MARITIME AFFAIRS: THE JOURNAL OF THE NATIONAL
MARITIME FOUNDATION OF INDIA
VOLUME 22 SPECIAL ISSUE 2026

SUBMARINE CABLE ATTACKS AS EMERGING MARITIME SECURITY THREATS AND ACTIONS FOR INTEGRATED MARITIME SECURITY IN THE INDO-PACIFIC: UTILISING RESPONSIBILITY TO PROTECT (R2P) AS A CATALYST FOR INTERNATIONAL COOPERATION

Dr Alan H Yang

ABSTRACT

This paper analyses deliberate attacks on submarine cables as an emerging hybrid maritime security threat in the Indo-Pacific, with Taiwan at the centre of escalating coercion. It argues that undersea cables are vital digital lifelines sustaining global data flows, energy security, economic stability, and the exercise of human and digital rights. Existing legal regimes, including UNCLOS, remain inadequate to address intentional sabotage and grey zone interference. The study reframes cable protection as a matter of shared coastal state responsibility and collective security. It advances the application of the Responsibility to Protect (R2P) to digital infrastructure governance, linking sovereignty to the duty to safeguard resilient connectivity. By proposing transparency mechanisms, regional coordination, and indigenous repair capacity, the paper situates submarine cable resilience within integrated Indo-Pacific maritime governance and a rules-based order.

INTRODUCTION: THE IMPACT OF THREATS TO SUBMARINE CABLES

In the current digital era, global communications rely not only on intangible technologies such as satellite signals but also — more crucially — on tangible transnational ICT infrastructure, particularly undersea cables. As the world advances rapidly into the age of artificial intelligence (AI), states across the globe are not only focusing on bolstering their domestic computing power and developing sovereign AI capabilities, but are also increasingly dependent on stable transnational communication systems. Among these, undersea infrastructure — especially undersea cables — constitutes a critical backbone, facilitating both global data transfer and, in some cases, energy transmission. These cables are

responsible for carrying over 95 per cent of the world's international data traffic. They not only serve the commercial interests of the enterprises that invest in and operate them, but also represent vital assets for national security and international stability.

Notably, these submarine cables have become targets of deliberate threats in recent years, particularly by authoritarian expansionist powers seeking to expand their geopolitical influence through coercion and grey zone area tactics. This paper contends that attacks on such cables constitute a form of hybrid warfare. When cables serve as energy transmission lines, their sabotage poses a direct threat to national security; when used for data transmission, such attacks jeopardise commercial and corporate interests. The former threatens fundamental human rights, while the latter undermines digital rights — both of which are essential to modern societies.

According to *TeleGeography,* as of early 2020, there were approximately 406 operational submarine cables globally, stretching over 1.48 million kilometres.[1] For example, the CeltixConnect cable linking Ireland and the UK spans just 131 kilometres, whereas the Asia-America Gateway extends up to 20,000 kilometres. The Indo-Pacific region is especially critical in this context, serving as a key conduit for undersea cables. Singapore, a major network hub in Southeast Asia, is connected to nearly 40 undersea cables and hosts several major data centres, forming a central pillar of the region's digital infrastructure.

Taiwan, situated at the heart of the Indo-Pacific, is also a critical node in the regional submarine cable network. Ten domestic submarine cables connect Taiwan with its offshore islands — Kinmen, Matsu, and Penghu — while 14 international cables make landfall at five key locations in Yilan, New Taipei, Taitung, and Pingtung. Facing the persistent authoritarian threat posed by China, these cables have increasingly become strategic targets for adversarial interference. On 03 January 2025, an undersea cable connected to the Trans-Pacific Express Cable System off the coast of Yehliu, Taiwan, was severed by the Hong Kong-flagged cargo vessel *SHUNXIN 39*, registered in Cameroon. Later that month, on 22 January, two additional cables connecting Taiwan and Matsu were damaged due to natural degradation, with the Taiwan-Matsu No 2 cable fully severed on 17 February and the Taiwan-Penghu No 3 cable reportedly cut by another cargo vessel on 25 February.

The uninterrupted operation of these cables and undersea infrastructures is essential to what is referred to as "cable resilience" or "infrastructure resilience."

This concept is deeply tied to governance legitimacy and the legal foundations necessary for maintaining operational stability. Since the interest in such cables extends beyond any one nation, involving multiple coastal and stakeholder states, international cooperation becomes not just beneficial but imperative.

This paper explores the governance frameworks surrounding undersea cables, arguing that they are not merely infrastructural assets but "vital digital lifelines" sustaining the daily functioning of modern human society. Accordingly, their governance intersects with both human rights and security governance. The paper advocates that states and populations closely tied to undersea cable infrastructure should be guaranteed digital rights and security, free from threats and coercion. It further calls on coastal states and relevant stakeholders to proactively foster closer and more robust international cooperation in this domain.

ATTACKS ON SUBMARINE CABLES ARE ATTACKS ON TAIWAN: LEGAL FRAMEWORKS AND STRATEGIC CHALLENGES

In recent years, incidents involving deliberate damage to submarine cables have become increasingly frequent — not only in Taiwan, but also in Europe. Notable examples include attacks in the Baltic Sea in 2024 and off the coast of Sweden in 2025. In the Indo-Pacific, China has emerged as a key actor in these threats, while in Europe, both Russia and China have been implicated. Growing bodies of evidence indicate a systematic pattern behind such activities.

China's targeted threats against undersea cables in waters near Taiwan appear to serve three strategic objectives. First, they aim to disrupt Taiwan's energy and communication security directly. Second, such actions are intended to erode Taiwan's international reputation as a responsible protector of commercial cable infrastructure, while simultaneously undermining public confidence in its government's ability to effectively manage recurring crises. Third, these attacks serve as tests of Taiwan's coastal response capabilities — probing response time and emergency protocols. These incidents also impose a significant burden on public institutions and regulatory agencies, leading to operational fatigue and a weakening of Taiwan's overall governance capacity.

While international legal instruments do provide a certain degree of protection for undersea cables, the current framework is far from sufficient. *The 1982 United*

Nations Convention on the Law of the Sea (UNCLOS) reaffirmed the principles established in the *1958 Geneva Convention*, particularly the freedom to lay and maintain undersea cables and the obligation to protect them. Coastal States have the right to regulate cable routes within their continental shelf by granting or denying approval for foreign cable installations.

Additional conventions touch upon relevant issues. *The Convention on the International Regulations for Preventing Collisions at Sea* (COLREGs) requires cable-laying vessels to signal their activities and mandates that powered and fishing vessels maintain a safe distance. *The London Convention on the Prevention of Marine Pollution* by Dumping of Wastes and Other Matter explicitly excludes submarine cables from its definition of marine pollutants. Likewise, the UNESCO Convention on the *Protection of the Underwater Cultural Heritage* specifically excludes submarine cables from the scope of underwater cultural property.

Nonetheless, these frameworks remain insufficient when it comes to addressing intentional attacks. There is no clear consensus under current international law as to what constitutes an illegal act against undersea cables, nor are there established mechanisms for accountability or enforcement. This legal ambiguity emboldens malicious actors, allowing them to operate with relative impunity.

Taiwan faces even greater constraints due to its exclusion from the United Nations and related international legal regimes. As a non-member, Taiwan has limited access to international cooperation platforms and is often left out of multilateral agreements or emergency response frameworks. This isolation significantly hinders Taiwan's ability to coordinate with international partners to prevent or respond to threats against its critical undersea infrastructure. In this context, Taiwan's strategic vulnerability is not just technical or logistical, but deeply institutional and legal as well.

SAFEGUARDING SUBMARINE CABLES AS DIGITAL LIFELINES: COASTAL STATE RESPONSIBILITIES AND THE IMPERATIVE OF INTERNATIONAL COOPERATION

Submarine cable damage generally results from one of four causes: (1) natural disasters, such as earthquakes or tsunamis near continental shelves; (2) animal interference, particularly from large fish such as sharks; (3) natural wear and ageing; and (4) human activities. In recent years, Taiwan has experienced a

growing number of external disruptions to its cable systems — 12 incidents in 2023 alone. Beyond internationally connected cables, cables in the shallow coastal waters near Taiwan's offshore islands, such as Matsu, have been frequently damaged by Chinese dredging vessels or entangled by trawlers, often resulting in prolonged communication outages.

While accidental manmade interference can be managed, deliberate attacks or hybrid warfare tactics present a more serious and urgent threat — not only to cable infrastructure but to the very concept of cable resilience and digital lifeline security. These challenges go to the heart of Taiwan's national sovereignty and security.

This raises a critical question: how should the international community respond to increasingly frequent attacks on submarine cables? More pointedly, how can a non-UN member like Taiwan fulfil its responsibility to ensure the integrity of its domestic cable connections while upholding the principles of good governance and fairness as a coastal State, particularly in safeguarding economic livelihood and ensuring stable information flow?

To this end, this paper proposes applying the principle of the "*Responsibility to Protect*" (R2P) to submarine cable protection and governance. R2P, in essence, asserts that States have a duty to protect their populations from genocide, war crimes, ethnic cleansing, and crimes against humanity. If a state is unable or unwilling to fulfil this obligation, the international community must be prepared to take collective action under the UN Charter. In this sense, R2P reorients sovereignty as a responsibility, not just a right, and places the protection of human rights above absolute non-interference.

If the undersea cables are conceptualised not merely as undersea infrastructure, but as "digital lifelines" integral to human rights (e.g., the right to survival through stable access to energy) and digital rights (e.g., access to secure and stable communications), then invoking R2P to promote international cooperation on cable resilience becomes both compelling and justified.

From this perspective, Taiwan's approach to ensuring submarine cable resilience can be framed on two levels. Domestically, Taiwan must take full responsibility for securing the energy and communication cables that connect its main island to offshore territories within the Taiwan Strait — this is a sovereign obligation tied to national security. Internationally, however, attacks on commercial or

communication cables near Taiwan should be framed as threats to the global digital commons, with Taiwan advocating for international cooperation through the lens of digital lifeline protection and R2P.

Hence, this paper proposes six specific international cooperation measures aimed at strengthening submarine cable resilience:

(a) *Establish Protective Zones Through Domestic Legislation*. Coastal states should enact laws to create cable protection zones. These include designated restricted areas where unauthorised vessels may not enter without permission from cable owners and the coastal state. An extended "warning zone" around these areas should be monitored by maritime law enforcement, which can issue alerts or take active measures to intercept unauthorised vessels.

(b) *Promote a Cable Security Transparency Initiative*. Establish a mechanism for regularly reporting attacks on domestic and international submarine cables in nearby waters. Reports should include detailed data (e.g., time, scale, damage type, frequency, vessel identification), and this information should be shared in real time with other coastal states and cable operators.

(c) *Report Incidents to International Bodies*. All attacks should be reported to *the International Telecommunication Union* (ITU) and *the International Cable Protection Committee* (ICPC), and connected with a proposed International Advisory Body for Submarine Cable Resilience to raise global awareness and correct public perception.

(d) *Host International Press Conferences and Public Condemnations on a regular basis*. Materialise the undersea cable transparency initiatives by regularly publicising attacks and convene international press briefings involving stakeholders to jointly denounce aggressors and demonstrate unified resistance;

(e) *Convene Regional Forums and Summits*. Organise regional undersea cable resilience forums, inviting neighbouring coastal states to collaborate and share response strategies. An undersea Cable Resilience Summit or regional dialogue platforms could foster joint planning, capacity building, and multilateral contingency protocols.

(f) *Develop Regional Cable Maintenance and Repair Supply Chains*. Currently, maintenance often requires applying through the ICPC

for foreign cable repair ships — a process that is time-consuming and expensive. Coastal states should invest in their own cable repair and deployment infrastructure, enabling faster response and reducing dependence. Building a regional supply chain for cable maintenance would also encourage inter-state collaboration in defending the digital lifeline.

CONCLUSION: EXPANDING MARITIME CORRIDORS AND BUILDING SUBMARINE CABLE RESILIENCE

Taiwan, situated at the crossroads of the Indo-Pacific, is uniquely positioned within a maritime corridor that links multiple regional seas from north to south. This geographic reality calls for a broader conceptualisation of maritime corridors — not just as strategic sea lanes or naval passages, but as comprehensive governance zones encompassing critical infrastructure, including resilient submarine cables. In this context, submarine cable resilience must be regarded as an essential component of maritime governance and regional security and cannot be overlooked.

Today, more than 15 countries and international organisations (EU and ASEAN) have either adopted or are actively formulating Indo-Pacific strategies/approaches. Many of these States — such as those in Europe — are geographically distant, yet they remain deeply concerned about peace, stability, and security in the Indo-Pacific. These concerns are further amplified by shared vulnerabilities to undersea cable sabotage and authoritarian interference, linking their interests closely with those of Taiwan and other regional stakeholders.

Submarine cable resilience offers a compelling focus for engagement and cooperation between Indo-Pacific nations and European States — particularly those with defined Indo-Pacific policy agendas. Here, this paper argues that embedding undersea cable governance into the broader framework of maritime corridor management should become a concrete expression of existing Indo-Pacific strategies. Such an approach carries three key implications:

(a) *Operationalising R2P for Digital Lifelines and Digital Rights*. Integrating submarine cable protection into Indo-Pacific strategies gives tangible expression to the Responsibility to Protect (R2P) in the context of digital infrastructure. It affirms the value of safeguarding digital lifelines

and protecting digital human rights, while reinforcing a rules-based international order.

(b) *Deterring Authoritarian Threats through Cross-Regional Solidarity.* Cooperation on submarine cable resilience promotes mutual learning and strategic coordination among democracies, fostering transparency initiatives and joint protection mechanisms. This can lay the foundation for a Euro-Asian network dedicated to submarine cable monitoring, disclosure, and deterrence.

(c) *Strengthening Coastal State Responsibility through Pragmatic International Cooperation*. Undersea cable governance highlights the shared responsibilities and sovereign rights of coastal states. A practical, cooperative framework can provide an effective means of safeguarding this global public good—ensuring that the infrastructure underpinning the world's communications remains secure, resilient, and universally accessible.

In sum, the governance of submarine cables should no longer be treated as a peripheral technical issue but as a central element of Indo-Pacific strategy and maritime governance. Taiwan, through the lens of R2P and digital resilience, can not only safeguard its own security and sovereignty but also contribute meaningfully to the development of a cooperative, rules-based Indo-Pacific order.

ENDNOTES

1 https://newswire.telecomramblings.com/2021/09/telegeographys-interactive-submarine-cable-map-hits-487-cables-stretching-over-1-3-million-kilometers-globally/?utm_source=chatgpt.com

About the Author

Dr Alan H Yang is Executive Director of the Taiwan-Asia Exchange Foundation (TAEF), Taiwan and Deputy Director of the Institute of International Relations, National Chengchi University. He also serves as Professor of Southeast Asia Studies at the Graduate Institute of East Asian Studies, leading the Centre for Southeast Asian Studies at National Chengchi University, Taiwan. also leads the

Centre for Southeast Asian Studies, National Chengchi University, which has served as the Secretariat of the Consortium for Southeast Asian Studies in Asia since 2018. Dr Yang has been a SUSI Fellow at the University of Florida and a visiting scholar at Kyoto University. His research focuses on ASEAN regionalism, disaster governance, border politics, and Southeast Asian international relations.