state or non-state actors as part of grey-zone tactics. In recent years, competition between the US and China to lay submarine cables has intensified. Having control of the vast amount of data flowing through the submarine cables allows the great powers to exert greater influence, particularly in the Indo-Pacific region, and concerns about mass surveillance by foreign states through tapping into fibre-optic cables have grown. Amidst the backdrop of escalating competition for strategically valuable data flowing through these undersea cables, the data and privacy of citizens from smaller states are left vulnerable to exploitation due to insufficient legal protection from their national governments. This vulnerability arises as the legislation of major powers primarily focuses on protecting their own citizens when conducting surveillance activities, as highlighted by Elina Noor from the Carnegie Endowment for International Peace.

Furthermore, the cybersecurity of the shore-based cable landing stations and the companies operating the submarine cables has often been overlooked, despite the fact that it is critically important in terms of strengthening the resilience of submarine cable connectivity. Many submarine cable owners use internet-based remote network management systems to monitor and control submarine cables and landing sites, exposing the critical infrastructure and the sensitive data flowing through it to cyber threats.

Very often, the remote network management systems are provided by a third-party vendor and are poorly secured with common operating systems like Linux or Microsoft Windows, increasing the possibility of exploitation by malicious parties. Hackers can easily exploit this vulnerability to infiltrate a cable management system, obtain administrative privileges, and breach the presentation server. Attackers can then have high-level access to multiple cable management systems through the presentation server and delete the wavelengths of the cable systems to disrupt or reroute the data traffic. This could hamper communication between countries and affect supply chains. In April 2022, there was an attempted hack on the server of a company that operates a submarine cable that links Hawaii and the Pacific region by an unidentified international hacking group; but fortunately it was foiled by the US Homeland Security Investigations.

Non-state actors such as terrorist and criminal organisations are also capable of

hacking network management systems controlling the submarine cables remotely. A notable cyberattack by organised crime groups on critical maritime infrastructure involved the attempt to smuggle drugs from the port of Antwerp to the Netherlands by hacking into the computer systems of harbour companies and container terminals to monitor drug-containing containers. While no reported cases have involved undersea data cables thus far, companies operating submarine cables remain equally susceptible to cyber threats posed by organised crime groups.

Governance and legal gaps

There are gaps in international law concerning the governance of submarine cables. International law scholar Robert Beckman points out that States cannot legally board and penalise foreign nationals on a foreign-flagged vessel engaging in intentional theft or damage of submarine cables in waters beyond their territorial seas, under the 1982 United Nations Convention on the Law of the Sea (UNCLOS). Moreover, many States have not adopted Article 113 of UNCLOS in their national laws, which would require them to enact laws making the damage of submarine cables beneath the high seas or in the EEZs, whether wilfully or through culpable negligence, by a ship flying its flag or by a person subject to its jurisdiction, a punishable offence. One reason is that submarine cables have historically been dominated by private companies, and their significance is only recently being taken more seriously by national governments; therefore, legislation in many countries remains inadequate.

Other than the gaps in the international legal regime, the regulatory situation in some countries often involves many ministries and agencies with overlapping jurisdictions and weak interagency coordination, which complicates the licensing process for submarine cable installation and repair. If it is not clear which agency is in charge, there could be a significant security problem when submarine cables are at risk during emergencies such as natural disasters.

A submarine cable is owned by either a consortium consisting of private and state-controlled firms or a single company. The majority of undersea cables (65 percent) deployed globally are owned by a single entity; 33 percent have multiple owners from different countries while the situation relating to the remaining two percent is unclear. A multiple-ownership consortium can bring benefits such as sharing the financial costs and easing the management of landing points in another country. But that can create governance difficulties and potentially involve security and resilience

risks. There is concern regarding whether a country might seek to leverage its influence over both private and state-owned firms participating in submarine cable projects for espionage purposes, especially in the context of intensifying geopolitical competition in the Indo-Pacific.

Additionally, many countries mandate permits for the installation and repair of cables within their waters, even where there is no legal or practical justification for such requirements. In the South China Sea, overlapping maritime claims could delay the process as permits from multiple countries are required, and each step could be lengthy and cumbersome. One of the examples was the delay in the construction of the Southeast Asia-Japan Cable 2 due to the protracted permit issues in China. Any delays to the repair and installation could significantly increase the costs of construction; hence, Google and Meta's Apricot, Echo, and Bifrost are laying cables in the Java Sea rather than the South China Sea. However, this could increase the latency (the time it takes for data to travel from its source to its destination) of the submarine cable systems due to the longer distances involved.

Conclusions and recommendations

Internet data traffic is expected to grow in the Indo-Pacific as the digital economy grows. To strengthen the resilience of undersea infrastructure critical to the global supply chain, surveillance and monitoring of submarine cables should be enhanced. Drones and unmanned surface vehicles can be utilised to increase maritime domain awareness so that regional maritime law enforcement agencies can react faster to sabotage of submarine cables in their waters.

Besides, public-private partnerships are increasingly important to protect submarine cables. Submarine cable companies can lend their expertise to assist governments pass appropriate legislation and regulations, especially in relation to penalties for sabotage of submarine cables in their jurisdictional waters. Additionally, collaboration between governments and private companies facilitates timely responses to emerging challenges through information-sharing, ensuring the resilience of submarine cables.

As the maritime industry becomes more digitised, maritime cybersecurity will become a more prevalent maritime crime in the years to come. Submarine cable companies should invest in educating personnel about potential cyber threats and best practices to mitigate risks. This training should encompass various aspects,

including identifying phishing emails and recognising malware. By fostering a culture of cybersecurity awareness among staff, submarine cable companies can significantly reduce the likelihood of cyber incidents and protect critical maritime infrastructure and data from potential threats. The International Maritime Bureau, alongside the Information Fusion Centre, could report maritime cybersecurity crimes, including submarine cable damage. This enhances industry awareness and underscores the importance of maintaining cable resilience. Private cable companies could contribute by notifying these organisations of any damage.

Increasing the number of cable ships in the region is also necessary. National governments could play an important role here by providing subsidies to the submarine cable owners for cable repair ships. Shortening the repair time can significantly reduce the impact of cable faults on economic and social activities in affected countries due to the slowdown of internet connectivity. Some states such as the US and India have started their own government-led or government-subsidised cable ships program to ensure that ships are always available for cable installation and repair.

Finally, regional cooperation among Indo-Pacific states is critical to ensure more comprehensive governance of submarine cables and the resilience of the critical infrastructure. The ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables is important to streamline and simplify regulations and policies of ASEAN member states to expedite the permit application process for cable repairs. Additionally, table-top exercises that re-enact scenarios of intentional or unintentional damage to submarine cables and dialogues could be held during meetings and workshops of ASEAN-led mechanisms like the ASEAN Regional Forum, ASEAN Defence Ministers' Meeting Plus, and the Expanded ASEAN Maritime Forum. This could improve the cooperation between regional maritime law enforcement agencies to protect submarine cables.

Image: HAW-1 cables seen off the coast of Hanauma Bay Nature Preserve in June 2021. Credit: Colin Petty/WikiCommons.

This article is part of the 'Blue Security' project led by La Trobe Asia, University of Western Australia Defence and Security Institute, Griffith Asia Institute, UNSW Canberra and the Asia-Pacific Development, Diplomacy and Defence Dialogue (AP4D). Views expressed are solely of its author/s and not representative of the Maritime Exchange, the Australian Government, or any collaboration partner country government.