

THE CHANGING SUBMARINE CABLES LANDSCAPE

BRIEF / 19
Oct 2024

Expanding the EU's role in the Indo-Pacific

 The EUISS is an agency
of the European Union

by

Yuka Koshino

Associate Fellow, The International
Institute for Strategic Studies (IISS)

The rapid development of digital technologies has dramatically increased global internet bandwidth demand, with submarine cables today accounting for nearly 99% of intercontinental data traffic. These undersea cables are the backbone of global communications and the internet economy. Despite their critical importance, these cables remain inadequately protected, particularly in the Indo-Pacific region.

Globally, approximately 100–200 cases of damage to undersea cables are reported annually according to the International Cable Protection Committee (ICPC). Most of these incidents are accidental, typically caused by fishing or anchoring. Physical protection measures, such as burial in shallow waters and electronic monitoring of anomalies, along with legal regulations, all contribute to cable security. However, much of the responsibility for protecting these cables lies with operators, limiting private-public cooperation and creating vulnerabilities, whether during times of peace, 'grey zone' situations or at moments of crisis. Ensuring seamless protection that spans from peacetime to periods of potential volatility remains a significant challenge.

The Indo-Pacific, a region marked by complex geopolitics and rising tensions, faces unique challenges

Summary

- › Advances in digital technologies are driving a dramatic increase in the demand for global submarine cables. However, protection efforts in the Indo-Pacific remain inadequate amid growing risks from China.
- › These risks affect the EU's strategic and economic interests, as outlined in its 2021 Indo-Pacific Strategy, thus requiring greater EU engagement.
- › The EU and its Member States must assume a broader role in protecting submarine cables. Five areas for engagement include: enhancing public-private partnerships; collaborating with the Quad; developing legal and regulatory frameworks; investing in seabed monitoring technologies; and coordinating strategic infrastructure investments.

in ensuring the security of its submarine cables. For the European Union, whose interests in the region are framed by its 2021 Indo-Pacific Strategy, the vulnerabilities related to this critical infrastructure pose a strategic risk, calling for more proactive measures to manage them.

EUROPE'S EXPERIENCE: LESSONS FROM THE NORD STREAM INCIDENT

The sabotage of the Nord Stream pipelines in September 2022 amid Russia's war in Ukraine served as a wake-up call for Europe. It exposed the vulnerability of undersea infrastructure and underscored the urgent need to accelerate efforts to improve national and regional capabilities to collectively protect and repair critical subsea assets. In response, NATO increased its maritime patrols, surveillance and exercises aimed at safeguarding critical undersea infrastructure. It also established new mechanisms such as the Maritime Centre for the Security of Critical Undersea Infrastructure and the Critical Undersea Infrastructure Coordination Cells which facilitate information sharing among allies, partners and private sector stakeholders.

Several EU Member States have launched their own initiatives, including the Critical Seabed Infrastructure Protection project, aimed at enhancing the operational efficiency of underwater assets in the region. The EU-NATO Task Force on the resilience of critical infrastructure has also conducted a comprehensive assessment of Europe's undersea infrastructure, identifying key challenges and providing recommendations for improvement. However, similar efforts are largely absent in Asia, leaving the region vulnerable and exposed. This also directly affects the EU's interests in the region as articulated in the 2021 EU Strategy for Cooperation in the Indo-Pacific.

EMERGING CHALLENGES FROM CHINA

Several trends involving China are also raising concerns about the security of undersea cables in the Indo-Pacific and, by extension, the EU's interests in the region.

First, Chinese companies are rapidly expanding their presence in the submarine cable construction and repair industry. Since its establishment in 2008, China's HMN Tech (formerly Huawei Marine) has emerged as the fourth-largest submarine cable builder in the world, behind the US's SubCom, France's Alcatel Submarine Networks (ASN) and Japan's NEC. Backed by Chinese government subsidies under the Digital Silk Road (DSR) – the digital arm of the Belt and Road Initiative (BRI) – Chinese firms had reportedly built or repaired almost 100 of the world's 400 submarine cables by 2021⁽⁴⁾. Despite holding a global market share of less than 10%, China's strategic influence is growing.

The primary concern here is security. Under China's National Intelligence Law of 2017, Chinese companies are required to cooperate with intelligence efforts. This has led to fears that backdoors could easily be inserted during the construction and repair process, potentially enabling surveillance or sabotage. In 2018, the Japanese government reportedly discovered a Chinese wiretapping device on a cable near Okinawa⁽⁵⁾, confirming the security risks posed by increased Chinese involvement in the global cable network in the vicinity of geopolitical hotspots.

A second concern is growing Chinese interference in both ongoing and new cable construction projects in the South China Sea. In recent years, lengthy permit processing times and other bureaucratic roadblocks have resulted in construction delays for major projects, including the Southeast Asia-Japan 2 (SAJ2) cable connecting Japan to Singapore by way of Taiwan and Hong Kong. There is speculation that given Beijing's increasing control over cable construction projects in the South China Sea, these delays could be a form of retaliation against the exclusion of Chinese vendors from such infrastructure ventures⁽⁶⁾. Still others suggest that governance gaps and differing interpretations of international law—such as Article 7 of the United Nations Convention on the Law of the Sea (UNCLOS) — enable China to impose stricter permit requirements beyond internationally recognised territorial waters⁽⁷⁾.

Finally, there is the risk posed by Beijing's potential use of cables in a regional contingency, especially in Taiwan's remote islands in the East China Sea. Since 2020, Chinese sand-dredgers have been swarming around the Matsu Islands – part of Taiwan and located just 20 km away from mainland China – scooping sand from the seabed, often damaging undersea infrastructure, disrupting local economies and intimidating residents⁽⁸⁾. In February 2023, a Chinese fishing vessel and a cargo ship cut two cables, leaving the island with limited internet access for 50 days. While it remains unclear whether the damage

was deliberate, this incident further highlights how Taiwan's communication resiliency could be challenged in the face of future potential cable sabotage in a contingency scenario⁽⁶⁾.

REGIONAL RESPONSES AND GAPS

Regional coordination on submarine cable security in the Indo-Pacific has been fragmented, largely due to the lack of region-wide formal security institutions, akin to the EU or NATO. Additionally, different countries in the region have varying levels of threat perception, further complicating coordinated action.

The US, Japan and Australia have taken the lead in countering these threats, but their efforts to date have primarily focused on preventing the expansion of high-risk Chinese vendors within the region's submarine networks. The Trilateral Infrastructure Partnership, developed under the aegis of the Free and Open Indo-Pacific (FOIP) framework, and signed in 2018, serves as the main platform for promoting infrastructure development by trusted vendors. Under this framework, projects like Palau's 2020 second cable, connecting it to the Southeast Asia-United States (SEA-US) network, and the 2023 East Micronesia Cable, connecting Micronesia, Kiribati and Nauru, are examples of these efforts. Also in 2023, the Quad (comprising the US, Japan, Australia and India) launched its Quad Partnership for Cable Connectivity and Resilience, aimed at supporting cable construction as well as providing cybersecurity capacity building and technical assistance for the security of the region's cables. However this initiative has yet to yield tangible results.

Despite these efforts, regional responses to deter malicious attacks, as well as to protect and repair cables, remain sluggish and inadequate. To begin with, there is often a lack of clarity over which agencies are primarily responsible for submarine cable protection, creating further hurdles for effective regional cooperation⁽⁷⁾. In the case of Japan, despite being a key regional hub for trans-oceanic submarine networks hosting 20 cables, government policy papers did not address the need to protect submarine cables or their landing stations until 2023. Furthermore, the role of the Japanese Self-Defense Forces has yet to be clarified, despite the government's emphasis on civil-military cooperation for critical infrastructure protection under the 2022 National Security Strategy. These discrepancies create obstacles to conducting joint exercises and impede information-sharing between allies, hindering coordinated efforts to respond to threats.

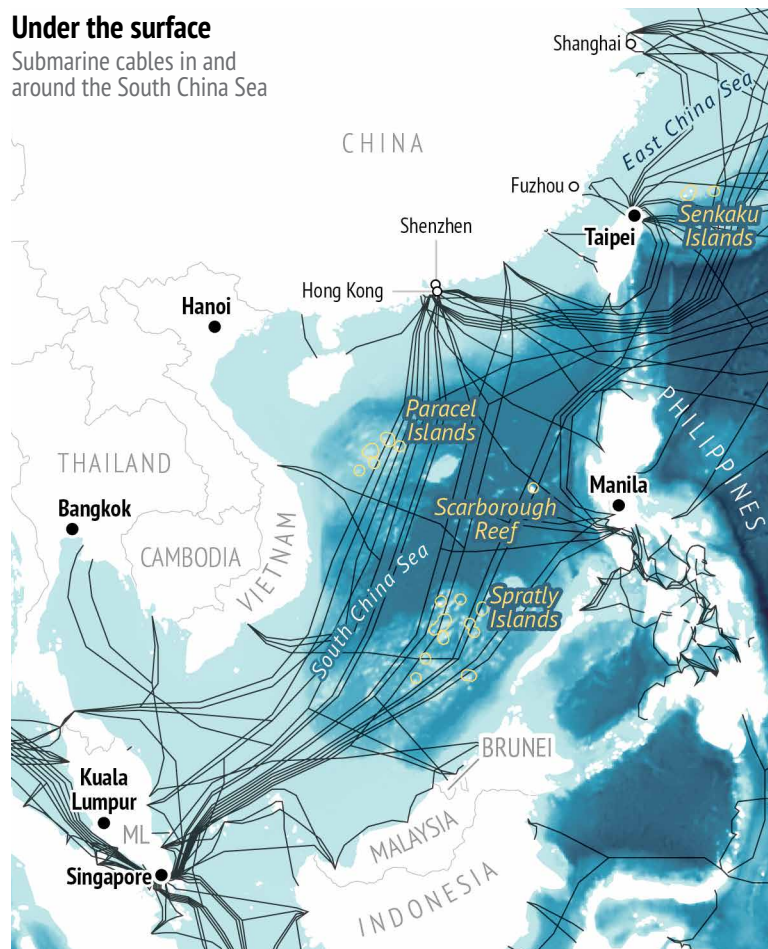
Gaps in seabed surveillance technologies, and limited cable-laying and repairing capacities, further jeopardise the security of regional submarine cables. The Guidelines for Strengthening Resilience and Repair of Submarine Cables, released by the Association of Southeast Asian Nations (ASEAN) in 2019, represent an important step towards streamlining permit processes for cable repairs. However, ASEAN has yet to launch a comprehensive initiative to tackle the broader challenges facing regional cables.

THE EU'S ROLE: OPPORTUNITIES FOR GREATER ENGAGEMENT

The EU's 2018 vision for connecting Europe and Asia, articulated through the Global Gateway initiative, and the EU-Japan Digital Partnership have laid some groundwork for addressing these challenges. However, the EU's role in ensuring submarine cable security in the Indo-Pacific remains limited.

Under the surface

Submarine cables in and around the South China Sea



Data: submarinecablemap.com, 2024;
European Commission, GISCO, 2024;
NOAA, ETOPO Global Relief, 2023

One notable EU initiative is the Far North Fiber project, which aims to connect Europe and Japan via the Arctic, bypassing critical chokepoints in the South China and Red Seas. By avoiding these vulnerable areas, the project aims to reduce communications delays by 20% and improve security⁽⁶⁾. This project represents a significant EU effort to add redundancy to key routes between Europe and Asia.

Yet, to play a more comprehensive role in the Indo-Pacific, the EU must go further. Europe's experience in responding to the Nord Stream sabotage and its broader efforts to protect critical infrastructure against Russian aggression could prove invaluable in helping Indo-Pacific countries build resilience against potential cable sabotage in high-risk areas like the Taiwan Strait or the South China Sea. Specific recommendations for furthering the EU's Indo-Pacific engagement include:

- > **Enhancing public-private partnerships:** The EU should actively engage with Indo-Pacific governments to foster public-private partnerships that enhance cable protection and resilience. Europe's experience in this area, particularly through NATO's mechanisms for safeguarding critical infrastructure, could serve as a blueprint for the Indo-Pacific. Encouraging joint exercises between governments, private operators and military forces would improve preparedness for potential cable disruptions.
- > **Collaborating with the Quad:** Engaging with the Quad could allow the EU to pool resources with key regional partners and take advantage of their on-the-ground capabilities. The EU's technical expertise in infrastructure resilience and cybersecurity could complement the Quad's efforts, allowing for a more coordinated response to security threats in the region.
- > **Developing legal and regulatory frameworks:** The EU can assist Indo-Pacific nations in developing stronger legal frameworks for cable protection, modelled after European initiatives. Clearer governance and enforcement mechanisms, especially in areas like the South China Sea where jurisdictional disputes can complicate security efforts, would be beneficial.
- > **Investing in seabed monitoring technologies:** Given the EU's advanced technological capabilities, Europe could lead efforts to improve seabed surveillance in the Indo-Pacific. Investments in cutting-edge monitoring systems would help detect and prevent cable damage more quickly, and sharing this technology with partners could strengthen regional resilience.

One notable EU initiative is the Far North Fiber project, which aims to connect Europe and Japan via the Arctic.

- > **Coordinating strategic infrastructure investments:** The EU should work closely with like-minded partners to coordinate submarine cable investments, ensuring that resources are directed to areas with the greatest need. Avoiding duplication and maximising impact will be key, particularly as regional actors look to diversify cable routes and build redundancy.

All in all, despite the critical importance of secure and reliable submarine networks in the Indo-Pacific region for its connectivity with Asia, the EU's role so far has been limited due to its focus on traditional land infrastructure development. However, its history, experiences and capabilities in addressing undersea critical infrastructure challenges means that the EU is uniquely positioned to support the region's secure, reliable and sustainable digital connectivity agenda as well as strengthen its engagement with the Indo-Pacific.

References

- (1) Bergin, A. and Bashfield, S., 'Digital age lies vulnerable to threats from underwater', Australian Strategic Policy Institute, 18 October 2021 (<https://www.aspi.org.au/opinion/digital-age-lies-vulnerable-threats-underwater>).
- (2) 'Okinawa kinkai no hikarifaiba- kaitei ke-buru ni Chūgokusei tōchō sōchi zai Okinawa Beigun muke jōhōshi ga shiteki' ['Chinese wiretapping devices in fiber-optic submarine cables near Okinawa pointed out by an information magazine for U.S. military forces in Okinawa'], *The New Lens*, 16 June 2023 (<https://japan.thenewslens.com/article/4070>).
- (3) Noor, E., 'Entangled: Southeast Asia and the Geopolitics of Undersea Cables', *Indo-Pacific Outlook*, Vol. 1, No. 5, 7 February 2024 (<https://manoa.hawaii.edu/indopacificaffairs/article/entangled-southeast-asia-and-the-geopolitics-of-undersea-cables/>).
- (4) *Ibid.*, p.32.
- (5) Bueger, C., Liebetrau, T. and Franken, J., 'Security threats to undersea communications cables and infrastructure – consequences for the EU', In-Depth Analysis requested by the Sede Sub-Committee, European Parliament, June 2022 ([https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA\(2022\)702557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf)).
- (6) Taiwan News, 'Matsu undersea cable repaired ending 50-day internet outage', 31 March 2023 (<https://www.taiwannews.com.tw/en/news/4852575>).
- (7) Congressional Research Service, 'Protection of Undersea Telecommunications Cables: Issue for Congress', August 2023 (<https://sgp.fas.org/crs/misc/R47648.pdf>), p.7.
- (8) Ministry of Economy, Trade and Industry of Japan, 'Japan-EU Joint Statement of the first meeting of the Japan-EU Digital Partnership Council' 3 July 2023 (<https://www.meti.go.jp/press/2023/07/20230703003/20230703003-4.pdf>).