Undersea Cybersecurity: Countering Gray Zone Operations and Strengthening the Digital Resilience of Subsea Cables for Taiwan[1]

Hon-min Yau
ROC National Defense University (Taiwan)

Abstract

Subsea cables are critical infrastructure for digital communications, economic stability, and national security. This undersea infrastructure, which was previously relegated to the periphery of public awareness, has emerged as a target of geopolitical conflict and hybrid threats, particularly through gray zone operations. This study highlights incidents involving subsea cable security in 2024 and 2025 throughout the Indo-Pacific and Europe, revealing a pattern of low-intensity, deniable operations aimed at disrupting transoceanic communications. The methods by which malicious actors leverage legal ambiguity and maritime vulnerabilities to damage subsea cables are analyzed through the case study of Taiwan. In this context, traditional deterrence by punishment approaches, such as legal penalties, are insufficient to stop state-sponsored aggression. Instead, a compound strategy is proposed for impairing hostile actors' access to key resources and preventing their ability to achieve strategic objectives. The case of Taiwan demonstrates a need for a timely and context-based approach to alternative methods of managing subsea cable attacks that are contingent upon the particular geopolitical context in which a country is located. A shift in strategic mindset is required: rather than deterrence by punishment alone, digital resilience depends on the ability to disrupt the execution and deny adversaries from achieving the objectives of gray zone operations.

Keywords: Cybersecurity, Cyberspace, Subsea cables, Submarine cables, Gray zone, Hybrid threats

1 This paper was written for Project No. NSTC 113-2410-H-606-004 of the National Science and Technology Council (NSTC), Taiwan.

Introduction

In the 21st century, information and communications technology plays a foundational role in global society. The seemingly borderless and ubiquitous flow of information requires global communications infrastructure, which is largely invisible to the public eye and discussed primarily within small-scale technical communities. Notably, most information traffic is carried by submarine systems rather than satellites. Subsea cables (also referred to as submarine cables) transport most internet data across oceans (Starosielski 2015, 1). As noted in a statement by the United Nations, "fiber optic submarine cables transmit most of the world's data and communications and, hence, are vitally important to the global economy and the national security of all States" (UN General Assembly 2010, 6). Hence, these cables, submerged at the bottom of the ocean, increasingly surface in conversations on global security.

On January 3, 2025, the Chinese-operated and Cameroon-registered cargo ship *Shunxin 39* allegedly caused anchor damage to the Trans-Pacific Express (TPE) submarine cable within Taiwanese territorial waters off the coast of Keelung in northern Taiwan (Davidson 2025). The TPE is a joint venture facilitating transnational communication between Taiwan, South Korea, Japan, the United States (US), and China. Because of the location of the cable damage, only international communications in Taiwan were affected. Negative geopolitical interactions between Taiwan and China have spiked since August 2022, when then-Speaker of the US House of Representatives Nancy Pelosi visited Taiwan (Wu and Baptista 2022). Notably, the subsea cables that were cut connect Taiwan proper to the offshore island of Matsu. Taiwan was forced to rely on backup satellite links and microwave technology to maintain communications with Matsu during the cable failures in early January and February 2025 (Focus Taiwan News 2025). In early 2023, submarine cables were also damaged because of illegal dredging carried out by Chinese ships in the Taiwan Strait, causing internet

disruptions for over 50 days and garnering substantial media attention (Taiwan News 2023).

Similar security challenges have emerged in Europe amid the Russian government's growing hostility toward European countries. In December 2024, the Estlink 2 power transmission cable between Finland and Estonia, as well as four nearby communication cables, were damaged by the Russian vessel *Eagle S*, which was subsequently detained by the Finnish Coast Guard at Porvoo Port for investigation (Reuters 2024). On January 20, 2025, the British Royal Navy made a rare public accusation against a Russian Yantar-class reconnaissance vessel, claiming that it entered UK waters with threatening intent vis-à-vis UK critical infrastructure. The Royal Navy immediately dispatched the frigate *HMS Somerset* and patrol ship *HMS Tyne* to track and monitor the suspicious activities of the Russian vessel (Hughes 2025). By January 22, 2025, in an unprecedented move, the UK Navy also publicly acknowledged deploying a submarine that surfaced and escorted the Russian ship to send a clear visual warning. In a later Parliamentary session, UK Defense Secretary John Healey accused Russia of mapping the UK's underwater critical infrastructure in preparation for future gray zone operations, stating: "We see you. We know what you are doing" (Al Jazeera 2025).

These events are not random incidents. Rather, they reflect growing geopolitical upheaval and threats to global cyber infrastructure in both the Indo-Pacific and the Baltic Sea in Europe. Although the Russo–Ukraine War has underscored the necessity of robust external communication infrastructure in contingencies, the smooth operation of transatlantic or transpacific communications frequently relies on the security of undersea cables. On March 14, 2025, the G7 countries recognized the importance of such infrastructure in a joint statement on maritime security and prosperity that highlighted "a growing concern that undersea communications cables, subsea interconnectors and other critical undersea infrastructure have been subject to critical damage through sabotage, poor seamanship or irresponsible behaviour…" (US

Department of State 2025).

However, the Baltic Sea is surrounded by NATO members, and access to it from the Atlantic is easily controlled by geographical entry points held by Sweden and Denmark. By contrast, Taiwan is surrounded by open water, and few in the region have well-known, active, operational security collaboration with Taiwan. The above distinction presents Taiwan as a challenging case to explore the possibility of policy responses. In addition, while some scholars' work has paid attention to the European context (Bueger and Liebetrau 2021; Ganz et al. 2024; Besch and Brown 2024b), very few have investigated the case in the Indo-Pacific (Cannon 2025). As such, in this article Taiwan is used as a case study to investigate potential policy responses to hybrid threats and methods for strengthening digital resilience in subsea cable communications. Specifically, this study focuses on possible countermeasures to confront the challenge of malicious state actors leveraging gray zone operations to damage subsea cable communications. The main argument of the paper is that, rather than deterrence alone, digital resilience could be enhanced with a better ability to disrupt the execution and deny adversaries from achieving the objectives of gray zone operations.

The remainder of this article is organized as follows. The first section presents an overview of the literature on the conceptual relationship between strategy, gray zones, and hybrid threats to establish an analytical framework. Next, the role of subsea communications within Taiwan's security context is examined in depth. The subsequent section outlines the limitations of international norms and regulations within this domain. In addition, Taiwan's current efforts to deter malicious actors are reviewed. Finally, the last two sections before the conclusion propose a detailed potential strategy incorporating compound elements and steps forward for future discussion and dialogue about this issue.

Conceptual Connections: Gray Zone, Hybrid Threats, and Strategy

Gray zones are established through the implementation of diversified capabilities to achieve a particular objective (Mazarr 2015), which commonly involves exerting high pressure without it constituting an overt declaration of war. In this sense, gray zone operations render peacetime more violent without creating the conditions of a hot conflict. In *The Art of War*, Sun Tzu argues that "though we have heard of stupid haste in war, cleverness has never been seen associated with long delays," and "there is no instance of a country having benefited from prolonged warfare" (Sun Tzu 2009, 7). As a form of long-term competition, gray zone operations contradict this supposition. Gray zone operations may manifest as a form of salami slicing in which gradual steps are taken to achieve specific goals, resulting in a "boiling the frog" effect rather than instigating an immediate reaction from opponents. Malicious state actors engaged in gray zone operations are familiar with international norms, which assist them in circumventing them. When such norms are lacking, gray zone operations can exploit this socio-political reality.

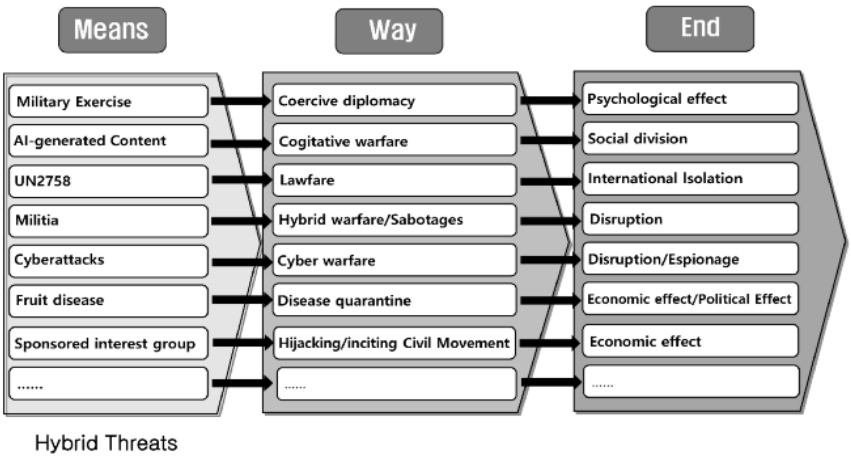
In the 21st century, states may exercise statecraft through gray zones. Gray zone strategies can be understood within the widely applied ends–ways–means framework: depending on attackers' ***ends***, they may adopt various ***ways*** of reaching their goal (e.g., military exercises, economic coercion, sabotage, or cognitive warfare) through traditional and nontraditional ***means*** (i.e., assets, such as military force, mercenaries, digital technology, media, and civilian ships) to circumvent accusations of waging a hot conflict. However, attackers may nonetheless harbor the ambition to engage in a hot conflict, for which gray zone operations may set the stage and shape the operational environment. In contrast to Clausewitz's framing of war as an extension of politics by other means during conflict, gray zone operations often emerge during peacetime, transforming politics into an extension of war by unconventional means.

State actors employ this strategy to increase violence during peacetime and exploit ambiguities in international law, which can hamper responses from other states. Hence, traditional and nontraditional hybrid ***means*** are a defining feature of gray zone operations. This operational concept is mentioned by the chief of Russia's general staff, General Valery Gerasimov, when he states that all available means, including military, technological, informational, diplomatic, economic, legal, and cultural tools, should be used to accomplish strategic goals, a position later controversially referred to as the "Gerasimov Doctrine" (Bartles, 2016).

A gray zone is also similar to the asymmetric warfare concept described by two officers of China's People's Liberation Army, Qiao Liang and Wang Xiangsui. These officers argued that information technology has fundamentally changed the nature and means of war, and consequently they proposed 24 forms of conventional or unconventional warfare tactics for conflict with other superpowers (Qiao and Wang 1999). Hybrid threats are the primary means in gray zone strategies. The conceptual relationship between gray zone operations and hybrid threats is illustrated in Figure 1.

Figure 1

FRAMEWORK OF GRAY ZONE OPERATIONS

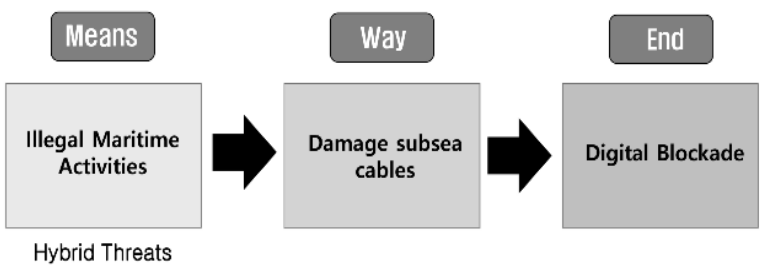


In short, gray zones normalize what may otherwise be considered exceptional behaviors. Hence, when gray zone operations may violate existing international norms, attackers attempt to establish plausible deniability to avoid being accused of violating global norms and exerting coercive pressure; meanwhile, in the absence of explicit international norms, attackers typically attempt to exploit this legal vacuum and conduct their activities more openly. Gray zone strategies can reduce political costs but do not always account for economic factors.

On the basis of this conceptual framework, the overall strategy of gray zone operations on subsea cables can be broken down into three key components: the end (strategic objective), ways (methods), and means (resources). Hence, as depicted in Figure 2, for the case of the Taiwan Strait, malicious state actors, such as China, may use ***means***, such as illegal maritime activities, to leverage subsea cable damage as a ***way*** to achieve the ***end*** of a digital blockade. As will be explained in the latter part of the article, subsea cables are particularly important for the external communications of an island state. Hence, opponent state actors can attack Taiwan's subsea cables to achieve the goal of increasing violence during peacetime, thus wearing down resilience without immediate escalation into a hot conflict.

Figure 2

GRAY ZONE STRATEGY FOR ATTACKING SUBSEA CABLES



Strategic Importance of Transoceanic Communication

International submarine cables present bountiful opportunities for malicious actors to leverage gray zone strategies to profoundly affect a target's external communication efficiency. Present-day flows of transoceanic information are typically fixed along fairly narrow cables, which are manufactured within the small, highly specialized cable industry to ensure the safe transit of media and communications through turbulent environments. The first cross-sea cable was installed between England and France in 1850, with this followed by the first transatlantic cable in 1857. As of 2025, over 300 submarine cables have been laid worldwide. They carry more than 98% of cross-border internet traffic globally (DHS 2024). The crucial role of subsea cables in digital infrastructure is highlighted in a *New York Times* report: "People think data is in the cloud, but it's not. It's in the ocean" (Satariano 2019). In the contemporary highly digitized world, any disruption to subsea cables necessitates emergency rerouting of traffic through an alternative path, potentially causing data congestion at critical bottlenecks, intensified communication delays, or service interruptions. Subsea cable disruption may even result in the outright failure of voice- and data-based communication, video streaming, financial transactions, and international trade (Palmieri et al. 2013). Consequently, the global topology of submarine cables has emerged as a matter of pressing geopolitical concern.

Unlike ships over high seas, which are governed by flag-state jurisdiction, submarine cables are typically jointly installed by consortia of private telecommunications companies from multiple countries (Bueger and Liebetrau 2021, 398). The US, as the world's largest data provider, has historically been the dominant destination of international submarine cable networks. However, under the increasing global fragmentation of tech regulations, data localization requirements, and the strategic calculations of private businesses,

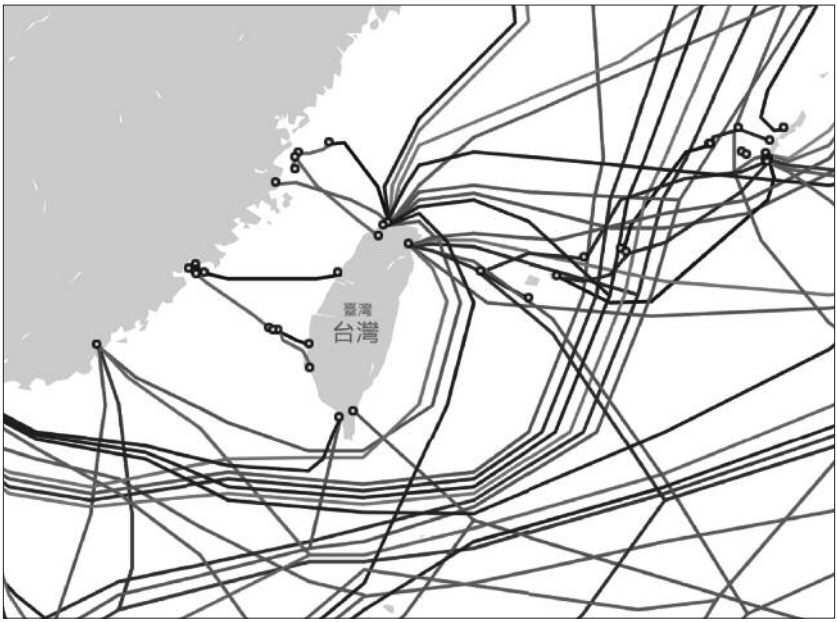
major internet content providers, such as Google and Meta, have begun investing in submarine cables connecting data centers outside the US to improve user experiences through closer access to distributed data (Carter et al. 2023, 4).

The aforementioned strategic characteristics of subsea cables have distinct implications for Taiwan's digital survival, given its location within the western Pacific Ocean. Because Taiwan has a relatively friendly regulatory environment for telecommunications companies, strong demand for transnational network traffic, and a strategic location within the cable topology of the western Pacific, the number of data centers operated by Google, Amazon, and Microsoft located in Taiwan has increased. Moreover, the Bashi Channel in southern Taiwan is the only exit route for subsea cables traveling through the South China Sea and has thus become a crucial transit point for international submarine cables. Taiwan's centrality within subsea cable networks is exemplified by the aftermath of the 2006 earthquake in Hengchun, southern Taiwan, which not only disrupted Taiwan's external connections to Southeast Asia but also affected global communications in Hong Kong and transcontinental data links in China because of damage caused by undersea landslides to subsea cables within the Bashi Channel (Saito 2019, 109).

As of 2025, Taiwan proper relies on 14 international submarine cables to communicate with the world and 10 domestic cables to communicate with offshore islands (TeleGeography 2025). Likewise, as indicated in Figure 3, much of the international network traffic across the Pacific is carried along submarine cables southeast of Taiwan. Numerous internationally operated subsea cables pass through waters adjacent to Taiwan, connecting Northeast Asia and points south and west that run through Taiwan. Hence, disruptions around Taiwan could affect Southeast Asia, South Korea, and Japan. An attack on the subsea cables around Taiwan is a global communication issue that goes beyond the Indo-Pacific region.

Figure 3

SUBSEA CABLES SURROUNDING TAIWAN



Source: https://www.submarinecablemap.com/country/taiwan

Limitations of International Norms Regarding Subsea Cable Protection

International law offers limited protections for subsea cables, attacks on which are typically discussed from the angles of *jus in bello* (the ways through which warfare is conducted) and *jus ad bellum* (the conditions under which states may resort to war) in relation to legal complications.

Regarding *jus in bello*, submarine cables are in practice legitimate targets for military conflict. A historical example of this phenomenon is the destruction of the German Empire's subsea cables by the British during World War I (Ryan 2024, 21). In a contemporary case, Russian operatives cut Georgia's external communication cables during its 2008

military intervention in the breakaway regions of South Ossetia and Abkhazia (Deibert, Rohozinski, and Crete-Nishihata 2012, 6). Although malicious state actors are aware of international norms, this is typically in order to ensure they can effectively circumvent these norms. That is, their use of gray zone operations often reflects an instrumental rather than normative view of international law. In the case of subsea cables, attacks on this infrastructure during wartime are somewhat uncontroversial; as such, gray zone attacks on subsea cables primarily require exploitation of the legal ambiguity of *jus ad bellum*.

Consequently, as regards the discussions in the context of *jus ad bellum*, the most commonly referenced international law is the United Nations Convention on the Law of the Sea (UNCLOS), Article 112 of which allows states to lay cables in international waters. Notably, submarine cables pass through territorial waters, contiguous zones, exclusive economic zones (EEZs), and the high seas. The legal implications of the territorial distribution of cables afford states complex judicial responsibilities in dealing with disruptions. For example, states have full authority to stop and investigate a ship, regardless of its nationality, in their territorial waters, but only flag states can exercise such authority once ships are over the high seas, as specified in UNCLOS Articles 113 to 115. Threats to subsea cables encompass natural causes, such as earthquakes or fish bites, and human actions, such as fishing activities or sabotage (Bafoutsou, Papaphilippou, and Dekker 2023). Within the context of the need of *jus ad bellum* in identifying the origin of the attacks, the public cannot immediately determine whether damage resulting from human activities is a careless accident or a malicious attack, an issue exacerbated by the stovepiping within the government agencies investigating such incidents, resulting in a challenge to identify the source of the actual cause in a timely manner. Although Article 100 of UNCLOS encourages all states to cooperate in addressing maritime criminal activities, states' actual conduct remains a topic of debate. The fragmentation of legal authority to identify attackers creates attribution difficulties related to *jus ad bellum* when subsea cables may be attacked

over territorial waters, contiguous zones, exclusive economic zones (EEZs), and the high seas.

Nevertheless, long before UNCLOS was drafted, several countries signed the 1884 *Convention for the Protection of Submarine Telegraph Cables*, which provides a limited foundation for states to enforce cable protection through military vessel authority (Besch and Brown 2024b). Article X of this convention allows officers of official ships to board suspected foreign ships and inspect their documentation to report to their flag states. States, like the US, view challenging the freedom of navigation and the right of innocent passage as a customary international norm within this particular legal context (Azaria and Davenport 2024, 16). This enforcement regime was first enacted in 1959, when a US destroyer, the USS *Roy O. Hale*, stopped a USSR trawler, *Novorossisk*, on the high seas on suspicion of damaging cables (Starosielski 2015, 152). A second incident likely took place in November 2024, when the Danish Navy detained the Chinese vessel *Yi Peng 3* on suspicion of damaging two Baltic Sea cables connecting Scandinavia and mainland Europe, the BCS East–West Interconnection and C-Lion1 (Besch and Brown 2024a). Although UNCLOS requires civilian vessels to be registered with a flag state, the economic incentive of low ship registration fees has caused widespread abuses of flags of convenience (Rajan 2024). Even landlocked countries such as Mongolia provide global vessel registration services. Consequently, if a submarine cable within Taiwan's territorial waters is disrupted by a ship operating under a flag of convenience, malicious state actors have the plausible deniability to evade direct responsibility because of a lack of concrete evidence.

Hence, current international norms regarding subsea cables problematically allow malicious state actors to either exploit the ambiguity of law enforcement boundaries or leverage plausible deniability, enabling low-intensity gray zone attacks on these cables to flourish without crossing the threshold into warfare. Attacks occurring over the high seas can bypass accusations of engagement in the seven types

of aggression defined in UN General Assembly Resolution 3314 of December 14, 1974. These forms of aggression include military occupation, bombing, naval blockades, military attacks on another state's forces or civilian vessels, security treaty violations, the use of a state's territory by a third party to facilitate invasion, and irregular warfare on other states by armed forces or mercenaries (UN General Assembly 1974). In short, even if a submarine cable attack results in a digital blockade against a specific country, current international regulations hinder effective measures to address such incidents.

Hybrid Threats and National Cybersecurity

The problematic strategic and legal environment outlined in the preceding sections positions subsea cables as a convenient target for coercive statecraft practices. At the height of the Cold War, submarine cables were often used for military communication and became frequent targets for military action. A well-known attack on submarine cables was *Operation Ivy Bells*, which spanned 1971 to 1981, when the US Navy successfully tapped Soviet military cables made of copper in the Sea of Okhotsk. Notably, technological advancement kickstarted by the globalization of communication in the 1990s has resulted in the development of fiber optic cables that can transfer enormous volumes of data and have more protected designs. Underwater tapping is technically challenging, and therefore, in 2023, the European Union reported that threats to submarine cables stem primarily from technical defects, poor design, natural disasters, or sabotage rather than underwater espionage (Bafoutsou, Papaphilippou, and Dekker 2023). Although supplies for subsea cables had historically often been provided by specialized companies within an industry dominated by Western firms, by 2024 China's Huawei Marine Networks (HMN Technologies) aggressively expanded into submarine cable projects in developing nations, challenging the dominance of companies such as Alcatel

(France), NEC (Japan), and SubCom (US) (Ganz et al. 2024). To safeguard submarine cable networks in response to this development, numerous Western nations have endeavored to achieve more robust supply chain security, system design, and legal compliance mechanisms (Guarascio, Nguyen, and Brock 2024).

On January 26, 2025, a submarine cable across the Baltic Sea connecting Sweden and Latvia was severed under unclear circumstances. The prime minister of Latvia, Evika Siliņa, stated that the incident was likely the result of a use of external force. Alongside authorities from Sweden and the North Atlantic Treaty Organization, Latvia immediately launched a joint investigation into suspicious vessels in the area (Sytas and Ahlander 2025). These Baltic countries demonstrated the need for international collaboration regarding subsea cable protection because of their close proximity and the fragmented authority governing the Baltic Sea. However, Taiwan's submarine cable infrastructure is distant from the territorial waters of other countries. In addition, the number of Taiwanese agencies and regulations involved in subsea cable protection complicates this task. For example, if a security incident occurs within Taiwan's territorial land and waters, Article 72 of the Taiwanese *Telecommunications Management Act* and Chapter 25 of the Taiwanese *Criminal Code* provide the authority for law enforcement to prosecute the perpetrators of attacks on critical communications infrastructure. Additionally, the Taiwanese *Civil Code* authorizes the owner of the damaged infrastructure to secure relevant compensation from malicious actors through legal action. Furthermore, if security incidents occur 12 or more nautical miles beyond Taiwan's territorial waters, Taiwan has domestic legislation, the *Law on the Exclusive Economic Zone and the Continental Shelf*, that specifies requirements for foreign maritime activities throughout the EEZ within 200 nautical miles of Taiwan. Nevertheless, for incidents on the high seas, only a ship's flag state has investigation authority under UNCLOS Articles 113 to 115. For a single-state actor, like Taiwan, the interconnectedness of subsea cables creates governance challenges in terms of coordination and legal

compliance.

In short, for Taiwan, the Ministry of Transportation regulates cable licensing, the Homeland Security Office of the Executive Yuan oversees infrastructure protection, the Ministry of Digital Affairs manages cybersecurity, the Ministry of the Interior enforces land-based telecommunications security, and the Ocean Affairs Council manages maritime security. Political scientist Graham Allison noted in *Essence of Decision* that institutional positions often shape stances among policymakers, leading to bureaucratic inertia and compartmentalized responses. Government bureaucrats often react to incidents on the basis of departmental norms instead of developing the most appropriate solution to a challenge (Allison 1971, 176). Hence, whether government employees follow organizational norms in managing problems is often prioritized over a problem's actual resolution. As such, Taiwan's lack of integrated interagency response mechanisms places it at risk of inefficiently reacting to foreign hybrid threats targeting its submarine cables.

Taiwan's Current Countermeasures Against Gray Zone Attacks on Submarine Cables: *Deterring* Malicious Actors

As an archipelago in the Indo-Pacific, Taiwan heavily relies on subsea cables for domestic and international communications during both peacetime and wartime. Hence, strengthening the nation's digital resilience against external threats to subsea cables is a crucial priority of the Taiwanese government. Since late 2018, when extensive media coverage emerged regarding damage to Taiwan's subsea cables due to illegal dredging activities by Chinese ships (Turton 2025; Braw 2023), Taiwan has implemented both legal and technical deterrence measures to address similar threats.

Taiwan has modified its domestic regulations to impose stricter

penalties on illegal dredging around its territorial waters. In 2020, Taiwan's Legislative Yuan amended Article 18 of the Taiwanese *Law on the Exclusive Economic Zone and the Continental Shelf*, which specifies the types of legal actions available in cases of violation (Huang and Chung 2020). Violators may be fined, have their operating license suspended, be charged with a civil lawsuit, or be pursued with criminal violations by the public office, depending on the severity of their behaviour. In 2023, the Legislative Yuan modified Article 36 of the *Sand and Gravel Excavation Act*, which specifies a fine for related misconduct (Hsieh and Chen 2023). Both of the modifications are aimed at deterring illegal activities. In addition to legal deterrence, Chunghwa Telecom owns and operates the majority of Taiwan's external subsea cables and has developed the Submarine Cable Automatic Warning System, with this system being a response to repeated damage caused by illegal dredging and trawling vessels under Chinese flags near Matsu and other outlying islands (Legislative Yuan 2023). This detection system, which serves as a technical support for deterrence, incorporates tracking signals from the shipboard Automatic Identification System (AIS), a standard safety and tracking system required by the International Maritime Organization and other management bodies enabling authorities to monitor vessels approaching Taiwan's subsea cables. When a suspicious vessel approaches a cable, an alert message is broadcast via the Navigational Telex system to the approaching ship. Taiwanese Coast Guard and law enforcement agencies are also notified of the incursion and can subsequently decide whether to take action.

Although these measures may discourage actors with general illegal intentions, they are unlikely to deter gray zone operations orchestrated by state-backed entities, as state-sponsored aggressors with strong strategic incentives likely switch off their onboard AIS or conduct GPS spoofing to conceal their identity and seek to damage subsea cables through all possible means. Defenders of these cables may only realize an attack has taken place after substantial damage has already been inflicted. Given the relatively high benefits of gray zone tactics, efforts

to reduce malicious actors' intention to engage in this behavior are met with considerable challenges, which highlight the limitations of employing traditional deterrence approaches that build digital resilience by raising law enforcement penalties against hybrid threats (Matisek 2017).

Nevertheless, the use of deterrence generally follows logics such as "deterrence by punishment" or "deterrence by denial" (Mazarr 2018; Snyder 1959). For deterrence by punishment, as explained above, the government of Taiwan has employed legal penalties to deter malicious intentions to damage subsea cables. However, legal deterrents are typically only effective for ordinary malicious actors rather than state-sponsored groups. Deterring state-sponsored sabotage is very difficult, as states always have resources, time, and incentives to achieve their eventual objective in an anarchic international environment. In addition, even if Taiwan broadens its strategy to "deterrence by denial" alone, this strategy would place excessive emphasis only on impairing the "means" of sabotage without creating conditions for preventing the adversary from trying to achieve the "end" of digital blockade by altering the adversary's perception regarding whether to do so is in its interest. Taiwan's action would be passive, ceding intent, time, and place to the adversary's actions. As such, this paper suggests that Taiwan should develop a compound strategy of going beyond "deterrence by punishment" and "deterrence by denial" by employing psychological/influence/information strategies that function as measures to undermine an adversary's vision of achieving a digital blockade via gray zone subsea cable activities.

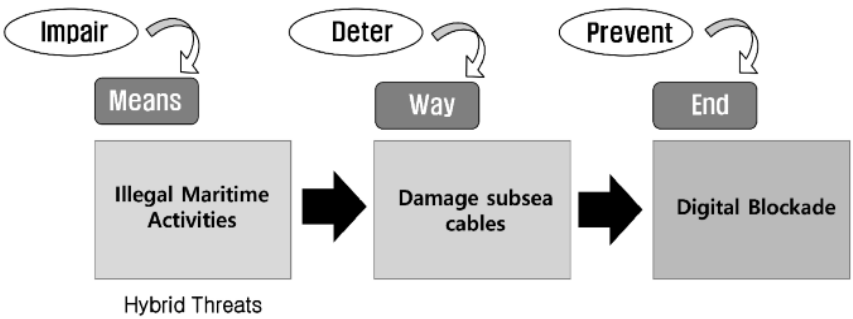
In accordance with the conceptual framework depicted in Figure 2, for malicious state actors the success of a strategy relies on the simultaneous substantiation of the three elements of the strategic triad: ends, means, and ways. Consequently, the defender can disrupt the attackers' strategy as long as any element of the strategic triad is sufficiently undermined. While Taiwan has complicated legal tools to deter malicious actors from subsea cable attack, more emphasis should be placed upon ***impairing*** potential ***means*** and ***preventing*** adversaries

from achieving their ***ends***.

In essence, this article proposes that Taiwan's countermeasures should involve disconnecting the alignment of a gray zone strategy's ***ends***, ***ways***, and ***means***, such that the gray zone aggressor perceives the strategy as unlikely to work, rather than deterring states' malicious intentions outright. Given the challenges of deterring malicious intentions and the necessary alignment of objectives, methods, and means for state actors' successful gray zone strategies, Taiwan's defense strategy should also focus primarily on impairing malicious state actors' access to means (illegal maritime activities) and preventing adversaries from achieving their strategic end (digital blockade). Even if the ***ways*** (i.e., malicious state actors' intention to damage cables) cannot be eliminated, successful impairment of the available ***means*** for illegal activities or prevention of malicious state actors' ***end*** of staging digital blockades can mitigate the effects of gray zone attacks and strengthen digital resilience, as depicted in Figure 4. Accordingly, the following two sections outline recommended strategies for impairing means *(hybrid threats)* and preventing ends *(digital blockades)*.

Figure 4

COMPOUND STRATEGY TO DETER AND COUNTER GRAY ZONE ATTACKS ON SUBSEA CABLES



Impairing Means (Hybrid Threats)

Rather than merely focusing on deterring malicious intentions through the threat of punishment, Taiwan can block access to potential resources that malicious state actors could exploit by proactively managing emerging threats and strengthening capacity across the following five domains.

First, boosting the capacity to monitor suspicious vessels and dark/shadow fleets: Given the risks to subsea cables globally, Taiwan could proactively confront incoming threats rather than simply responding to incidents. At the global level, given that there are known incidents of cable cutting in Europe and Asia, Taiwan could consider collaborating with countries in these areas in order to exchange information on the movements of dark/shadow fleet vessels around the world. At the regional level, while the risk of communication disruption to neighboring countries of Taiwan is more imminent compared to countries in other parts of the world, such proactive measures could include closer collaboration with like-minded countries to establish a blacklist of suspicious vessels, track and share their movements, and conduct joint policing. A concrete example is the Information Fusion Centre (IFC), operated by Singapore, for enhancing maritime security in the South China Sea. In addition, many of the suspicious vessels and dark/shadow fleets often operate in conditions of AIS or GPS spoofing, and it would be an opportunity for Taiwan to convince the neighboring countries to facilitate more cross-border collaboration for maritime surveillance. Finally, with the advancement of artificial intelligence (AI) technology, the application of pattern recognition to ship surveillance data and AI-driven automated alert systems could also provide timely warnings whenever suspect vessels approach sensitive waters.

Second, establishing cable protection zones: Although the decision to board and investigate a foreign-flagged ship over the high seas is controversial, countries such as Australia have developed domestic legal tools to regulate maritime activities within their EEZ (Jacob 2020a4).

Taiwan can learn from these practices and designate cable protection zones within its jurisdiction to impair access to illegal maritime activities under the cover of fishing, dredging, and other commercial activities, which are often used by foreign adversaries.

Third, improving cross-agency coordination: Rather than mere legal infractions, attacks on subsea cables could be considered serious national security threats requiring cross-agency collaboration. Securing subsea cables, just like many other hybrid threats, requires public and private close partnership, as such attacks exploit the significance of private assets in national security. Taiwan understands that not only are many of the subsea cables operated by the private sector, but also, as argued in earlier parts of this paper, a gray zone attack on subsea cables very often treats politics as an extension of war by unconventional means. Hence, the Whole-of-Society Defense Resilience Committee, established by Taiwan on June 19, 2024, continues to promote ideas and develop procedures to enhance societal resilience via regular meetings every three months in principle. However, the reality is challenging. As Deng Xiaoping famously reflected on how the Chinese Communist Party won its conflict with Chiang Kai-shek, "[t]he reason we defeated Chiang Kai-shek is that we did not always fight in the conventional way. Our sole aim is to win by taking advantage of given conditions" (Weber 2021, 156). The Whole-of-Society Defense Resilience Committee is an advisory body under Taiwan law with no actual administrative power, and standard operational procedures are often insufficient for managing hybrid threats. Hence, the government of Taiwan should not leave agencies to manage related challenges individually within their own areas of responsibility. Instead, a centralized command entity should be designated and given sufficient responsibility and authority to oversee coordination and response efforts in a timely manner.

Fourth, strengthening international cooperation: On September 25, 2024, the US led fourteen nations—including the UK, EU members, and key Indo-Pacific allies—to sign the New York Joint Statement on

the Security and Resilience of Undersea Cables, signifying an intention to increase investment in cable protections in response to growing security concerns (European Commission 2024). The joint statement was also endorsed under the Trump Administration in the G7 Foreign Ministers' Declaration on Maritime Security and Prosperity, which was released on March 14, 2025 (US Department of State 2025). Taiwan could leverage its strategic geopolitical position at the center of cables crossing the Indo-Pacific to deepen cooperation with allies and strengthen joint enforcement measures surrounding concerns over subsea cable security.

Fifth, protecting cable landing stations: Although focus has primarily been devoted to maritime activities, security measures should also extend to cable landing stations, which are subject to less jurisdictional ambiguity, are more accessible via land, and are even more vulnerable than subsea cables to physical sabotage and cyberattacks (Cannon 2025, 4). Taiwan must fortify the land-based physical and information security of these critical installations in light of their direct security implications for subsea cables.

Preventing Ends (Digital Blockades)

To counter gray zone operations, adversaries should be prevented from achieving a digital blockade. Prevention efforts can encompass both creating barriers to adversaries' strategic objectives and building capacity for rapid recovery. Suggested measures are as follows.

First, increasing the difficulty of digital blockade attempts: Taiwan could reinforce nearshore cables, which are highly accessible and more vulnerable to attacks than are other cables, with steel pipe casings that incorporate protective layers. Additionally, the sustainability of subsea communications often hinges on minimizing the mean repair time during the cable's operational service life. However, only a few specialized business actors are involved in cable maintenance, which substantially

increases the time and effort required to schedule repair work (Runde et al. 2024). Hence, Taiwan could increase the number of external subsea cables and promote related infrastructural investment, which may ultimately prove cheaper than the financial, political, and security costs of the maintenance required after an incident. In addition, the installation of new cables involves complex legal and administrative due process implicating numerous government agencies with fragmented authority. Thus, Taiwan could simplify its regulatory procedures for the installation of new submarine cables through proper digitalization, which can encourage investment, increase redundancy, and reduce the risk of single points of failure.

Second, reducing exposure to digital blockade risks: On the one hand, to the west of Taiwan, the Taiwan Strait is approximately 60 meters deep on average, and the shallow underwater terrain renders subsea cables in this region vulnerable to maritime activities. Taiwan could bury cables with better protection in this area, accepting the trade-off between maintenance and security, as well as adopt a more distributed cable network topology. Taiwan could avoid laying cables in geologically sensitive areas and ensure deployment of alternative communication methods, such as microwave and satellite technology, particularly within outlying islands such as Kinmen and Matsu. On the other hand, to the east of Taiwan, because of Taiwan's geopolitical position in the Indo-Pacific, a vast number of international subsea cables travel through the fragile underwater terrain to the east and south of Taiwan without reaching the island's shore. Hence, land conduits or land-based infrastructure spanning northern to southern Taiwan can be developed to avoid these geographically hazardous areas. These efforts can encourage cable landing in Taiwan, thus improving subsea cable security and increasing Taiwan's digital resilience at the same time.

Third, minimizing the duration of disruptions: Given that submarine cables are private assets, their maintenance relies on zone-based agreements with international repair contractors with distributed domains of responsibility (Agarwal 2024, 120). Taiwan could streamline

entrance procedures and work permits for cable repair vessels operating within designated protection zones to minimize any communication downtime resulting from unnecessary administrative delays. Additionally, given the capital-intensive industry to which specialized ships for cable repair and laying belong, Taiwan could collaborate with like-minded countries (e.g., the US, the UK, and Japan) in joint ventures to improve cable-laying and repair capabilities. Backup communication mechanisms could also be strengthened. Satellite and microwave links, which have traditionally been used for emergency communication, have limited bandwidth. The rapid development of low-Earth orbit (LEO) satellite networks, such as Starlink, OneWeb, Telesat, and Kuiper, and the high demand for satellite distribution and inter-satellite communications, have provided new opportunities to improve backup connectivity. Taiwan could invest in redundant satellite communication mechanisms and establish offshore ground stations to ensure continuous connectivity during cable disruptions.

Conclusion and Implications for Policymakers

Global communications are facilitated by subsea cables, which are wired rather than wireless, territorial rather than borderless, and bottlenecked rather than distributed. The case of Taiwan presented herein illustrates that countering foreign threats to subsea cables requires alternative thinking and a compound approach, including impairing the ability of malicious actors to exploit key resources and preventing them from achieving strategic objectives. Policymakers must have a more nuanced strategic understanding and better technological literacy to contribute to the global conversation on security challenges to digital infrastructure. Given the growing global focus on submarine cable security, policymakers must actively shape this strategic terrain by participating in international dialogues, investing in technological advancements, and strengthening public–private partnerships and

international cooperation to safeguard critical communication infrastructure in order to live through this complex challenge in the 21st century.

Furthermore, many of the subsea cables that travel through Taiwan also pass by the contested geopolitical hotspot of the South China Sea. Considering the growing tension of territorial disputes in the area, some may worry that international telecom carriers could decide to avoid going through the South China Sea, which would accidentally marginalize Taiwan's status in international subsea communications. However, these claims often ignore that Taiwan's significance in international communication is not only due to its geolocation, but also the actual demand of network traffic from the numerous international data centers operated by Amazon, Google, Meta, and Microsoft on the islands. For the foreseeable future, as long as substantial network traffic needs to visit Taiwan, security over subsea cables around Taiwan remains a central issue of transoceanic communication and global cybersecurity.

Hence, rather than providing a prescriptive universal solution for all countries, this paper presents Taiwan as a case study to illuminate alternative methods of managing subsea cable attacks that are contingent upon the geopolitical context in which an individual country is located. The key contribution of this paper is the compound strategy proposed for strengthening the prevention of gray zone operations by malicious state actors and circumvention of their objectives to compensate for the limitations of the deterrence-based strategy currently in place to protect Taiwan's subsea cables. Amidst ongoing investments and regulatory changes worldwide due to submarine cable security becoming an international focal point, this paper offers the following three considerations for policymakers.

First, policymakers must actively track ongoing dialogues surrounding global subsea cable governance, including conversations on redefining governance norms under the UNCLOS framework and exploring whether subsea cables should be classified as global commons. Additionally, states should closely follow any future development of the New York Joint Statement on the Security and Resilience of Undersea

Cables in a Globally Digitalized World, which was initiated by the US in September 2024. In November 2024, the International Advisory Body for Submarine Cable Resilience was established by the International Cable Protection Committee to improve global standards for submarine cable security (ITU 2024). Sustained participation in the development of relevant international frameworks is crucial for policymakers to ensure their strategies remain current and contextually appropriate.

Second, investment in the development of technological solutions for the protection of communications infrastructure is vital. Although subsea cables remain the backbone of global digital communications, policymakers should explore alternative technologies to mitigate the risk of digital blockades, including advancements in LEO satellite networks and high-frequency microwave communication. Additionally, unmanned systems can be deployed for communication relay, subsea cable inspection, maritime reconnaissance, and cable maintenance to address security gaps that cannot be mitigated through diplomatic or regulatory means.

Finally, public–private partnerships must be strengthened to promote subsea cable security. Although subsea cables are privately owned, threats to their security directly affect national stability. Thus, improvements must be made in terms of public–private collaboration, which may include efforts to strengthen cooperation between government agencies, maritime and fishery industries, and international telecommunications operators to establish rapid intelligence-sharing mechanisms. Furthermore, policymakers worldwide should promote joint efforts between regulatory bodies, telecommunications firms, and cable operators to develop security technologies and improve cable repair capabilities. Partnerships with international organizations and nongovernmental entities should also be strengthened to promote information-sharing and cross-border enforcement efforts.

Ultimately, states can learn from international best practices and adopt innovative approaches to boost the resilience of their submarine cable infrastructure and mitigate risks posed by foreign adversaries.

References

Agarwal, Soham. 2024. "Enhancing Capacity-of and Capabilities-In Repair of submarine Communication Cables through International Cooperation." In *Viewing Maritime Activities Through a Legal Lens* (eds. P. Chauhan and J. Vachaparambil), 116. New Delhi: National Maritime Foundation.

Al Jazeera. 2025. "'We see you': How a Russian spy ship prompted a UK scramble." *Al Jazeera*. January 23. https://www.aljazeera.com/news/2025/1/23/we-see-you-how-a-russian-spy-ship-prompted-a-uk-scramble

Allison, Graham. 1971. *Essence of decision: explaining the Cuban missile crisis*: Boston: Little, Brown and Company.

Azaria, Danae, and Tara Maria Davenport. 2024. "Submarine Cables and Pipelines under International Law: [Third] Interim Report 2024." International Law Association. London, UK. https://discovery.ucl.ac.uk/id/eprint/10196160/

Bafoutsou, Georgia, Maria Papaphilippou, and Marnix Dekker. 2023. Subsea Cables—What is? European Union Agency for Cybersecurity. Brussels, Belgium. https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf

Bartles, Charles. 2016. "Getting Gerasimov right." *Military Review* 96/1: 30-38.

Besch, Sophia, and Erik Brown. 2024a. "A Chinese-Flagged Ship Cut Baltic Sea Internet Cables. This Time, Europe Was More Prepared." Carnegie Commentary. December 3. https://carnegieendowment.org/emissary/2024/12/baltic-sea-internet-cable-cut-europe-nato-security?lang=en

Besch, Sophia, and Erik Brown. 2024b. *Securing Europe's Subsea Data Cables*: Carnegie Paper. December 16. https://carnegieendow-

ment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en

Braw, Elisabeth. 2023. "China Is Practicing How to Sever Taiwan's Internet." *Foreign Policy*. February 21. https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/

Bueger, Christian, and Tobias Liebetrau. 2021. "Protecting hidden infrastructure: The security politics of the global submarine data cable network." *Contemporary Security Policy* 42/3: 391-413.

Cannon, Brendon. 2025. "Undersea cable security in the Indo–Pacific: Enhancing the Quad's collaborative approach." *Marine Policy* 171: 106415.

Carter, Nicole et al. 2023. Protection of Undersea Telecommunication Cables: Issues for Congress. Congressional Research Service. August 7. https://www.congress.gov/crs-product/R47648

Davidson, Helen. 2025. "Taiwan investigating Chinese vessel over damage to undersea cable." *The Guardian*. January 7. https://www.theguardian.com/world/2025/jan/07/taiwan-investigating-chinese-vessel-over-damage-to-undersea-cable

Deibert, Ronald J, Rafal Rohozinski, and Masashi Crete-Nishihata. 2012. "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war." *Security Dialogue* 43/1: 3-24.

DHS. 2024. Priorities for DHS Engagement on Subsea Cable Security & Resilience. December 18. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/publication/priorities-dhs-engagement-subsea-cable-security-resilience

European Commission. 2024. The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World. European Commission. September 26. https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world

Focus Taiwan News. 2025. "Undersea cable linking Taiwan-Matsu disconnects again." *Focus Taiwan News*. February 17. https://fo-

custaiwan.tw/sci-tech/202502170012

Ganz, Abra, Martina Camellini, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi. 2024. "Submarine cables and the risks to digital sovereignty." *Minds and Machines* 34/3: 1-30.

Guarascio, Francesco, Phuong Nguyen, and Joe Brock. 2024. "Exclusive: Inside the US push to steer Vietnam's subsea cable plans away from China." *Reuters*. September 18. https://www.reuters.com/business/media-telecom/inside-us-push-steer-vietnams-subsea-cable-plans-away-china-2024-09-17/

Hsieh, Chun-lin, and Yu-fu Chen. 2023. "Illegal PRC dredgers to be confiscated." *Taipei Times*. December 19. https://www.taipeitimes.com/News/front/archives/2023/12/19/2003810833

Huang, Hsin-po, and Jake Chung. 2020. "MOI drafts stricter punishments for illegal sand mining." *Taipei Times*. July 16. https://www.taipeitimes.com/News/taiwan/archives/2020/07/16/2003740025

Hughes, David. 2025. "Russian spy ship in UK waters warned off by Royal Navy." *Independent*. January 22. https://www.independent.co.uk/news/uk/home-news/russia-ship-royal-navy-b2684289.html

ITU. 2024. "Launch of international advisory body to support resilience of submarine telecom cables." International Telecommunication Union. November 29. https://www.itu.int/en/mediacentre/Pages/PR-2024-11-29-advisory-body-submarine-cable-resilience.aspx

Jacob, Jessie. 2024. "Let's take a close look at how we protect our undersea cables." Australian Strategic Policy Institute. August 30. https://www.aspistrategist.org.au/lets-take-a-close-look-at-how-we-protect-our-undersea-cables/

Legislative Yuan. 2023. "Research on legal issues related to liability for damage to submarine cables" ["海底電纜毀損責任相關法制問題研析" (Haidi dianlan huisun zeren xiangguan fazhi wenti yanxi")]." Legislative Yuan. March 30. https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=227877

Matisek, Jahara W. 2017. "Shades of gray deterrence: Issues of fighting

in the gray zone." *Journal of Strategic Security* 10/3: 1-26.

Mazarr, Michael J. 2015. *Mastering the gray zone: understanding a changing era of conflict*. Carlisle, PA: Army War College Press.

Mazarr, Michael J. 2018. *Understanding Deterrence*. Santa Monica, CA: RAND Corporation.

Palmieri, Francesco, Ugo Fiore, Aniello Castiglione, Fang-Yie Leu, and Alfredo De Santis. 2013. "Analyzing the internet stability in presence of disasters." Security Engineering and Intelligence Informatics: CD-ARES 2013 Workshops: MoCrySEn and SeCIHD. September 2-6. Proceedings 8. Regensburg, Germany.

Qiao, Liang, and Wang Xiangsui. 1999. *Unrestricted warfare [Chao xian zhan (超限战)]*. Beijing, China: PLA Literature and Arts Publishing House *[Jiefangjun wenyi chubanshe (解放军文艺出版社)]*.

Rajan, Shruthi. 2024. "Gaps in Governance: Lack of State Responsibility in Regulation of Flag of Convenience and Its Impact on Laborers." *International Journal of Law Management & Humanities* 209. 2837-2842.

Reuters. 2024. "Finland moves tanker suspected of undersea cable damage closer to port." *Reuters*. December 28. https://www.reuters.com/world/europe/finland-moves-tanker-suspected-undersea-cable-damage-closer-port-2024-12-28/

Runde, Daniel et al. 2024. "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition." Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Ryan, Sophie. 2024. "Submarine Communication Cables and Belligerent Rights in Armed Conflict." *Ocean Yearbook Online* 38/1: 459-503.

Saito, Yusuke. 2019. "Reviewing Law of Armed Conflict at Sea and Warfare in New Domains and New Measures: Submarine Cables, Merchant Missile Ships, and Unmanned Marine Systems."

Tulane Maritime Law Journal 44: 107-125.

Satariano, Adam. 2019. "How the Internet Travels Across Oceans." *New York Times*. March 10. https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html

Snyder, Glenn. 1959. *Deterrence by denial and punishment*. Woodrow Wilson School of Public and International Affairs, Center of International Studies. Princeton NJ.

Starosielski, Nicole. 2015. *The undersea network*. Durham, NC: Duke University Press.

Sun Tzu. 2009. *The Art of War*. Singapore: Pax Librorum.

Sytas, Andrius, and Johan Ahlander. 2025. "Sweden opens sabotage probe into Baltic undersea cable damage." *Reuters*. January 27. https://www.reuters.com/world/europe/baltic-undersea-cable-damaged-by-external-influence-sunday-latvian-broadcaster-2025-01-26/

Taiwan News. 2023. "Matsu undersea cable repaired ending 50 day internet outage." *Taiwan News*. March 31. https://www.taiwannews.com.tw/news/4852575

TeleGeography. 2025. Submarine Cable Map. TeleGeography. March 11. https://www.submarinecablemap.com/country/taiwan

Turton, Michael. 2025. "Notes from Central Taiwan: Cable cutting as strategy." *Taipei Times*. January 13. https://www.taipeitimes.com/News/feat/archives/2025/01/13/2003830099

UN General Assembly. 1974. Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX). United Nations.

UN General Assembly. 2010. Oceans and the law of the sea. A/RES/65/37.

US Department of State. 2025. G7 Foreign Ministers Declaration on Maritime Security and Prosperity. US Department of State. March 14. https://www.state.gov/g7-foreign-ministers-declaration-on-maritime-security-and-prosperity/

Weber, Isabella M. 2021. *How China escaped shock therapy*: *The market reform debate*: Abingdon-on-Thames, UK: Routledge.

Wu, Sarah, and Eduardo Baptista. 2022. "From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit." *Reuters*. August 5. https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/

Article submitted 4/6/25, revised 7/9/25, accepted 7/31/25.