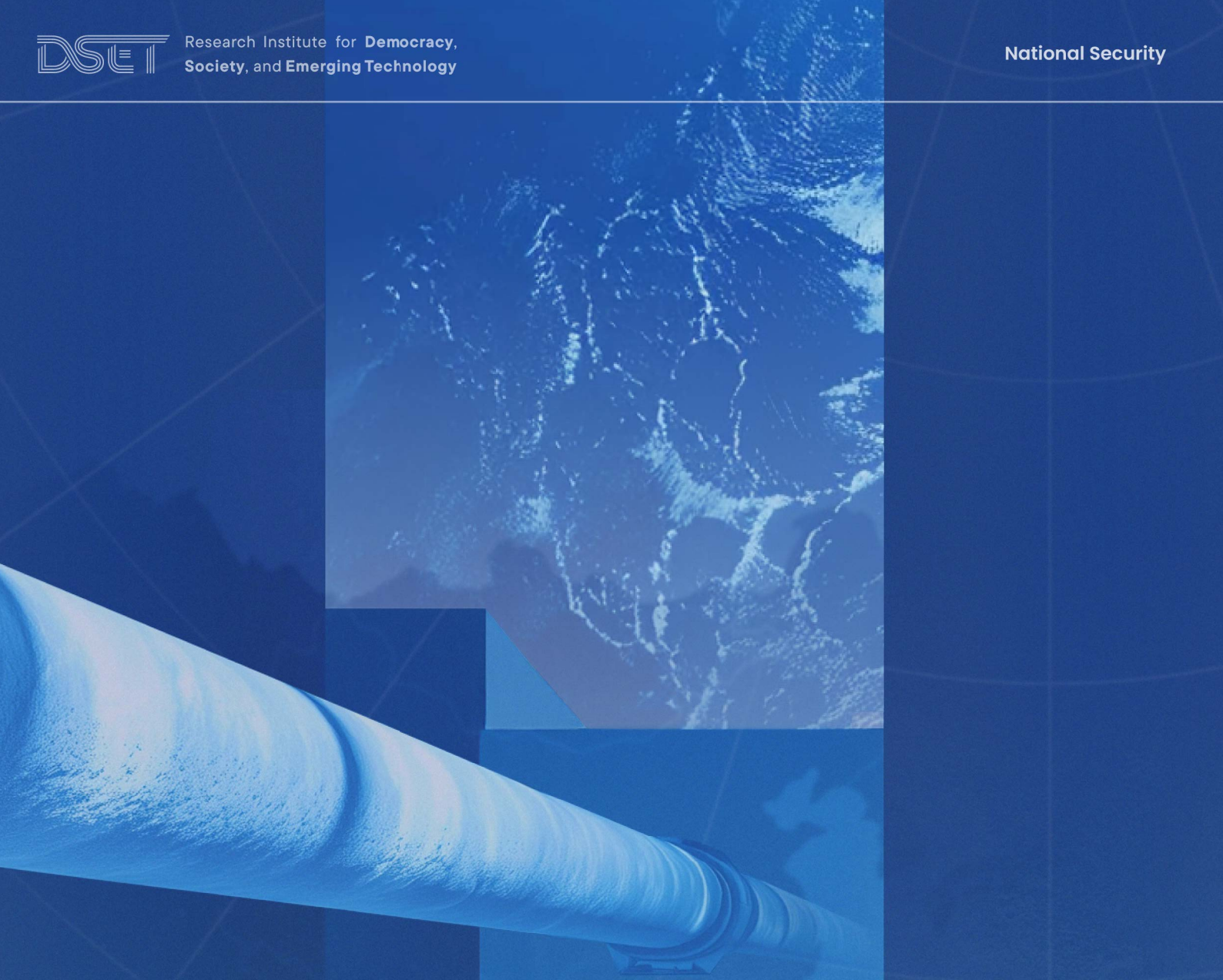


Undercurrent:

Limits and Prospects of Submarine Cable Security for Taiwan

Ta-Chen Chen

JUL 2025

Undercurrent:

Limits and Prospects of Submarine Cable Security for Taiwan

Research Institute for Democracy, Society, and Emerging Technology (DSET)

The Research Institute for Democracy, Society, and Emerging Technology (DSET) was established by the Taiwanese government in 2023 as a national think tank dedicated to providing strategic policy recommendations on geopolitics and emerging technologies. Our research covers key areas including semiconductors, artificial intelligence, energy security, and defense technologies—including drones, satellites, submarine cables, and robotics. DSET's work has been widely cited by international media, and we actively collaborate with leading think tanks worldwide to address these critical global challenges.

About National Security Research Program of DSET

The National Security Research Program at DSET conducts research and provides policy recommendations on dual-use technologies. Our focus includes building a China-free drone supply chain domestically and supporting democratic allies by supplying drones and drone components. We also prioritize enhancing communication resilience through trusted satellite communication service providers and strengthening the protection of submarine cables. Additionally, we assess the alignment of Taiwan's military strategy with that of our allies from strategic to operational levels.

Author

Ta-Chen Chen (Non-Resident Fellow)

Ta-Chen Chen is an S.J.D. candidate at the George Washington University Law School, where he focuses on the law of the sea and national security policies. His scholarship explores how international law defines and responds to gray zone activities. Before joining DSET, he was a staff member at the Taiwan National Security Council. He holds an LL.M. degree in National Security Law from the Georgetown University Law Center and an LL.M. degree from National Taiwan University College of Law.

Contents

Executive Summary

This report examines the persistent challenges in protecting submarine cables, particularly in the context of perceived gray zone activities. Despite numerous policy initiatives from both domestic and international experts, key limitations continue to limit effective prevention, enforcement, and attribution.

First, the inherent narrow time window for preventing submarine cable damage caused by the current notification and enforcement procedures may not be addressed by existing advanced technologies. Second, the international norms generally limit coastal states' jurisdiction within their territorial waters and provide few unilateral options to hold offending vessels accountable in international waters. Third, the intelligence currently available regarding gray zone activities overall fails to meet the threshold required for attribution, and thus further hinders response efforts and risk policy legitimacy.

In light of these constraints, this report proposes three policy tracks to address submarine cable damage on the premise of perceived gray zone activities: **punish**, **offset**, and **address**. These tracks reflect different policy decisions, and each comes with trade-offs, risks, and different levels of dependencies on certain factors such as intelligence, consensus among the international community, and key national interests such as freedom of navigation and sovereignty.

This report provides possible starting points for policymakers to develop their strategies based on their evaluations of different factors. Policymakers are urged to continuously evaluate and weigh these factors to form a responsive and actionable strategy.

I.
Introduction

Submarine cables are critical infrastructure for global communications, carrying over 95% of international data traffic.[1] As an island nation, the importance of submarine cables to Taiwan may be more significant than to the others. Taiwan relies almost entirely on submarine cables to maintain its internet connectivity and international communications.[2] In addition, Taiwan's outlying islands are generally connected by no more than two submarine cables. In recent years, a noticeable increase in cable breakages around Taiwan has raised concerns about its communication resilience and suspected gray zone activities in the maritime zones around Taiwan. A series of events can be dated back to February 2023, when the two submarine cables connecting Matsu, Taiwan's outlying island approximately 10 nautical miles off China's coast, were reportedly severed separately within a span of six days by PRC vessels.[3]

While the event was widely cited as a tactic of PRC's gray zone activities[4], no subsequent official report or comment was published by the relevant agency, such as the Taiwan Coast Guard Administration, the Ocean Affairs Council, the National Security Bureau, or the Mainland Affairs Council, potentially due to the then limited scope of Telecommunications Management Act.[5] Soon afterward, Telecommunications Management Act was amended to include submarine cable damages and an aggravated penalty provisions for national security in May 2023.[6] Two years later, in January 2025, a Cameroon-flagged vessel, "Shunxing 39," believed to be a PRC flag-of-convenience vessel, damaged Taiwan's northeastern submarine cable.[7] The Shunxing 39 was subsequently approached by the Coast Guard within Taiwan's territorial sea.[8] However, due to the sea condition, the Coast Guard was unable to board the Shunxing 39, and thus unable to attain the evidence needed to detain the vessel.[9] The Coast Guard subsequently requested Shunxing 39 to enter the Keelung port for investigation.[10] However, due to unspecified failure in coordination between the Coast Guard and the Maritime Port Bureau, Shuxing 39 ultimately did not enter the Keelung port and proceed to its next destination in Korea instead.[11]

Following the unsatisfying result, in January 2025, Taiwan's Legislative Yuan Foreign Affairs and National Defense Committee invited relevant authorities to report on the case of Shunxing 39. At the Legislative Yuan hearing, Taiwan National Security Bureau Director-General Ming-Yen Tsai stated that Taiwan's submarine cables have suffered more frequent damage in recent years.[12] Based on intelligence gathered by the National Security Bureau, most damage cases appear to result from vessels of Chinese origin.[13] Director-General Tsai also stated that the National Security Bureau would continue compiling intelligence based on the

observed trends.[14] Taiwan Mainland Affairs Council, the ministry-level agency responsible for overall Taiwan-PRC interaction, Deputy Minister You-Zhong Shen noted that although the incident requires further investigation, the Mainland Affairs Council preliminarily assessed that it was likely a case of PRC “sabotage”.[15]

For this Legislative Yuan hearing, several agencies, including the National Security Bureau, Coast Guard Administration, the Mainland Affairs Council, and the National Communications Commission, submitted written reports outlining future submarine cable protection policies. In addition to the reports of the aforementioned agencies submitted to the Legislative Yuan, several governmental agencies also conduct their own research. In February 2025, the Legislative Yuan's Legislative Research Bureau, the legal research department for the Legislative Yuan, issued a policy report recommending that a specialized regulation is needed for submarine cable protection to ensure effective enforcement.[16] The Ministry of Digital Affairs also proposed its multi-year research projects dedicated to submarine cables. According to the Ministry of Digital Affairs’ proposed "Submarine Cable and Network Development Policy and Security Plan" (September 2022), the Ministry of Digital Affairs has begun its research on policy and regulation recommendations for submarine cable protection since 2021.[17] Ministry of Digital Affairs’ proposed research primarily focuses on submarine cable legislation, submarine cable redundancy and backup mechanisms, and industry development strategies.[18]

Internationally, experts and academics have stressed the importance of submarine cable protection and proposed various policy recommendations. Considering Taiwan's unique geopolitical position, how to ensure Taiwan’s protection of submarine cables has become a touchstone of the future of the regional dynamic. In this context, the key question remains: With extensive discussions and policy initiatives to date, is Taiwan adequately prepared to protect its submarine cables? Especially under the generally perceived gray zone activities scenarios, what should Taiwan expect going forward?

Table 1.

Timeline of Submarine Cable Incidents and Taiwan's Security Response

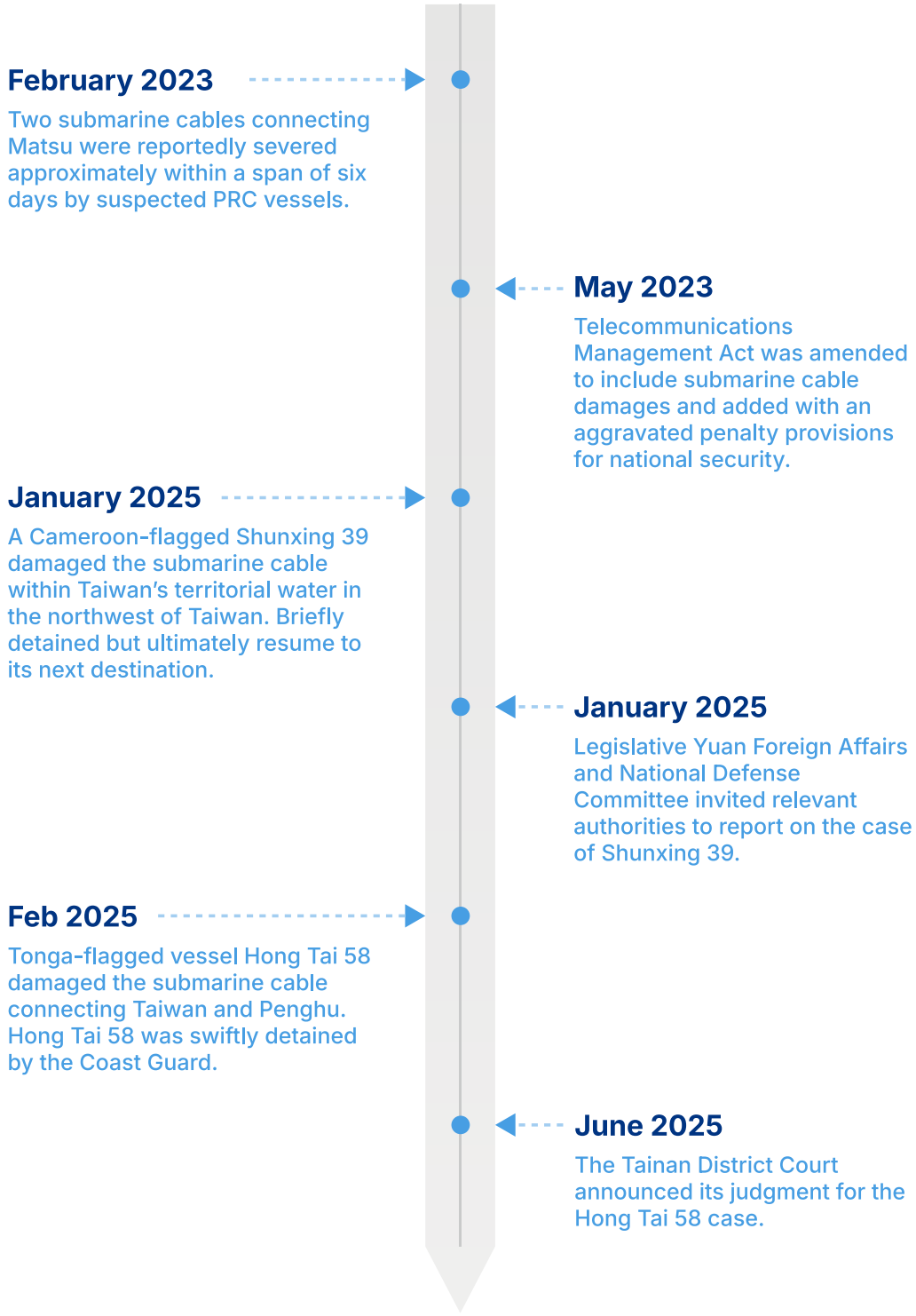
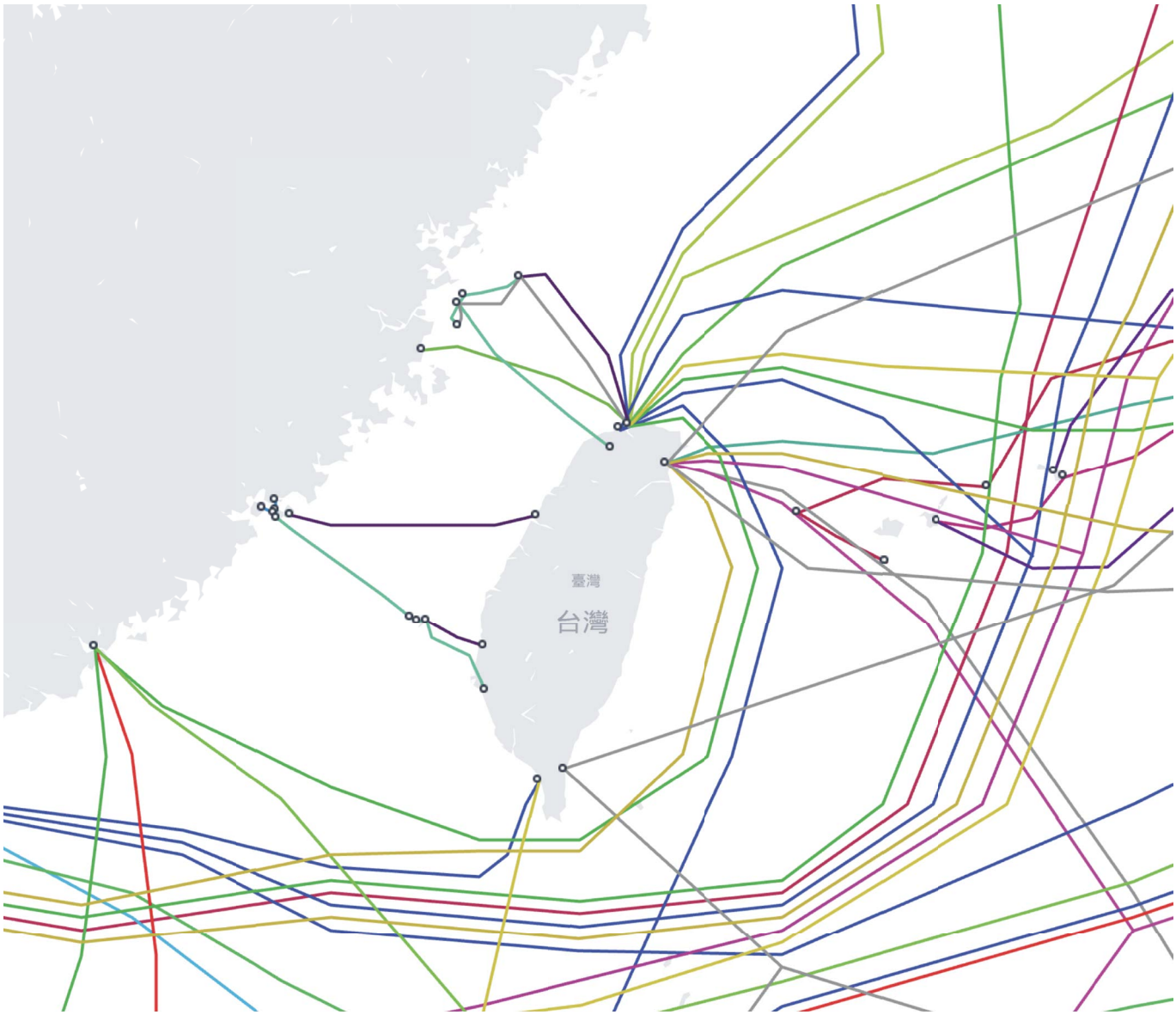


Figure 1.

Submarine Cable Map of Taiwan

Source:

Submarine Cable Map. https://www.submarinecablemap.com



II.
Contemporary Policy Initiatives on Submarine Cable Protection

Taiwan has experienced multiple cases of submarine cable damage. Given the geopolitical implications, relevant governmental agencies are handling the issue with heightened focus. Internationally, the suspected gray zone activities of PRC and Russia have drawn attention, especially following the recent submarine cable damage in the Baltic Sea. To briefly summarize, contemporary mainstream domestic and international policy initiatives for submarine cable protection include:

A. Initiatives Proposed by the International Community and Experts

1. Enhancing Maritime Surveillance with Emerging Technologies

Experts suggest that coastal states should deploy satellite imagery, drones, unmanned vessels, and underwater vehicles to monitor maritime zones, especially against "gray zone" or "shadow fleet" vessels that manipulate or disable AIS (Automatic Identification System).[19] For instance, NATO launched the Baltic Sentry mission in January 2025, which aims to deploy more aircraft and vessels as well as a small drone fleet to monitor vital underwater infrastructure.[20] In addition, the Joint Expeditionary Force, led by the UK and comprising 10 European nations, launched the Nordic Warden mission, which claims to incorporate AI and AIS data to detect possible sabotage in advance.[21]

2. Strengthening Norms and Enforcement

Many experts also advocate that coastal states can expand their legislation to international waters or enhance their enforcement methods to effectively curb submarine cable damage. As early as 2005, Australia amended its Telecommunications Act 1997, announcing the establishment of protection zones around submarine cables in its surrounding waters and stipulating penalties for damage to cables within these zones.[22] These protection zones extend beyond Australia's territorial waters.[23] Several domestic and international experts regard

Australia's legislation as a benchmark for submarine cable protection.[24]

In addition, according to Estonia's Public Broadcasting, the Estonian Riigikogu passed an amendment in 2025 allowing the Estonian Navy to use force, if necessary, to sink civilian vessels that pose a threat to Estonia's critical maritime infrastructure within its Exclusive Economic Zone (EEZ).[25] Simultaneously, the Estonian Ministry of Justice is also drafting a bill to increase penalties for damaging submarine cables and to expand the application to include its EEZ.[26] A similar argument has been presented by Taiwanese scholars. For example, Professor Yu-Hsiung Lin proposed that Taiwan should revise the Telecommunications Management Act to explicitly extend its application beyond Taiwan's territorial sea regarding submarine cable damage.[27]

3. Improving Industry Resilience

Many experts agree that the redundancy rate and maintenance capacity of submarine cables are also critical components of submarine cable protection policies. Overall, experts generally recommend incentivizing the development of related industries to ensure the accelerated deployment of submarine cables. In addition, it is often suggested that governments should develop dedicated repair fleets to ensure sufficient maintenance and repair capacity.[28] Moreover, as the current submarine cable industry is concentrated among a small number of companies, experts also recommend promoting more favorable industrial policies to attract investment and foster cooperation in order to increase the industry's capacity for submarine cable construction.[29]

4. International Cooperation

International cooperation is also a key component of contemporary policy initiatives for submarine cables. Specific recommendations include establishing joint maritime patrols to prevent submarine cable damage and enhancing international intelligence sharing to ensure that vessels involved in damaging submarine cables cannot easily evade surveillance, thereby facilitating investigations into such incidents. A recent example of this would be NATO's Baltic Sentry mission.

5. Promoting International Legal Regulation Through Multilateral Cooperation

Experts suggest that nations can promote new international norms first by promoting joint resolutions on submarine cable protection within major international organizations such as the United Nations or the International Maritime Organization (IMO), within the scope of their respective mandates. Ultimately, nations can gradually build consensus and work toward the development of an international convention that would incorporate submarine cable protection into existing international legal frameworks.[30]

B. Current Policy of the Taiwanese Government

1. Early Warning Systems

Regarding submarine cable protection, relevant government agencies in Taiwan have worked together and implemented a range of early warning systems. These systems monitor vessels' AIS signals continuously and identify vessels with abnormal transit patterns in an attempt to prevent damage to submarine cables. For example, Taiwan's Maritime Port Bureau has launched the "Smart Navigation Safety Program," which monitors AIS signal and locations of blacklisted vessels to identify suspicious activities in a timely manner.[31]

Chunghwa Telecom, Taiwan's leading communication service provider, has also established a submarine cable warning and detection system, which automatically sends alerts to vessels of certain sizes and speeds when they enter Taiwan's submarine cable warning zones.[32] Alternatively, the Vessel Traffic Service (VTS) tower may broadcast via radio to request the vessel to leave the area.[33] In addition, the Coast Guard Administration, in coordination with the Maritime Port Bureau and the Ministry of National Defense, has compiled a list of suspicious vessels to keep track of potential threats.[34]

2. Regulation Amendments

In 2023, Taiwan amended Article 72 of the Telecommunications Management Act, which not only broadened the scope of regulation to include submarine cables as protected objects but also increased penalties for damage motivated by intent to harm national security.[35]

In addition, in April 2025, Ocean Affairs Council Minister Bi-ling Kuan explained before the Legislative Yuan that the maintenance of submarine cables involves multiple competent governmental authorities and thus cannot be fully addressed through the enactment of a single dedicated law.[36] As for a specific plan for regulation amendments, Minister Kuan stated that Taiwan should amend the Electricity Act to ensure that the protection of submarine power cables is consistent with that of submarine telecommunications cables[37];amend the Law of Ships to prescribe penalties for disabling AIS[38]; and amend the Telecommunications Management Act to add provisions to allow the authority to confiscate the vessel when necessary.[39]

3. Intelligence and International Collaboration

In 2025, National Security Bureau Director-General Tsai stated that the National Security Bureau will share relevant intelligence with like-minded countries, with the aim of understanding the emerging trends in potential submarine cable sabotage and the overall gray zone activities.[40] In addition, the National Security Bureau will place more focus on intelligence gathering on PRC-flagged vessels and PRC flag-of-convenience vessels operating in the waters around Taiwan.[41]

III.
Limitations

From the above discussion, it is evident that both the international community, experts, and the Taiwanese government place a high level of attention and share a strong consensus on the protection of submarine cables. Comprehensive assessments and detailed recommendations have been made regarding various aspects of submarine cable protection. In addition, there seems to be a consensus of a high degree among these stakeholders. However, this report stresses that the implementation and international legal frameworks still present certain significant limitations in submarine cable protection. In particular, when viewed through the lens of gray zone activities, significant vulnerabilities in submarine cable protection remain.

A. Emerging Technologies Have Yet to Replace the Existing Submarine Cable Damage Notification Process

Regarding submarine cable monitoring, most commentators have suggested the use of emerging technologies such as drones and satellites, combined with AI-based real-time analysis of vessel traffic and registries to enable early identification of suspicious vessels. This report acknowledges that drones and satellites are indeed valuable tools for enhancing Maritime Domain Awareness (MDA), and they are certainly worthy of full governmental support as part of Taiwan's broader maritime security efforts.

However, when it comes to preventing submarine cable damage, the current notification process still relies heavily, perhaps solely, on telecommunications service providers to detect a cable disconnection and then report it to the Ministry of Digital Affairs and the Coast Guard Administration. Only after such a notification do relevant authorities begin reviewing ship traffic data within the incident timeframe using their maritime surveillance systems, followed by enforcement actions led by the Coast Guard.[42] This process inevitably takes time, and factors such as the location of the suspect vessel and the proximity of Coast Guard assets can significantly affect enforcement feasibility. Moreover, telecommunications service providers may initially misidentify the exact location of the cable disruption.[43] A Similar finding can also be found in the recent interim report by the International Law Association, a leading international NGO that consists of leading experts in international law around the world, where the International Law Association also finds that preventing submarine cable damage

is inherently difficult without very specific information beforehand.[44]

Regarding the emerging technologies that are considered the solution to preventing submarine cable damage, based on interviews conducted by DSET with subject matter experts, current satellite imagery technologies cannot identify whether a submarine cable is severed or disrupted, and drone-based surveillance over such vast maritime zones all day remains impractical at this stage. Even if a Taiwanese governmental vessel or aircraft were present at the scene during the moment of damage, it may still not be able to confirm damage to the submarine cable directly and effectively, and such confirmation could practically only come from the telecommunications service provider. As a result, the enforcement procedures, in most of the cases, can be triggered by the report of the telecommunication service provider. It may be possible to deploy sensors along cable routes to detect approaching damage factors, such as anchors or other devices, but no such deployable technology is available at this moment.

Certainly, Taiwan could still dispatch Coast Guard vessels preemptively based on the identified suspicious vessel movements, either for surveillance or deterrence. However, such early-warning measures must take into account personnel capacity, vessel availability, the distance to the identified vessels, and sea conditions.[45] In any case, confirmation of submarine cable damage, along with the initiation of law enforcement, still heavily hinges on telecommunications service providers.

In summary, while emerging technologies contribute positively to strengthening overall maritime domain awareness and addressing a range of maritime security challenges faced by Taiwan, when it comes to identifying and confirming damage to submarine cables, the process still relies on telecommunications service providers. Barring specific factors of individual cases, the emerging technologies hailed by many contemporary commentators have yet to overcome these operational obstacles.[46] Overall, unless there's specific information before the damage, prevention of submarine cable is inherently difficult.

B. Limited Coastal State Jurisdiction

At present, both nations and experts generally agree that coastal states have jurisdiction over vessels damaging submarine cables within their territorial seas. Recent cases include the Togo-flagged vessel Hong Tai 58 and the earlier Cameroon-flagged Shunxing 39, both of which were brought back to Taiwan by the Coast Guard without any significant dispute.

However, under international law, if the submarine cable damage occurs beyond the territorial sea, the coastal state does not, in principle, have jurisdiction over the offending vessel. According to the United Nations Convention on the Law of the Sea (UNCLOS), acts committed in a coastal state's Exclusive Economic Zone (EEZ) generally fall exclusively under the jurisdiction of the flag state.[47] One of the cases that reflects such a limit of jurisdiction is the Yi Peng 3, a PRC-flagged vessel responsible for damaging submarine cables in the Baltic Sea. The Yi Peng 3 was suspected of damaging the submarine cables in the Swedish EEZ.[48] While the PRC government and the ship owner of the Yi Peng 3 agreed to cooperate with the relevant European authority, the PRC authority only allows these European officials to observe an investigation being conducted by PRC officials and refused to allow the Swedish public prosecutor on board the vessel.[49] Yi Peng 3 ultimately refused to enter Swedish water[50] and proceed to its next destination.[51] So far, the PRC has yet to release the findings.

Another similar yet more promising case would be the Cook Islands-flagged vessel Eagle S, another vessel suspected of damaging other submarine cables in the Baltic Sea. According to major news outlets, the damage occurred in international waters in the Baltic Sea. While Finland was ultimately able to conduct an investigation by obtaining the ship's captain's voluntary cooperation to enter Finnish territorial waters, and cooperated with authorities, anonymous experts and a EU legal officer quoted by the Financial Times admit that the situation would be less clear had Eagle S refused to cooperate.[52] To sum up, this report notes that the jurisdiction of the coastal state in its EEZ is still limited, in both international law and practice.

This report observes that there are several Taiwanese scholars who have proposed that Taiwan should expand the application of its relevant rules regarding submarine cable beyond the territorial sea in order to deter the suspected gray zone fleet. This report also observes that Australia's Telecommunications Act 1997 is frequently cited by Taiwanese researchers as a desirable model.

This report notes that Australia indeed expanded the applicability of its Telecommunications Act 1997 to its EEZ. However, according to Australia's Telecommunications Act

1997, Schedule 3A, section 44A, the Telecommunications Act is clear that the offences do not apply to acts done by foreign nationals or foreign vessels unless it is connected with Australian's sovereign right exploration of the continental shelf, the exploitation of the resources of the continental shelf, or the operation of artificial islands, installations or structures that are under Australia's jurisdiction.[53] Australian domestic news reports also suggest that Australia has not yet successfully prosecuted any cases under this expanded jurisdiction.[54] It is also important to stress that, even if the coastal state expands its law to criminalize certain submarine cable damage in its EEZ, experts suggest that the coastal states can only enforce these laws when the suspect vessel subsequently enters its territory.[55]

As aforementioned, the flag state generally has the exclusive jurisdiction over the offending vessels in the EEZ, and the coastal state's unilateral law enforcement over the offending vessel in the EEZ would violate international law. Even setting the limit of enforcement aside, the International Law Association, one of the leading international NGO in international law studies, also suggests that the coastal state should limit its prescriptive criminal jurisdiction to the recognized sovereign rights in the international waters.[56] This report considers that the view of the International Law Association aligns with one of the fundamental principles of the law of the sea, which is to balance the freedom of navigation and the coastal state's jurisdiction in different maritime zones. As a result, such a balance should not be unilaterally altered until further consensus is formed among the international community.

Certain scholars proposed that such gray zone activities amount to an abuse of rights, and given the grave impact posed by submarine cable sabotage, coastal states may deploy proportionate countermeasures under the generally accepted principle of international law in response to gray zone activities actor's state responsibility for their internationally wrongful acts, even if such actions are not in accordance with the jurisdiction allocated under UNCLOS.[57] However, scholars also suggest that these measures should not involve the use of force that violates Article 2(4) of the UN Charter.[58] The aforementioned Estonia's latest legislation, which authorizes the navy to use lethal force, seems to be exceeding the existing international norms. Whether such legislation will be successfully enforced or receive wide international support remains to be seen.

In addition, even if a State is entitled to utilize countermeasures under the generally accepted principle of international law to take on the suspected gray zone activities, as will be discussed in the next section, such a State will still need to identify relevant facts and establish attribution to invoke such countermeasures.

Overall, while these proposals are still evolving, this report observes that most states continue to adhere to current international norms, showing no systematic trend toward extending coastal states' jurisdiction, both prescriptive and enforcement, to international waters.

In conclusion, when submarine cable damage is viewed through the lens of gray zone activities, current international legal frameworks offer little recourse for holding the responsible state accountable.[59] While it is certainly possible for coastal states to develop innovative countermeasures to address the existing limitation of international norms under the generally accepted principle of international law, these countermeasures are inevitably escalatory without detailed intelligence, and this report has not yet observed consensus among the international community.[60] Whether Taiwan will consider extending its domestic legislation and enforcement measures to its EEZ remains a matter for further deliberation by the relevant authorities.

C. Establishing the Attribution Behind Submarine Cable Damage Is Difficult Yet Necessary

As with any covert operation, the link between the actor and its sponsor is inherently difficult to establish. At present, most of the vessels involved in Taiwan's submarine cable incidents are civilian ships that fly the flags of convenience. Even if investigations successfully establish that the crew operating the vessel or the entity managing its operations is of PRC origin, and even if it can be successfully proven that the vessel deliberately damaged the submarine cable, under international law, such actions cannot be automatically attributed to the PRC government.[61] It must further be demonstrated that the act was carried out under the direction or command of the PRC government.

In any case, to effectively punish and deter gray zone activities, Taiwan's intelligence agencies must gather concrete, actionable intelligence. In addition, invoking the aforementioned countermeasures under international law would require certain factual evidence to establish right and attribution. Some commentators may argue that one of the core features of gray zone activities is the deliberate evasion of state responsibility, and therefore, responses to such actions need not be strictly constrained by existing international norms. However, both domestic judicial processes and the formation of new international norms require a high standard for attribution. In this context, gaining a clear understanding of the full picture of submarine cable damage and its link to gray zone activities remains a critical task.

In April 2025, the Tainan District Prosecutors' Office prosecuted the PRC captain of the Togo-flagged vessel Hong Tai 58 under Article 72, Paragraph 1 of the Telecommunications Management

Act for damaging the submarine cable. The Hong Tai 58 incident has been frequently cited by the media as a potential example of gray zone activity.[62] According to the press release issued by the Tainan District Prosecutors' Office and Taiwan Coast Guard Administration, the damage took place within the outer limit of Taiwan's territorial waters, and the vessel was successfully escorted to a Taiwanese port for investigation by the Coast Guard.[63] Given the limited jurisdiction of coastal state under international law concerning submarine cable damage, and considering the possibility that the vessel was acting as an instrument of the PRC's gray zone activities against Taiwan, the successfully capture of Hong Tai 58 seems to a prime case, and the prosecution of the captain of Hong Tai 58 would be highly symbolic and precedent-setting.

However, this report observes that the judgment for the Hong Tai 58 case was not as satisfying as many commentators anticipated. On June 12, 2025, the Taiwan Tainan District Court rendered its judgment, which considered that the captain "intentionally" damaged the submarine cable and sentenced the captain to three years' imprisonment.[64] Before this report unpacks this judgement, this report would like to remind readers from common law countries that Taiwan is a civil law country and Taiwan has different categorizations of intent under its criminal law. In the Hong Tai 58 case, while the court determined the captain of the Hong Tai 58 intentionally damaged the submarine cable, the specific intent in this case was mostly comparable to "recklessness" under the common law system.

In this case, the prosecutor contended that the vessel dropped the anchor in the publicized Prohibited Anchoring Area and the dredge anchor in a zigzag pattern around the submarine cable. The captain of Hong Tai 58 argued that the zigzag pattern was caused by the fact that Hong Tai 58 failed to hook the anchor to the seabed, and the vessel was therefore drifted by the waves to the position of the submarine cable. The captain acknowledged that he did not notice the position of the submarine cable in the nautical chart when he decided to drop the anchor. The captain admitted that he failed to pay due regard; however, he never intended to damage the submarine cable. The court ultimately ruled that the captain is aware that dropping the anchor in the publicized Prohibited Anchoring Area is very likely to result in dragging and damaging the submarine cable, and the captain proceeded to drop the anchor and allow the vessel to drift around the position of the submarine cable and ultimately result in damage of submarine cable.[65] Under the Taiwan Criminal Code, such conduct is considered an intentional commission of the offense, and the captain committed the crime under Article 72, Paragraph

1 of the Telecommunications Management Act.

Compared to the previous enthusiasm demonstrated by several commentators and the prosecutor, the findings of the court are not as satisfying as expected. This report wishes to highlight that the prosecution was based on Article 72, Paragraph 1 of the Telecommunications Management Act, rather than the more recently added Paragraph 2, which was specifically introduced in response to national security concerns. Such an arrangement signals that the prosecutor did not obtain qualified information that can demonstrate the Hong Tai 58's intent to endanger national security in the first place. While the prosecutor attempted to establish that the captain knowingly and intentionally damaged the submarine cable, the court ultimately considered that the vessel damaged the submarine cable recklessly.

While under the Taiwan Criminal Code, the court's finding still renders the actions of the captain an intentional offense, such a finding did not support the assumption that there is a hidden scheme behind the actions of the captain of the Hong Tai 58. This report suggests that the matter could be followed up by national security agencies to determine whether any foreign powers were involved in this case. On the other hand, this case could also be a revelation for relevant authorities to re-examine other potential sources of the damage to Taiwan's submarine cables. Either way, this report considers the findings of this case to be a starting point to shed light on the challenges Taiwan currently faces in dealing with submarine cable damages.

D. No Observable Consensus for a More Comprehensive International Cooperation or International Norm

Taiwan's relevant authorities have all proposed the possibility of international cooperation to counter submarine cable damage, such as through intelligence sharing or joint surveillance efforts. This report agrees that intelligence sharing is instrumental in clarifying the full picture of gray zone activities. However, as previously discussed, coastal states are primarily constrained by limited jurisdiction and high legal thresholds for attribution of state responsibility. In addition, there seems to be no intelligence so far that meets the aforementioned threshold of attribution since such intelligence would be very difficult to gather. Without changes to the current international legal framework or actionable intelligence, whether intelligence sharing or joint surveillance can contribute to the legal basis of countermeasures against submarine cable damage remains to be seen.

Many experts have also advocated for the establishment of multilateral cooperation. This report agrees that multilateral initiatives provide a fundamental and structural solution. Depending on the specific arrangements, a new multilateral framework could indeed help address existing gaps in the current international norm. However, such agreements would require not only broad consensus among states but also actionable intelligence and concrete proposals to move forward. At present, there is no publicly available evidence to suggest that such consensus has been substantially reached, nor are there clear indications of ongoing initiatives, proposed frameworks, or potential leading states driving such efforts.

Table 2.

Policy Options for Submarine Cable Security

Proposals	Limitations	Good for	Feasibility for submarine cable protection
Introducing drone fleet, satellites surveillance, AI-powered AIS signal early warning systems	• Can't help identify the submarine cable damage, or replace the service providers' role in reporting submarine cable damage. • Impossible to cover a vast area • Limited coastal state jurisdiction • Limited law enforcement personnel and assets to perform preemptive measures	• Overall Maritime Domain Awareness • Gathering necessary information to establish overall accountability afterward	✕
Unilaterally expand coastal state jurisdiction to international waters	• Against the law of the sea. • No sufficient state practice yet • Needs to be further coordination among nations	N/A	✕
Joint patrol or joint law enforcement	• In general, vessels are under the exclusive jurisdiction of flag states in international waters.	N/A	✕
Facilitating international norms	• Require a broad consensus and detailed arrangement to address the limitation of the existing norm while balancing the interests of international community • Lengthy process and coordination	• Addressing the limitation of the law of the sea directly • Legitimacy	○

IV.
Findings and the Ways Forward

Although domestic and international experts have proposed numerous policy recommendations for submarine cable protection, significant limitations remain in key aspects. First, the window for preventing submarine cable damage is inherently narrow due to the existing submarine cable damage notification process. Emerging technologies may help identify high-risk vessels in advance, but they still cannot significantly shorten the time between detecting cable damage and initiating enforcement actions. Secondly, limitations in international norms make it difficult to punish submarine cable damage in international waters. Thirdly, the intelligence gathered so far seems to be still below the threshold of attribution under both domestic and international norms, which results in the attribution of suspected gray zone activities remaining difficult. These limitations might explain why the nations, especially the executive branch, seem to be passive against rising “gray zone warfare” in the eyes of many experts and stakeholders. Despite the strong resolve to take action against the generally perceived gray zone activities, nations will inevitably find their options limited.

Taking these limitations into consideration, this report proposes three possible tracks for policymakers to move things forward on the premise of gray zone activities regarding submarine cable damages. This report notes that“prevention” may not be a practical track since it requires very specific intelligence to be gathered before the incident, and such information needs to be sufficient for both enforcement and establishing jurisdiction. This report also stresses that all three tracks will have to proceed under the caveat that important interests, such as freedom of navigation, national interests of both coastal states and flag states, and commercial interests, are carefully balanced. This report stresses that each track has its own risks and drawbacks, and the feasibility of each track ultimately relies on a series of negotiations between multiple states under multiple contexts. Due to the scope of this report, this report will not dive into each track to identify the specific risks and contention that may exist within each track. This report aims to provide systematic starting points for policymakers to evaluate their options based on the limitations and the prospects we have found so far. In general, under the context of gray zone activities, this report considers that there are three possible tracks for policymakers to pursue under the existing international norm: punish, offset, and address.

A. Punish

As noted earlier, leading law of the sea scholars suggest that it is possible to invoke countermeasures against gray zone activities and assert jurisdiction over these“gray zone fleet”or“shadow fleet”.[66] This report notes that this track may be collective actions, but the nature of these actions would be unilateral. Such a countermeasure aims to ensure that these gray zone activities will not go unpunished and that the state behind these gray zone activities will be deterred. However, to invoke such a countermeasure and maintain the legitimacy of such a countermeasure, the attribution to the gray zone activities actor should be duly established. To pursue this track, the intelligence community of like-minded nations inevitably needs to aim for more detailed intelligence and piece together a more comprehensive picture of gray zone activities to provide legitimacy for the policy and evidence needed to establish attribution.

B. Offset

As discussed in the “Punish” track, taking the gray zone activities head-on unilaterally could be risky and provocative since it creates an exception to the existing norm without setting a clear limit or meeting the threshold of attribution. An alternative to confront gray zone activities regarding the damage to submarine cables is to offset the gray-zone-actor-states’ political interest in other domains or venues that are within the control of like-minded countries and ultimately disincentivize the gray-zone-actor-states. The recent UN General Assembly Resolution A/Res/78/69 regarding the protection of submarine cables, support for enhanced Port State Control within the IMO structure, and other regional corporations falls under this track. While it is not clear to what extent these “softer” and indirect approaches will accumulate to the degree that the gray zone actor States will be deterred. This is the approach to avoid the risk of breaking the existing norm and to utilize the collective strength of like-minded nations. This report notes that this track seems to be a natural conclusion, and perhaps a more descriptive one to some readers, but this track still has its value when dealing with certain fundamental ambiguity of international norms that also benefit legitimate interests and the value of democratic nations, such as freedom of navigation and freedom of commerce.

C. Address

Another approach this report proposed is to counter the gray zone activities regarding submarine cable damage by addressing them at face value. To be more specific, to break down the elements of the perceived gray zone activities and address each element with an applicable norm. In the context of submarine cable damage, the starting point to address the submarine cable damage is to turn to the flag state of the vessels involved first and seek cooperation, regardless if it is a flag-of-convenience vessel or not. Such an approach is reflected in international fishery management mechanisms, where nations seek to regulate activities in international waters and where the flag state generally has the exclusive jurisdiction.

To briefly summarize, the international fishery management mechanism essentially establishes jurisdiction over the flag-of-convenience vessel by bringing all these flag States into coordination through negotiation and ultimately getting the consent from these flag States for specific matters to allow other members to assert jurisdiction over these flag-of-convenience vessels in the high seas.

Following the same vein, it is possible for the international community to work toward a multilateral coordination mechanism to include flag states that are involved in the submarine cable damage to gain jurisdiction over these suspected shadow fleets in international waters under a more detailed arrangement. In the context of recent submarine cable damage, such a coordination would have included flag states such as Togo, Cameroon, the Cook Islands, the PRC, and other flag states of common flag-of-convenience vessels. Such a coordination may be harder than setting up an international fishery management mechanism.

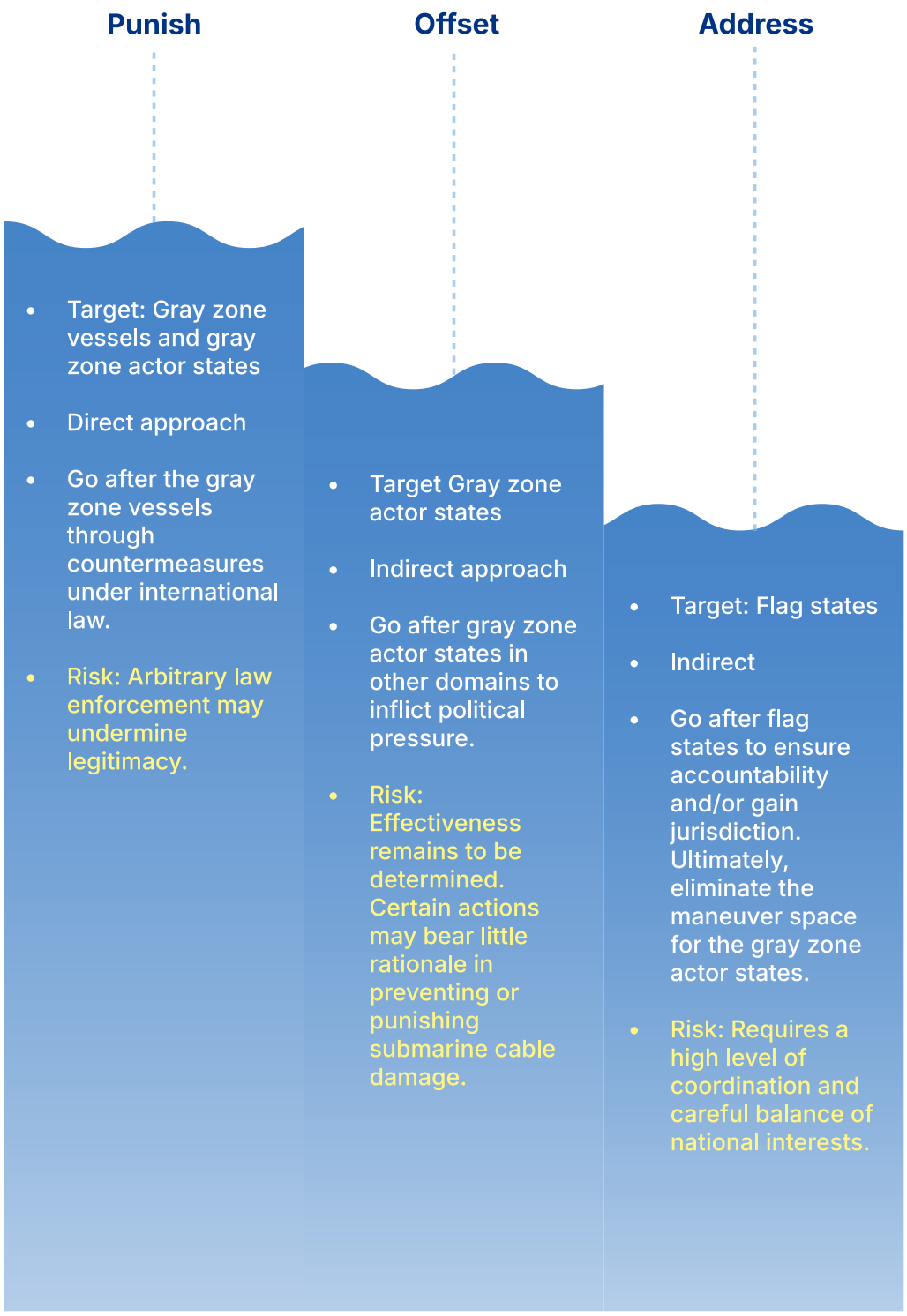
Other than the conflicts of several interests that also exist in the international fishery management mechanism, a multilateral coordination regarding the submarine cable damage in international waters would inevitably cast a shadow of antagonism, considering the shared conviction of gray zone activities by the PRC and Russia. One may consider countering gray zone actors through gaining the consent of these “lawless” flag states is not practical; however, this report would like to stress that the method illustrated by this report embodies the core formula to gain jurisdiction over flag-of-convenience vessels within the current structure of international norms. In addition, this report also notes that the success of such a coordination regarding submarine cable damage does not entirely hinge on the consent of the commonly suspected gray zone actor state, such as the PRC and Russia. The coordination will allow the international community to leverage flag states of the common flag-of-convenience vessels other than the PRC and Russia, who presumably have no interest in participating

in submarine cable damage, to cooperate and hence decrease the venue for gray zone activities.

Ultimately, the international community can shrink the room for gray zone actor states to maintain deniability without the risk of disrupting existing international norms. At first glance, this track seems to ignore the bigger picture of the gray zone activities against submarine cables. However, such a track presents a neutral and actionable solution to address the issue under the existing norms. Overall, this track would be a more systematic approach than the other tracks under the existing international norm.

Figure 2.

Three Options Against Gray Zone Threats



V.
Conclusion

This report proposes three possible tracks for policymakers on the premise of submarine cable damage caused by gray zone activities. It is up to the policymakers to evaluate the intelligence available, the degree of consensus among the international community, the national interest involved, and the existing international norm, and then determine the way to move forward. It is possible that a certain element becomes more significant and actionable as time develops, and ultimately makes a track that appears radical at first glance eventually seem natural and practical. It is crucial for policymakers to identify the elements and their development in order to develop a comprehensive solution. While this report maps the potential tracks, the feasibility of these tracks can only be determined by the knowledge of each element.

References

1. 數位發展部 [Ministry Of Digital Affairs], 海纜與網路之未來發展政策與安全防護計畫 (核定本) [Approved Plan for Future Development Policy and Security Protection of Submarine Cables and the Internet] 16 (2022), https://www.ey.gov.tw/File/312F12CDE9C9A230.

2. 國家通訊傳播委員會 [National Communications Commission], 審查「電信管理法第七十二條、第七十二條之一及第九十五條修正草案」報告 [Review Report on the Draft Amendments to Articles 72, 72-1, and 95 of the Telecommunications Management Act] 2-3 (2023), https://ppg.ly.gov.tw/ppg/SittingAttachment/download/2023042788/32209532129000050002.pdf.

3. 許靜之 [Ching-Chih Hsu], 台灣海底電纜專題報導 [*Special Report on Taiwan's Submarine Cables*], 公共電視台 [Public Television Service] (Aug. 5, 2023), https://news.pts.org.tw/projects/taiwan-submarine-cable/.

4. Wen Lii, *After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience*, The Diplomat (Apr. 25, 2023), https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/. *See also* Elisabeth Braw*, China Is Practicing How to Sever Taiwan's Internet*, Foreign Policy (Feb. 21, 2023), https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/. *See also* Hsu*, supra* note 3.

5. *See* National Communications Commission, *supra* note 2.

6. *See* 電信管理法 [Telecommunication Management Act] art. 72

7. *See* 中華民國大陸委員會 [Mainland Affairs Council of Republic of China (Taiwan)], 「針對海底電纜係國家對外重要通訊手段，為避免中共利用各種灰色地帶手段測試我國網路及電網韌性情事發生，如何建立有效備援系統以支援軍事作戰並支撐基礎建設防護韌性」報告 [Report on How to Establish an Effective Backup System to Support Military Operations and Enhance Infrastructure Resilience, in the Context of Submarine Cables Serves as a Crucial Means of International Communication and to Prevent the PRC from Testing Taiwan's Internet and Power Grid Resilience Through Gray Zone Tactics] 2 (2025), https://ppg.ly.gov.tw/ppg/SittingAttachment/download/2025011024/100451952602011000002.pdf.

8. 立法院公報 [Legislative Yuan Gazette] vol. 114, no. 22, at 303 (2025).

9. *Id.*

10. 海巡署 [Coast Guard Administration], 海委會召開跨部會協調會議 強化海底電纜監控及查處機制 [*Ocean Affairs Council Convenes Interagency Coordination Meeting to Strengthen Submarine Cable Monitoring and Enforcement Mechanisms*], 海洋委員會海巡署金門馬祖分署 [Kinmen-Matsu-Penghu Branch, Coast Guard Administration, Ocean Affairs Council] (Jan. 7, 2025) https://www.cga.gov.tw/GipOpen/wSite/ct?xItem=163127&ctNode=8195&mp=9996.

11. Legislative Yuan Gazette, *supra* note 8, at 290-92.

12. Legislative Yuan Gazette, *supra* note 8, at 288.

13. Legislative Yuan Gazette, *supra* note 8, at 288.

14. Legislative Yuan Gazette, *supra* note 8, at 288.

15. Legislative Yuan Gazette, *supra* note 8, at 292.

16. 安怡芸 [I-Yun An], 海底電纜毀損責任相關法制問題研析 [Legal Analysis of Accountability Related to Submarine Cable Damage] 3, Legislative Research Bureau of the Legislative Yuan (Mar. 30, 2023), https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=227877.

17. *See* Ministry of Digital Affairs, *supra* note 1, at 21. However, this report notes that the MODA has not yet published any of its findings other than its proposed research framework.

18. *See* Ministry of Digital Affairs, *supra* note 1, at 21.

19. Charles Mok & Kenny Huang, *Strengthening Taiwan's Critical Digital Lifeline: An Analysis of Taiwan's Undersea Cable Network Resilience* 20, Stanford Global Digital Policy Incubator Cyber Policy Center (Jul. 29, 2024),https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2024-08/undersea-cables-mok_huang-v4.pdf. *See also* Tara Davenport, *Intentional Damage to Submarine Cable Systems by States* 5–6, Hoover Institution (Oct. 26, 2023), https://www.hoover.org/sites/default/files/research/docs/Davenport_finalfile_WebReadyPDF.pdf.

20. *NATO launches 'Baltic Sentry' to increase critical infrastructure security*, NATO (Jan. 14, 2025), https://www.nato.int/cps/en/natohq/news_232122.htm.

21. GOV.UK, *Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet*, GOV.UK (Jan. 6, 2025), https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet.

22. Australian Communications and Media Authority, *Zone to protect Perth submarine cables*, https://www.acma.gov.au/zone-protect-perth-submarine-cables (last visited July 10, 2025).

23. Australian Communications and Media Authority, *Submarine telecommunications cables Perth protection zone map*, https://www.acma.gov.au/sites/default/files/2025-01/PPZ_2025.pdf (last visited July 10, 2025).

24. Jessie Jacob, *Let's Take a Close Look at How We Protect Our Undersea Cables*, Australian Strategic Policy Institute (Aug. 30, 2024), https://www.aspistrategist.org.au/lets-take-a-close-look-at-how-we-protect-our-undersea-cables/. *See also* 江雅綺 [Ya-Chi Chiang] & 陳瑞仁 [Jui-Jen Chen], 預防海底電纜危險 立法劃定保護區 [*Preventing Hazards to Submarine Cables Through Legislation for Protection Zones*], ETtoday (Jan. 20, 2025), https://forum.ettoday.net/news/2896054. *See also* Thea Coventry, *What Should States Do to Combat the Sabotage of Submarine Cables and Pipelines Beneath the High Seas/EEZs?*, EJIL: Talk! (Dec. 13, 2024), https://www.ejiltalk.org/what-should-states-do-to-combat-the-sabotage-of-submarine-cables-and-pipelines-beneath-the-high-seas-eezs/.

25. Vahur Lauri, *Riigikogu gives Defense Forces broader powers for use of force at sea*, Eesti Rahvusringhääling[Estonian Public Broadcasting] (Apr. 17, 2025), https://news.err.ee/1609666931/riigikogu-gives-defense-forces-broader-powers-for-use-of-force-at-sea.

26. *Id.*

27. Duschen Baer, 關鍵基礎設施的法制漏洞及填補：以海纜為例 [*Legal Gaps and Remedies in the Regulation of Critical Infrastructure: The Case of Submarine Cables*], Facebook (Jun. 6, 2025) ,https://www.facebook.com/share/p/1AaHSYbqrr/?mibextid=wwXIfr. *See also* 蕭白雪 [Pai-Hsueh Hsiao], 基礎建設頻遭破壞危國安？ 學者：立法疏漏多 [*Frequent Infrastructure Damage Threatens National Security? Scholars Point to Numerous Legislative Gaps*], Economic Daily News (Jun. 8, 2025), https://money.udn.com/money/story/7307/8792226.

28. Mok & Huang, *supra* note 19, at 8.

29. Mok & Huang, *supra* note 19, at 8, 20.

30. Coventry, *supra* note 24. *See also* Robert C. Beckman, *Protecting Submarine Cables from Intentional Damage—The Security Gap*, in Submarine Cables: The Handbook of Law and Policy 281, 290–94 (Douglas R. Burnett, Robert C. Beckman & Tara M. Davenport eds., 2014). *See also* Amy Paik & Jennifer Counter, *International Law Doesn't Adequately Protect Undersea Cables. That Must Change*, Atlantic Council (Jan. 25, 2024), https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/. *See also* Daniel Runde, Erin Murphy & Thomas Bryja, *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition* 9, CSIS (Aug. 2024), https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

31. 沈淑賢 [Shu-Hsien Shen], 智慧航安發展計畫 [*Development Plan for Smart Navigation Safety Program*], Maritime Port Bureau (Dec. 29, 2021), https://www.ttsb.gov.tw/media/5178/ 水路 _1_ 沈淑賢 _ 智慧航安發展計畫 .pdf.

32. Legislative Yuan Gazette, *supra* note 8, at 285–86. *See also* Legislative Yuan Gazette vol. 114, no. 38, at 324 (2025).

33. Legislative Yuan Gazette, *supra* note 8, at 285–86. *See also* Legislative Yuan Gazette vol. 114, no. 38, at 305 (2025).

34. Legislative Yuan Gazette, *supra* note 8, at 285–86.

35. 電信管理法 [Telecommunication Management Act] art. 72. *See also* National Communications Commission, *supra* note 2, at 2-3.

36. Legislative Yuan Gazette vol. 114, no. 38, at 330, 333-34 (2025).

37. *Id*. at 312.

38. *Id*. at 301, 333–334.

39. *Id*. at 311.

40. Legislative Yuan Gazette, *supra* note 8, at 278.

41. Legislative Yuan Gazette, *supra* note 8, at 288.

42. Legislative Yuan Gazette, *supra* note 8, at 281, 285, 303, 313.

43. Legislative Yuan Gazette, *supra* note 36, at 319.

44. International Law Association, *Submarine Cables and Pipelines Under International Law* 10, International Law Association (2024), https://www.ila-hq.org/en/documents/ilathi-1.

45. Legislative Yuan Gazette, *supra* note 36, at 324.

46. Davenport, *supra* note 19, at 6.

47. UNCLOS art. 92. *See also* Raul (Pete) Pedrozo, *Safeguarding Submarine Cables and Pipelines in Times of Peace and War*, 106 INT'L L. STUD. 45, 62-63 (2025). *See also* International Law Association, *supra* note 44, at 16. *See also* Coventry, *supra* note 24.

48. Pedrozo, *supra* note 47, at 47.

49. Louise Rasmussen, *Swedish police go board Yi Peng 3 vessel invitation China*, Reuters (Dec. 20, 2024), https://www.reuters.com/world/europe/swedish-police-go-board-yi-peng-3-vessel-invitation-china-2024-12-19/. *See also* Richard Milne, *Sweden criticises China for refusing full access to vessel suspected of Baltic Sea cable sabotage*,Financial Times (Dec. 22, 2024), https://www.ft.com/content/9094dcc4-b0f8-4191-b6f6-d1196a5f2822.

50. Richard Milne, Sam Learner, Lucy Rodgers, Irene de la Torre Arenas, Dan Clark, Ian Bott & Bob Haslett, *Inside Russia's Shadow War in the Baltics*, Financial Times (Mar. 9, 2025), https://ig.ft.com/baltic-sea/.

51. Reuters, *Chinese ship linked Baltic Sea cable breach resumes voyage* (Dec. 21, 2024), https://www.reuters.com/world/chinese-ship-linked-baltic-sea-cable-breach-resumes-voyage-2024-12-21/.

52. Milne et al., *supra* note 50.

53. International Law Association, *supra* note 44, at 29.

54. Karl Hoer, *What Lies Beneath: Undersea Cables and the Laws Protecting Them*, LSJ Online (Dec. 16, 2024), https://lsj.com.au/articles/what-lies-beneath-undersea-cables-and-the-laws-protecting-them/#:~:text=Schedule%203A%20of%20the%20Telecommunications,have%20served%20the%20country%20well.

55. Coventry, *supra* note 24. *See also* International Law Association, *supra* note 44, at 29.

56. International Law Association, *supra* note 44, at 30.

57. Pedrozo, *supra* note 47, at 63–64.

58. Pedrozo, *supra* note 47, at 64.

59. Pedrozo, *supra* note 47, at 62.

60. Pedrozo, *supra* note 47, at 62. *See also* Paik & Counter, *supra* note 30. *See also* Runde et al., *supra* note 30, at 9.

61. Davenport, *supra* note 19, at 7.

62. 鄭人豪 [Jen-Hao Cheng] & 許伯崧 [Po-Sung Hsu], 台灣海底電纜涉遭中資權宜輪損，破壞事件與地緣政治對抗加劇 [*Damage to Taiwan's Submarine Cables Linked to PRC-Affiliated Flag-of-Convenience Ships. Sabotage and Geopolitical Confrontation Escalate*], Initium Media (Mar. 10, 2025), https://theinitium.com/zh-hans/article/20250310-whatsnew-international-taiwan-chinese-cargo-sea-cables-foc. *See also* 海洋委員會 [Ocean Affairs Council], 海洋委員會攜手屏東地方檢察署 全國首創「海纜安全聯防地區應變平台」[*Ocean Affairs Council Partners with Pingtung District Prosecutors Office to Launch Nation's First "Regional Joint Response Platform for Submarine Cable Security"*], Ocean Affairs Council (Apr. 28, 2025), https://www.oac.gov.tw/ch/home.jsp?id=63&parentpath=&mcustomize=news_view.jsp&dataserno=202504280001 .

63. 臺灣臺南地方檢察署 [Taiwan Tainan District Prosecutors Office], 南檢偵辦大陸籍王姓船長駕駛「宏泰 58」貨輪在我國海域毀壞中華電信公司臺澎 3 號海纜線一案提起公訴新聞稿 [*Press Release on Public Prosecution Initiated by the Tainan District Prosecutors Office Against PRC National Captain Wang for Damaging Chunghwa Telecom's Taiwan-Penghu Subsea Cable No.3 in Taiwan's Waters with the Cargo Vessel "Hong Tai 58"*], Taiwan Tainan District Prosecutors Office (Apr. 11, 2025), https://www.tnc.moj.gov.tw/media/393934/1140411 南檢偵辦宏泰 58 貨輪毀壞我國電纜線案提起公訴新聞稿 .pdf?mediaDL=true.

64. 臺灣臺南地方法院 [Taiwan Tainan District Court], 臺灣臺南地方法院 114 年度訴字第 235 號違反電信管理法案件新聞稿 [*Press Release on the Judgement of Case Su Tzu 235 (2025) of the Taiwan Tainan District Court Regarding Violation of the Telecommunications Act*], 司法院 [Judicial Yuan] (Jun. 12, 2025), https://www.judicial.gov.tw/tw/cp-1888-1341586-34f43-1.html.

65. *Id.*

66. Pedrozo, *supra* note 47, at 64–65.

Research Institute for **Democracy**, **Society**, and **Emerging Technology**