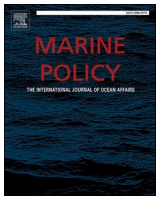
Marine Policy 180 (2025) 106809

Contents lists available at ScienceDirect

Marine Policy

journal homepage: www.elsevier.com/locate/marpol



Undersea cables, geoeconomics, and security in the Indo-Pacific: Risks and resilience

ARTICLE INFO

Keywords:
Undersea cables
Submarine cables
Subsea cables
Geoeconomics
Security
Critical infrastructure
Telecommunications
Economic security

ABSTRACT

Undersea cables constitute the critical infrastructure of international data connectivity, transmitting over 95 % of global Internet traffic, and they have attracted increasing attention from policymakers recently. How are threats to undersea cable networks evolving, and why is cable competition intensifying in the Indo-Pacific region? How is the policy discourse around undersea cables changing, and what implications does this have for the physical realities of these networks and their resilience? This article introduces a framework for understanding recent developments and presents an analysis of cross-regional trends, providing the foundation for a Special Issue of *Marine Policy*. First, the article argues that risks to cable networks can be characterized along two dimensions—source and frequency—and that the fundamental risks to undersea cables have not changed dramatically. Instead, it is the understanding of these risks that has evolved due to securitization of the maritime and economic domains, driven partly by intensifying US-China rivalry. Second, although the extent to which the new discourse of cable securitization resonates varies across countries and companies, securitization is already reshaping the physical layout of regional cable architecture as investments are redirected to account for changing understandings of risk. Third, ensuring resilience requires a "whole life cycle" approach to cables that considers not only investment and construction but also licensing, regulation, maintenance, protection, and repair. By integrating undersea cables into broader discussions across marine policy, economics, and security, this article enables scholars and policymakers to more comprehensively assess risks and to formulate more effective solutions.

1. Introduction

Submerged deep beneath the ocean, networks of undersea cables—also known as submarine cables or subsea cables—form the critical infrastructure that enables the communication and connectivity upon which societies are built [1]. Over 95 % of global Internet traffic relies on these undersea cables for high-volume, high-speed transmission of information, and they transmit approximately $10 trillion in financial transactions data throughout the global economy on a daily basis [2,3]. Undersea cables can carry far more data at a lower cost than satellites, so as Nicole Starosielski puts it, "Despite the rhetoric of wirelessness, we exist in a world that is more wired than ever" [4]. As of June 2025, there were over 600 active and planned cables, with 1.48 million kilometers of undersea cables in service globally (see Fig. 1) [5].

These undersea cables have enabled the boom in information and communications technology that has fueled economic growth and stimulated intellectual exchange across the globe over the past several decades. With the growth of cloud computing, streaming, and ecommerce, undersea cables have become even more essential than before to business and social activity [6]. For example, one study estimated the contribution of undersea cables to the US economy at nearly $649 billion in 2019—about three percent of the total US gross domestic product [7]. Therefore, the strategic importance of these cables will continue to grow "in tandem with our digital dependence" [8].

The Indo-Pacific has been a leading region for undersea cable construction for over a decade, and demand is expected to remain strong as regional digitalization progresses. In recent years, undersea cable construction and security have become the subject of increasing attention from policymakers. How are threats to undersea cable networks evolving, and why is cable competition intensifying in the Indo-Pacific? How is the policy discourse around undersea cables changing, and what implications do these shifts have for the physical realities of these networks and their resilience? This article introduces a framework for understanding recent developments and presents an analysis of cross-regional trends, providing the foundation for a Special Issue of *Marine Policy* that examines undersea cables using a combination of thematic and geographic approaches.

This article makes several arguments. First, risks to cable networks can be characterized along two dimensions (source and frequency), and the fundamental risks to undersea cables have not changed dramatically in recent years—rather, it is the understanding of these risks that has evolved. Specifically, securitization of the maritime and economic domains—driven in part by intensifying US-China rivalry—has affected the discourse around cables across marine policy and other policymaking arenas. Second, although the extent to which the new discourse of cable securitization resonates varies across the Indo-Pacific region, as well as across the public and private sectors, this securitization is already reshaping the physical layout of regional cable architecture as investments are redirected to account for changing understandings of risk. Third, ensuring resilience requires a "whole life cycle" approach that

https://doi.org/10.1016/j.marpol.2025.106809

Available online 24 June 2025

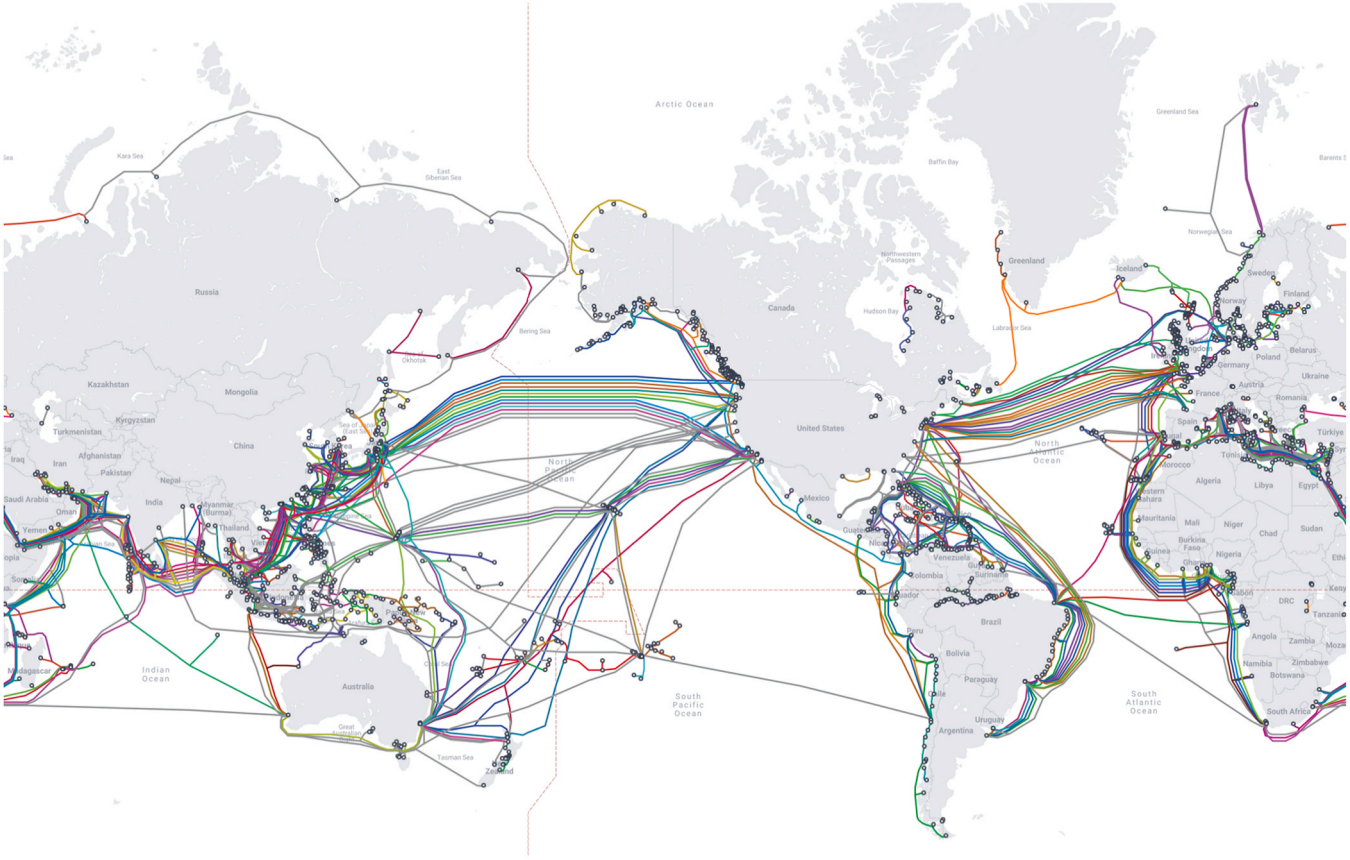


Fig. 1. Map of commercial submarine cables as of June 2025 [9].

considers not only investment in and construction of new cables but also licensing, regulation, maintenance, protection, and repair. The article develops each of these arguments in turn and concludes with a summary of the findings and an overview of the Special Issue.

This article contributes to the existing literature in several ways. First, it integrates discussions of undersea cables with broader discussions of marine policy, foreign policy, and geopolitics. While undersea cables have often been considered a niche issue, they are intimately intertwined with economic issues such as trade, development, and telecommunications, as well as with security issues related to critical infrastructure, sabotage, surveillance, and hybrid warfare. Undersea cables should be recognized as one of the most critical technologies for supporting connectivity and the digital economy, with significant implications for national and international security that extend across marine, terrestrial, and extraterrestrial spaces. Second, the article illuminates the ways that geoeconomics is influencing public and private actors' decisions around undersea cable networks, shaping their physical construction across marine spaces into new configurations that impact the region. However, there is also a distinct lack of consensus about the threats to undersea cables, which complicates the policy-making process. Third, the article enables a more holistic understanding of resilience that may inform more effective scholarship and policy by calling attention to the ways that undersea cables encounter different risks across their life cycle and at the points at which they are embedded within the broader telecommunications ecosystem. Incorporating cables into broader theoretical and empirical discussions enables scholars and policymakers to assess and formulate policy more comprehensively in ways that can effectively ensure the resilience of undersea cables and the societies that they underpin.

Table 1
Sources of risk to undersea cables.

	Routine	Non-Routine
Natural	current abrasion, wildlife attack	mud slide, earthquake, tsunami, cyclone, volcanic eruption
Man-made	fishing, ship anchor, dredging	espionage, sabotage

2. Conceptualizing risks to undersea cables

In the 19th century, the British Empire built a network of undersea telegraph cables linking it to its colonies around the world to expand its trade and colonial rule, and other countries such as the US and Japan later followed suit [10]. Over the decades, these undersea cables were upgraded to reflect new technologies, transitioning to analog coaxial cables of copper beginning in the 1950s and then to long-haul fiber-optic cables beginning in the late 1980s [4]. Since around 2010, growing demand for data transmission capacity from large Internet companies has driven an ongoing cable construction boom and prompted the so-called "hyperscalers"—Amazon, Google, Meta, and Microsoft—to invest in the cable industry.

A typical modern undersea communications cable measures roughly 17 mm in diameter in the case of a deep-water cable to about 70 mm in diameter for a more heavily armored cable in shallower water. These cables often lay exposed on the floor of the ocean, which makes them vulnerable to a wide variety of threats. If the damage is significant, it has the potential to bring down the communication systems of a country or even multiple countries. Even modest amounts of damage to undersea cables can result in serious disruptions in communications and economic activity. Although these cables are generally highly reliable, damage occurs on a regular basis: on average, a cable is damaged somewhere in the world every three days, with roughly 150–200 cable faults occurring each year [11].

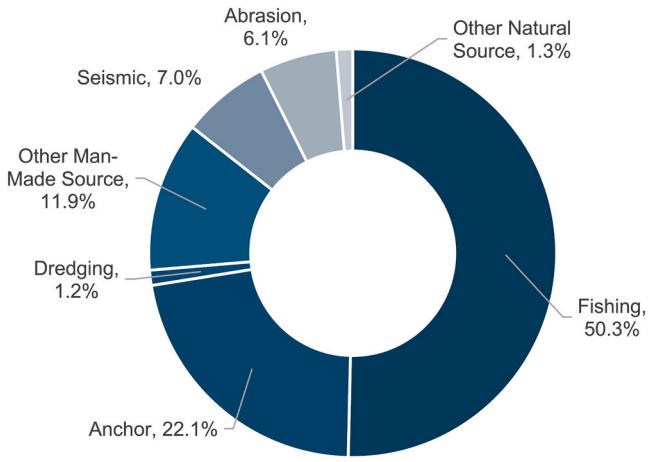


Fig. 2. Causes of faults worldwide on the telecommunications undersea cable network (1986–2023) [15].

In the context of undersea cable networks, *risk* can be understood the possibility of damage arising from a threat. Table 1 classifies potential risks along two dimensions: *source* and *frequency*. In terms of source, some risks have their origins in the *natural* world from marine wildlife, ocean currents, or weather patterns, while other risks are *man-made*. In terms of frequency, risks occur during *routine* activities (i.e., normal and daily operations) or during *non-routine* activities (i.e., exceptional circumstances). These frequencies occur along a spectrum, and the boundary between the two may not necessarily be clear. For example, Table 1 classifies espionage as a non-routine risk, but some analysts have pointed out that espionage is an integral part of statecraft and might therefore be considered to be a relatively routine risk [12]. Similarly, it may not be clear if an undersea cable has been damaged unintentionally or intentionally. It is rarely possible for operators to immediately identify the cause of a cable fault, and it can be challenging or impossible to use vehicle tracking information to determine whether and which vessels may have been present—and it is even more difficult to know if they acted with malice or not [13]. For example, in February 2023, Chinese vessels damaged two cables connecting the Matsu Islands to Taiwan on two separate dates, resulting in an "invisible blockade" that some observers believed was intentionally orchestrated by the Chinese government, but it was not possible to find evidence of such [14]. Nonetheless, separating risks into relative routine or non-routine frequency is a useful way of thinking about their character and associated policy responses.

Considering the intersection of the dimensions of frequency and source, the majority of undersea cable damage results from routine risks emanating from both man-made and natural sources. Fig. 2 shows the causes of cable faults worldwide from 1986 to 2023 [15]. In terms of *routine man-made risks,* fishing activity such as trawling accounted for 50.3 % of all cases, with another 22.1 % arising from ship anchors, which can cause damage to cables when they are fully deployed and dragged along the seabed. *Routine natural risks* such as current abrasion accounted for 6.1 % of faults. Natural wear and damage due to these two types of routine risks mean that the total number of active cables is constantly changing as older cables are decommissioned and new cables are built.

Sources of *non-routine natural risks* include disasters such as mud slides, earthquakes, tsunamis, cyclones, and volcanic eruptions. For example, the 2011 Tohoku earthquake and tsunami damaged about half of the undersea cables running across the Pacific and disrupted Internet connectivity in Japan and elsewhere in Asia [16]. The January 2022 volcanic eruption and earthquake in Tonga cut the only fiber-optic cable linking the country's 170 outer islands to the main island and to each other, leaving the country in a state of isolation that caused serious economic losses and made it impossible to effectively coordinate humanitarian aid. It took five weeks to restore Internet connectivity to the damaged international cable and 18 months to repair the domestic cable [17,18].

Non-routine man-made risks from sources such as sabotage have received increasing attention from the public and private sectors in recent years [19]. Sabotage has been suspected in several recent incidents, including the severance of cables between Estonia and Finland in December 2024 and near Taiwan in January 2025. These concerns have historical precedent. Undersea cables have always been a point of vulnerability in scenarios of conflict [20,21]. For example, both the United Kingdom and Germany cut each other's undersea cables during World War I, and the United States used the same military tactic during the Spanish-American War [10]. Since the beginning of the war in Ukraine, concerns have arisen that Russia could destroy the undersea cables connecting Europe and the US to the Internet or that China could cut the cables to Taiwan in the event of a conflict. Technological developments such as uncrewed undersea vehicles (UUVs) also present potential security challenges to cables if they are used to cut connections [22].

Espionage and surveillance are also concerns that have historical precedent. The British Empire took advantage of its dominance of the international telegraph infrastructure to surveil messages for intelligence purposes [23]. In the present too, controlling a cable landing station enables a government to more easily spy on traffic moving through the network. When the US Justice Department blocked the Pacific Light Cable Network in June 2020, it cited concerns that the project would advance the goal of the Chinese government to make Hong Kong a dominant hub for telecommunications infrastructure, which would increase the share of US data traffic moving through PRC territory and therefore increase the risk of espionage [24]. Even outside of Chinese territory, there are concerns that Chinese companies involved in undersea cable construction and operation could be required to cooperate with their government's intelligence efforts, leading to surveillance and espionage [25]. In addition, an increasing number of cable companies are using remote management systems to virtually monitor and control cable systems over the Internet. These systems have cost and efficiency advantages and can offer insights into marine activity surrounding the undersea cables, but they can also create cybersecurity vulnerabilities, creating opportunities for malicious actors to access or disrupt data from the cable or to damage cable infrastructure [26].

3. Securitization and changing understandings of the cable risk landscape

Considering the risks to cable network infrastructure, it is not surprising that security has been a concern since the earliest days of undersea cable construction. Despite their vulnerabilities, undersea cables have often been embraced as a more secure alternative to radio and satellite due to the insulating effect of the ocean's depths, which offered a layer of protection from disruption from man-made sources [4]. The fundamental sources of risk for undersea cables have not changed dramatically over the years—rather, it is the understanding of these risks and how to deal with them that has continually evolved.

It is notable that among the four types of risk described previously, concern about non-routine man-made risks has more strongly ebbed and flowed alongside international events, often reflecting the "dominant cultural fears of the time," such as sabotage from a rival superpower during the Cold War or from terrorists in the aftermath of dramatic attacks [4]. Most recently, these worries have intensified alongside US-China competition, which has led to the securitization of undersea cables, particularly in the Indo-Pacific region [27]. Securitization is a process whereby actors transform issues into matters of security through speech acts that claim that a referent faces an existential threat and convinces an audience that extraordinary measures are necessary to deal with this threat [28]. In doing so, they may be able to mobilize increased attention and resources from the public and private sectors to address

these issues, but there may also be negative consequences from securitization.

The integrity of undersea cable networks is not inherently a security issue; indeed, discussions of cables can be framed within a discourse of economic and technological development, which is common in places such as Southeast Asia and the Pacific Islands [29,30]. However, they have increasingly been caught up in three parallel processes of securitization. First, the maritime domain as a space has been increasingly securitized, which has had consequences for marine policy. This process began with the introduction of the concept of "maritime security" as a way of thinking about security at sea in the 1990s, and as the oceans have become dense sites of national, regional, and global infrastructure, countries' dependency on them has increased [31]. Moreover, over the last decade, the common areas of the maritime domain (i.e., the high seas) have also been securitized alongside concerns about China's increasingly aggressive behavior in the East and South China Seas and its use of gray zone strategies [32,33].

Second, the economic realm as a whole has been securitized in recent years. This has also been intertwined with the resurgence of two related concepts in the existing scholarship: geoeconomics and economic statecraft. Geoeconomics is "the use of economic instruments to attempt to promote and defend national interests and to produce beneficial geopolitical results," as well as "the effects of other nations' economic actions on a country's geopolitical goals" [34]. Economic statecraft is essentially a subset of the definition of geoeconomics; it is the use of economic means to pursue non-economic ends [35]. The instruments of geoeconomics or economic statecraft could be designed to cause a negative impact, through an embargo, boycott, tariff increase, or sanction, or they could try to entice actors through favorable trade terms, aid, subsidies, or investment. Essentially, economic activity is now increasingly perceived as linked to security concerns, and governments are intentionally crafting their policies to leverage their economic influence or protect their economies. For example, the Chinese government's strategic use of investment through its Belt and Road Initiative and its use of economic coercion have often been cited in discussions of geoeconomics [36]. Others have discussed the ways that the US has used "weaponized interdependence" by leveraging global networks of informational and financial exchange for strategic advantage [37].

Undersea cables can be easily linked to geoeconomic concerns, since connectivity underpins economic prosperity and national interests, and loss of such connectivity could be devastating both in peacetime and in conflict. Governments have used investment to influence the geography of undersea cable construction in ways that support their national political and security goals. For example, China has tried to support the participation of Chinese companies in undersea cable projects as part of its "Digital Silk Road" [38]. While Chinese companies were involved with only 7 % of disclosed cable projects between 2012 and 2015, they were expected to participate in 20 % of such projects between 2016 and 2019 [39]. However, other countries have expressed concerns that authoritarian governments such as China and Russia are reshaping the Internet's physical layout through companies that control Internet infrastructure, routing data in ways that will allow them to control and monitor data across both marine and terrestrial spaces, which poses risks to democracy, freedom of expression, and privacy [40]. In response, countries such as the US, Australia, and Japan have in turn tried to use their own geoeconomic instruments to alter the geography of undersea cable networks in ways that favor their national interests, as will be discussed further in Section 3.

Third, the cable industry itself has to some extent facilitated the securitization process. Cable companies historically took an approach of "security through obscurity"; information about cable networks was withheld from the public with the rationale that this would increase their security. However, this approach became unsustainable as the Internet made information on cable technologies, manufacturers, routes, repair ships, and landing sites more readily available to the public [41]. Moreover, over time, companies came to believe that the invisibility of undersea cables to governments, customers, and others was a liability because it meant that decisionmakers lacked the information needed to make networks more robust and accessible [4]. This invisibility also made it difficult to get help from governments to protect their assets and rights. Consequently, companies have demanded that governments devote increased attention and funding to the security of cable networks, thereby contributing to the securitization of the discourse.

As a result of these concurrent trends, the connection between undersea cables and security has been recognized across a wider range of public and private actors. This critical infrastructure has always been of some interest to those specializing in marine policy and telecommunications, but now cables are also a matter of regular discussion in circles more focused on general matters of economics, security, and politics. However, this does not mean that there is a consensus among stakeholders about the risks to cable networks and the desired solutions, which will be discussed further in the next section.

4. From risk perceptions to infrastructural realities

A key finding of this article and the associated Special Issue of *Marine Policy* is that the extent to which undersea cables have been securitized varies across the Indo-Pacific region, as well as across the public and private sectors. This lack of shared understanding is important because it complicates the policymaking process. The securitization discourse has been most strongly internalized in countries such as Australia, India, Japan, New Zealand, and the US [42–46]. However, for many countries in the Indo-Pacific region—particularly those in Southeast Asia and the Pacific Islands—the dominant view of undersea cables is that they are essential to communication and economic development [29,30]. In many of these areas, connectivity is currently very limited, so the primary concern of their governments is facilitating the construction of new cables, regardless of the nationality of the companies that might provide them. For these countries, non-routine man-made risks such as espionage and sabotage are the least salient, and the securitization of undersea cables has not been widely accepted.

In addition, there is not necessarily consensus across the region on the potential actors behind non-routine man-made risks. Although the governments of some countries have expressed concern about surveillance by China, for example, others point out that there are also dangers of espionage from the US, since section 702 of the US Foreign Intelligence Surveillance Act still permits US intelligence agencies to conduct surveillance activities on foreigners abroad for national security purposes [29]. Considering these differing national perceptions, levels of economic development, and political and legal contexts, it is not surprising that there is a wide diversity of approaches to the regulation of undersea cables across the Indo-Pacific [13,43].

Similarly, risk perception also varies across the public and private sectors. Private sector actors continue to be motivated primarily by business incentives, with the potential for profit or loss weighing most heavily in their calculations. Despite recent government interest, the private sector still plays the primary role in the cable industry. Cables are owned by combinations of private companies, state-owned firms, and international consortia from around the world, for example. The top three suppliers for undersea cables are US-based SubCom, Japan's NEC, and France's Alcatel Submarine Networks, and China's HMN Tech (formerly Huawei Marine Networks) is growing quickly. The "hyperscalers" Google, Meta, Microsoft, and Amazon play a large and increasing role in the industry, purchasing approximately 66 % of available capacity [47]. Other companies are engaged in the cable industry as providers of undersea cable components and related services.

Given their diverse positions in the cable supply chain, these companies have varying positions, but some common trends seem persistent industry-wide [46,48]. First, many companies do not share their governments' perceptions of threats from non-routine man-made risks. Second, some companies are concerned that government initiatives on undersea cables are ad hoc, with questionable impact on overall network

architecture. Third, there are disagreements among public and private sector actors about what constitutes an adequate supply of cables, which suggests that they have different definitions of resilience.

These debates about the nature and urgency of risks to cable networks have high stakes. The policy solutions that address some types of risk actually increase vulnerability to other types of risks. For example, to avoid routine man-made risks and routine natural risks, cable companies have generally tried to group undersea cables along well-established routes and to make their locations well known to maritime actors. However, this solution of centralized, publicized cable routes creates more vulnerability to non-routine man-made risks such as intentional sabotage. Since cables cannot be moved once laid, there is a path dependence to these networks that creates challenges; assessments of risk have the potential to change much faster than the physical realities of cable networks.

The lack of consensus about the risks to cable networks has meaningful implications for marine policy and other policymaking domains. Many factors go into making decisions about undersea cable construction routes. Governments and companies who believe that cost competitiveness and economic development are more important than security concerns are less likely to be receptive to arguments that they should choose more expensive, "trusted" partners for their undersea cable infrastructure. In addition, even if a government believes that security issues are paramount, government-business ties are weaker than they used to be in the era when national telecoms dominated the cable industry. Private companies now have weaker institutional ties to their home states, and they have increasing discretion over cable construction and operations [49]. Although undersea cables used to traditionally connect terrestrial population centers, which required obtaining a landing license from government agencies, they now often focus on connecting data centers; this makes it easier for companies to make decisions to avoid states that are perceived as trying to exert too much control.

However, despite these differences in perspectives, it is clear that the recent wave of securitization and the rising importance of geoeconomics is already reshaping the physical network of undersea cables. On one hand, China's interest in undersea cables has been growing over the years and has been incorporated into its Digital Silk Road initiative, which has in turn shaped its marine policy. The Chinese government seems to share the view that undersea cables are linked to strategic interests, setting out a goal of acquiring 60 % of the global fiber-optic market in its "Made in China 2025" plan [50]. One official Chinese Communist Party outlet claimed that "although undersea cable laying is a business, it is also a battlefield where information can be obtained" [51]. As of 2020, Chinese company HMN Tech had executed 16 undersea cable projects across 27 countries in the Indo-Pacific with considerable support from the Chinese government [52]. One major project is the Pakistan and East Africa Connecting Europe (PEACE) cable, which starts in Pakistan and ends in France; this cable has been described as a "rival" to the similarly located Sea-Me-We 6 (SMW6) cable, from which China's HMN Tech was blocked from participating [53]. China has also been very active in undersea cable construction in Southeast Asia.

On the other hand, the activities of these Chinese entities have in turn led the governments of the US, Japan, Australia, and other countries to become concerned about the political, economic, and security risks associated with dependence upon Chinese-controlled undersea cable infrastructure. These countries have also clearly articulated a link between undersea cables and security that has shaped their respective policies. For example, in their 2024 joint statement, the leaders of the Quad countries—Australia, India, Japan, and the US—discussed the importance of cable networks, "the capacity, durability, and reliability of which are inextricably linked to the security and prosperity of the [Indo-Pacific] region and the world" [54].

Consequently, these countries have reacted by attempting to reshape undersea cable networks in the Indo-Pacific region through their respective policies. They have done so through two primary mechanisms: the pursuit of new routes involving relatively trusted actors and the abandonment of existing or planned routes involving China or other locations perceived to be high-risk.

First, there has been a series of new initiatives by the US and its like-minded partners who have directed investment toward new undersea cable construction projects that they believe will mitigate risks and increase resilience, often by excluding non-trusted companies from countries such as China. The Pacific Islands region has been a particularly pronounced site of geoeconomic competition [30,46,55]. For example, in 2018, the Australian government announced that it would provide development funding to support a new undersea cable to the Solomon Islands and Papua New Guinea, displacing Huawei Marine's interest in providing a similar cable. A joint Japan-US-Australia partnership to fund a branch cable off Palau was announced in 2019, and the three countries agreed to fund an additional cable connecting Nauru, Kiribati, and the Federated States of Micronesia in 2021. In 2023, Australia and the US announced the Hawaiki Nui cable and the South Pacific Connect cable initiative with the potential to connect nine Pacific Island countries [46]. In May 2023, Australia, India, Japan, and the US also announced the Quad Partnership for Cable Connectivity and Resilience to address gaps in the infrastructure and coordinate on future builds [56]. By September 2024, the Quad countries had committed over $140 million to undersea cable builds in the Pacific [54].

Governments have also tried to reshape these new routes by discouraging the involvement of suspicious companies and their products, emphasizing the importance of trusted partners. Some governments have advocated for the exclusion of Chinese companies, such in the case of the Sea-Me-We 6 (SMW6) cable connecting Marseilles to Singapore. Although HMN Tech's bid was much cheaper than an alternative bid from SubCom, threat of crippling sanctions from the US government persuaded the consortium to choose SubCom [57].The governments of the US and other countries also worked to exclude Chinese company HMN Tech from projects such as a Singapore-to-France cable and from a cable connecting Nauru, the Federated States of Micronesia, and Kiribati.

Second, there have been decisions to forgo new undersea cables connecting to or through risky destinations. For example, cable projects have already begun to avoid the South China Sea, which is home to a set of territorial disputes and marine policy conflicts that exacerbate issues related to cable construction, operation, and repair [13]. Chinese authorities have been slow to grant permits for constructing new cables, according to companies involved [58]. Repairing existing cables has also become increasingly difficult as geopolitics intersects with the legal and regulatory structure governing activities in the maritime space. Although cable companies only require permission from a country to fix faults within its 12-mile territorial waters, many companies have started asking for permission to enter countries' 200-mile EEZs due to ongoing tensions, and they often seek permits from multiple countries when there are overlapping claims. Repairs of cables have been delayed by months in some cases because of lags in obtaining permits from China. Repair ships have also faced harassment; in April 2024, a Chinese coast guard vessel confronted and circled a Vietnamese naval vessel repairing a cable within Vietnam's 200-mile exclusive economic zone [59].

In addition to the South China Sea, plans to connect undersea cables to China have also been scrapped. The US government's Clean Network Initiative launched in 2020 aimed to ensure that cables "are not subverted for intelligence gathering by the PRC at hyper scale," essentially prohibiting the connection of any new cables to mainland China or Hong Kong [60,61]. Between 2020 and 2023, the interagency committee known as "Team Telecom" run by the National Security Division of the Department of Justice was instrumental in the cancellation of four undersea cables whose backers had proposed to link the US with Hong Kong [57]. One example was the Pacific Light Cable Network, which would have connected California with Hong Kong, which was blocked due to national security concerns. The committee cited specific issues

related to the Chinese government's efforts to acquire sensitive data, the relationship between the proposed cable's Chinese-based owners and Chinese government intelligence and security services, and dangers related to having an increasing share of US data traversing Chinese territory [24]. Other countries have also made similar decisions. In 2020, Chile announced that its new undersea cable would connect to Sydney via New Zealand instead of terminating in Shanghai, which was widely interpreted as a move to avoid the risks and sensitivities around Chinese technology [62]. As of this writing, no new international cable projects are scheduled to connect to China after 2025 [63].

These trends have led to concerns that undersea cable systems—and the Internet, more broadly—are becoming fragmented and that this fragmentation will grow more pronounced in the future [53,64]. Mobilizing fears about disruption and surveillance has been essential to the push to develop new routes that deviate from preexisting paths [4]. In addition to considering the economic costs and benefits to cables or addressing issues related to the digital divide, governments and companies are increasingly being asked to choose between cable infrastructure provided by the US and its partners versus that provided by China. This fragmentation may be considered necessary to security and resilience by some, but others worry that it may decrease the overall resilience of the cable network infrastructure because cable redundancy is reduced, leaving data limited to traveling through relatively few cables without backup options [29,65]. Resilience will be discussed further in the next section.

These efforts to reshape the physical infrastructure of connectivity in the Indo-Pacific will also interact with the natural life span of these undersea cables in the years to come. Cables are generally designed to have a minimum lifespan of about 25 years [5]. In some cases, they may remain operational longer, but in many cases, they are retired earlier because they become economically obsolete; continuous innovation in cable engineering means that older cables often cannot transmit as much information as newer ones, so they are too expensive to keep in service. Thus, the existing network of cables is path dependent, but older linkages are not permanent. As cables are retired, public and private actors will have the opportunity to make decisions about whether and how to replace them, which could work in tandem with the desire to reshape these networks for geoeconomic purposes.

5. Conceptualizing and bolstering resilience

As awareness of risks to undersea cables has increased, discussions about how to bolster resilience to these risks have become widespread in the Indo-Pacific and beyond. Resilience is a concept that has been examined across many fields, from psychology to business to political science. Recently, resilience has often been considered in the context of economic security, particularly due to concerns about supply chain disruptions due to natural disasters, pandemics, and coercion. Drawing on the research on supply chain resilience [66], this article defines undersea cable network resilience as the ability to mitigate risks and avoid disruptions where possible and to recover quickly from disruptions when necessary.

During the age of empire, ensuring resilience meant routing undersea cables through one's maritime territory or colonial holdings, often through a single company. Later, the nationalization of telecommunications led resilience to be associated with maintaining national control over building, operating, and maintaining undersea cable networks through consortiums of monopoly telecommunications carriers. Now, ensuring resilience is more complicated. International commercial undersea cables are owned by a single company or a consortium of companies (e.g., telecommunication providers, undersea cable companies, content producers, cloud computing service providers) that may be incorporated in different countries, and their cables cross international boundaries to land in two or more sovereign states [67]. When considering how to achieve resilience, contemporary policymakers and companies often focus on providing more connectivity to create redundancy and to mitigate the chance that countries will lose connectivity if a cable is damaged. Although this is important, it is insufficient to effectively bolster undersea cable network resilience for two reasons.

First, a narrow focus on damage to undersea cables ignores the other crucial components of the life cycle of these cables, each of which impacts the overall resilience of the overall cable network. When accounting for the "whole life cycle" of the cable, policymakers must include stages such as investment, construction, licensing, regulation, maintenance, protection, and repair. Cables face distinct risks at each of these stages, which are governed by rules and norms that vary across different marine and terrestrial jurisdictions. Much attention has been given to the investment and construction phases recently, particularly with respect to the involvement of non-trusted suppliers who might compromise security by exploiting their knowledge of cable laying routes or by manipulating security loopholes in equipment. However, more mundane parts of the cable life cycle such as protection and repair are equally important. For example, to avoid or recover from disruption to the network, quick repair is essential. Unfortunately, repair is often complicated by issues related to overlapping international and domestic laws and regulations that can delay access to damaged cables, as discussed previously [13,43]. Restoration of service can also be delayed by shortages of equipment due to supply chain problems and insufficient numbers of cable laying and repair ships [68]. Only around 60 ships operate worldwide to deal with over 600 active and planned cables, and the majority of these vessels are aging [69,70].

There are clear areas for improvement in regulation and enforcement when the whole life cycle of undersea cables is considered. States who are party to the UN Convention on the Law of the Sea (UNCLOS) are obligated to support the laying and protection of cables in their jurisdictions and should respect other states' rights to lay cables. In some cases, regulation or enforcement is inadequate. Domestic regulations only partially address undersea cables, and the international law protecting this infrastructure is weak and, in many cases, outdated [13,71]. The International Cable Protection Committee (ICPC) and others have noted that states are not sufficiently enforcing their existing obligations under UNCLOS, nor are they attentive enough to non-routine man-made risks [72]. Rules and penalties related to tampering and disrupting their operation should be strengthened [73]. For example, with the exception of Vietnam and Thailand, most Southeast Asian states have not adopted national legislation that explicitly criminalizes intentional damage to undersea cables in their internal waters, territorial seas, or archipelagic waters, although there is a legal basis to do so under UNCLOS [13]. There is also a lack of consistent cable protection standards across companies and across countries. For example, in the US, regulations for protection (e.g., restricted access to landing stations and operation centers, physical protections on cables, cybersecurity protocols) are not applied to all cables landing on its territory [67].

In other cases, regulation can be excessive. For example, some states are empowering their domestic authorities to create legislation governing cables (e.g., permit requirements), which interferes with the construction and repair activities of cable companies [74]. In some cases, multiple domestic authorities may have jurisdiction over undersea cables, which can result in confusing or conflicting policies. The involvement of multiple agencies in the review and permitting process also has the potential to make the process complex and potentially disjointed due to lack of coordination or differing institutional mandates spanning marine and terrestrial spaces [67]. Moreover, some studies have pointed out that moves by governments to classify cables as "critical infrastructure" have not necessarily been uniformly positive for improving cable resilience; instead, poorly conceived or non-adaptive critical infrastructure regulations may actually inhibit the ability of actors to respond flexibly to new risks and changing conditions [75].

Second, to fully address resilience, it is necessary to look beyond the undersea cable network to recognize the ways that cables are connected to the broader global telecommunications ecosystem. Fig. 3 illustrates some of the interconnections among the undersea cable network, the

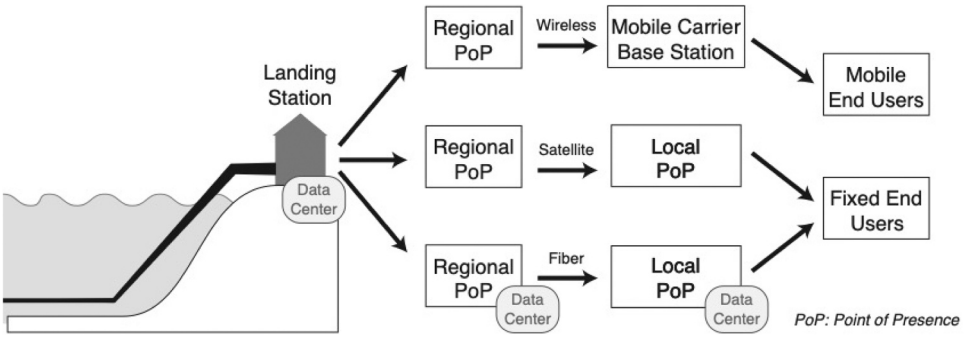


Fig. 3. Undersea cable infrastructure in the telecommunications ecosystem [76].

Internet backhaul, and users. Undersea cables connect with the shore at a landing station that houses the submarine line terminal equipment (SLTE). The line terminal equipment, network protection equipment, and network management equipment connect to a point-of-presence (PoP) and/or data center that directs data to backhaul networks that can be any combination of terrestrial fiber, wireless or mobile carriers, or satellite. These backhaul networks in turn connect to end users using a variety of devices. Since one undersea cable can be connected to multiple landing stations through the use of branching units, similar configurations of networks and equipment emanate from a number of different points, enabling connectivity.

The interconnections depicted in Fig. 3 demonstrate that a much more integrated discussion of resilience is necessary to address all the potential points of vulnerability in the global telecommunications ecosystem across marine, terrestrial, and extraterrestrial spaces. In addition to ensuring the security of the cables on the ocean floor, the protection of landing stations where these cables connect to network equipment is also critical. Governments have an opportunity take the lead on protecting landing stations, which are not subject to the same jurisdictional ambiguities that complicate cables in the water. Moreover, the resilience of the physical infrastructure of cables needs to be considered alongside that of wireless or mobile carriers, data centers, and end user systems as part of the broader cyber domain. Cyberspace has become the fifth domain of political and military dynamics, and cybersecurity is now a routine consideration in economic activity as well as military planning. Cybersecurity is intimately related to the security of undersea cables, and breaches can enable espionage or sabotage. For example, in April 2022, hackers accessed the systems of a private company that had access to the servers of an undersea cable linking Hawaii and the Pacific region [77]. These interconnections between cyber policy and marine policy need to be considered in terms of the whole ecosystem when making policy to mitigate risk and bolster resilience.

Much remains to be done on the policy front. Ensuring the security and resilience of these vital undersea cables requires regional and global partnerships across the public and private sectors, and this cooperation is especially important now as risks and tensions intensify [78]. Aside from constructing additional cables, issues related to maintenance, protection, and repair are also important. To address these challenges, there needs to be greater alignment across the community of stakeholders involved in creating and maintaining the undersea cable network ecosystem. Unfortunately, this alignment is becoming more difficult to achieve due to geopolitics and geoeconomics.

6. Conclusion and overview of the Special Issue

How are threats to undersea cable networks evolving, and why is cable competition intensifying in the Indo-Pacific? How is the policy discourse around undersea cables changing, and what implications do these shifts have for the physical realities of these networks and their resilience? This article has argued that risks to cable networks can be helpfully characterized along the two dimensions of source and frequency. The basic sources of risk for undersea cables have not changed dramatically in recent years—instead, it is the understanding of these risks that has evolved due to the securitization of the maritime and economic domains. The extent to which the new discourse of cable securitization resonates varies across countries and companies, which complicates policymaking. However, geoeconomics and changing understandings of risk are reshaping the physical layout of the Indo-Pacific undersea cable architecture through multiple mechanisms. Ensuring undersea cable network resilience requires a whole life cycle approach that considers not only investment and construction of new cables but also licensing, regulation, maintenance, protection, and repair.

This article provides the foundational framework and analysis for a Special Issue of *Marine Policy* that examines specific aspects of the shifting dynamics around undersea cables from a combination of thematic and geographic approaches. Tsuchiya and Govella explore the historical evolution of these cable networks and how they have been intertwined with geopolitics over time, offering some insights for the contemporary period [10]. Cannon investigates the motivations for Australia, India, Japan, and the US to become jointly involved as the Quad in promoting cable connectivity and resilience in the Indo-Pacific region [45]. Panda looks specifically at India's cable policy, arguing that India is using its multi-aligned "pointed" diplomacy to engage externally with partners to counter China's growing influence [44]. Davenport examines policies addressing the protection of undersea cables from intentional damage in Southeast Asia, mapping the web of legal and policy measures that are in place and highlighting the steps that need to be taken to address crucial gaps [13]. Watson analyzes the diverse and evolving government perspectives on undersea cables among the countries of the Pacific Islands region [30]. Finally, Rossiter looks at how technological advances may be exacerbating risks to cable networks in some ways while offering enhanced options for protection in others, focusing specifically on uncrewed undersea vehicles [22].

This article and the accompanying Special Issue integrate discussions of undersea cables with broader discussions of marine policy, foreign policy, and geopolitics. Together, they demonstrate that undersea cables are far from a narrow, technical concern—in reality, they have concrete, significant impacts on the economic prosperity and security of individual countries and the international system more broadly. These cable networks are in turn being impacted by changing discourses around geoeconomics, which are remapping the physical realities of this critical infrastructure. Understanding these undersea cables, the risks they face, and the steps that are necessary to enhance their resilience requires an interdisciplinary lens that integrates science, engineering, economics, politics, security, law, and other fields—and it also requires dialogue that bridges the divides among government, academia, and the private sector. A more holistic appreciation of the role of these cables in the broader telecommunications ecosystem will help to inform more effective scholarship and policy.

Acknowledgements

This article draws on ideas initially discussed at a workshop on "Undersea Cables, Geoeconomics, and Security in the Indo-Pacific: Risks and Resilience" that was convened at the University of Hawai'i at Mānoa on October 26–27, 2023 with the support of a grant from the Japan Foundation.

References

[1] C. Bueger, T. Liebetrau, Critical maritime infrastructure protection: what's the trouble? Mar. Policy 155 (2023) 105772.
[2] J. Gallagher, Undersea Telecommunication Cables: Technology Overview and Issues for Congress, Congressional Research Service, Washington, DC, 2022.
[3] Detecon Asia-Pacific Ltd, Economic Impact of Submarine Cable Disruptions, Asia-Pacific Economic Cooperation, 2012.
[4] N. Starosielski. The Undersea Network, Duke University Press, Durham, 2015.
[5] Telegeography, Submarine Cable 101, Telegeography, 2025. ⟨https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions⟩ (Accessed 11 June 2025).
[6] E. Rosenbach, K. Mansted, The Geopolitics of Information, Belfer Center for Science and International Affairs, Cambridge, MA, 2019.
[7] M. Goodman, M. Wayland, Securing Asia's Subsea Network: US Interests and Strategic Options, Center for Strategic and International Studies, Washington, DC, 2022.
[8] C. Kavanagh, Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour, United Nations Institute for Disarmament Research, Geneva, 2023.
[9] Telegeography, Submarine Cable Map, 2025. ⟨https://www.submarinecablemap.com⟩ (Accessed 11 June 2025).
[10] M. Tsuchiya, K. Govella, Undersea Cables and the Extension of Empire: The Rise of Britain, Japan, and the United States and the Competition to Connect Hawai'i, Marine Policy TBD, 2025. [Article in progress].
[11] European Subsea Cables Association, Baltic Sea Cable Faults, 2024. ⟨https://www.escaeu.org/news/?newsid=119⟩ (Accessed 11 June 2025)
[12] W. Burns, Spycraft and statecraft: transforming the CIA for an age of competition, Foreign Aff. 103 (2024) 74–85.
[13] T. Davenport, The protection of submarine cables in Southeast Asia: the security gap and challenges and opportunities for regional cooperation, Mar. Policy 171 (2025) 1–10.
[14] E. Braw, China is Practicing How to Sever Taiwan's Internet, Foreign Policy, 2023. ⟨https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/?fbclid=IwAR35zAN3VIwQOZRdQ6WaZwtPgvynsJsUeo0iDHOpjBE76FqU1CBVyGwbTXs⟩ (Accessed 11 June 2025).
[15] B. Perratt, Applying lessons from telecoms cable outages to the power cable industry, PES Wind (2023) 1–5.
[16] W. Qi, Submarine Cables Cut after Magnitude-9.0 Earthquake and Tsunami in Japan, Submarine Cable Networks, 2011.
[17] T. Bateman, Tonga is finally back online. Here's why it took 5 weeks to fix its volcano-damaged Internet cable, Euronews.Next, 2022. ⟨https://www.euronews.com/next/2022/02/23/tonga-is-finally-back-online-here-s-why-it-took-5-weeks-to-fix-its-volcano-damaged-interne⟩ (Accessed 11 June 2025).
[18] P. Lipscombe, Tonga's Domestic Submarine Cable Fixed 18 Months after Volcanic Eruption, Data Center Dynamics, 2023. ⟨https://www.datacenterdynamics.com/en/news/tongas-domestic-submarine-cable-fixed-18-months-on-from-volcanic-eruption/⟩ (Accessed 11 June 2025).
[19] H. McGeachy, The changing strategic significance of submarine cables: old technology, new concerns, Aust. J. Int. Aff. 76 (2022) 161–177.
[20] M. Matis, The Protection of Undersea Cables: A Global Security Threat, US Army War College, Carlisle, PA, 2012.
[21] R. Martinage, Under the sea: the vulnerability of the commons, Foreign Policy 94 (2015) 117–126.
[22] A. Rossiter, Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs), Mar. Policy 171 (2025) 1–6.
[23] E. Bruton, The cable wars: military and state surveillance of the british telegraph cable network during world war one, in: A. Marklund, M. Ruediger (Eds.), Historicizing Infrastructure, Aalborg University Press, Aalborg, Denmark, 2017, pp. 1–24.
[24] United States Department of Justice, Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States, 2020. ⟨https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea⟩ (Accessed 11 June 2025).
[25] Y. Koshino, The Changing Submarine Cables Landscape: Expanding the EU's Role in the Indo-Pacific, European Institute for Security Studies, Paris, 2024.
[26] J. Sherman, Cybersecurity under the Ocean: Submarine Cables and US National Security, Hoover Institution, Stanford, 2023.
[27] L. Munn, Technical Territories: Data, Subjects, and Spaces in Infrastructural Asia, University of Michigan Press, Ann Arbor, 2023.
[28] B. Buzan, O. Wæver, J. de Wilde, Security: A New Framework for Analysis, Lynne Rienner, Boulder, CO, 1998.
[29] E. Noor, Entangled: Southeast Asia and the Geopolitics of Undersea Cables, Indo-Pac. Outlook 1 (2024).
[30] A.H.A. Watson, Undersea Cables, The Official Perspectives Expressed in the Pacific Region, Mar. Policy 178 (2025) 1–8.
[31] C. Bueger, Maritime security in the age of infrastructure, in: P. Leucci, I. Vianello (Eds.), AscoMare Yearbook on the Law of the Sea: Maritime Security, New Technology and Ethics: Evolving Challenges and Opportunities, Luglio Editore, Trieste, 2023, pp. 73–88.
[32] A. Dell'Era, Securitizing Beijing through the maritime commons: the 'China threat' and Japan's security discourse in the Abe era, Pac. Rev. 37 (2024) 147–180.
[33] K. Govella, China's challenge to the global commons: compliance, contestation, and subversion in the maritime and cyber domains, Int. Relat. 35 (2021) 446–468.
[34] R. Blackwill, J. Harris, War by Other Means: Geoeconomics and Statecraft, Harvard University Press, Cambridge, MA, 2016.
[35] D. Baldwin, Economic Statecraft, Princeton, University Press, Princeton, 1985.
[36] S. Kurt, Economic security: increasing impact of economic factors on international security, in: A. Özkan, G. Tüysüzoğlu (Eds.), Security Studies: Classic to Post-Modern Approaches, Lexington Books, Lanham, MD, 2023, pp. 91–114.
[37] H. Farrell, A. Newman, Weaponized interdependence: how global economic networks shape state coercion, Int. Secur. 44 (2019) 42–70.
[38] H. Shen, Building a digital silk road? Situating the internet in China's belt and road initiative, Int. J. Commun. 12 (2018) 2683–2701.
[39] S. Lee, The Cybersecurity Implications of Chinese Undersea Cable Investment, Henry M. Jackson School of International Studies, University of Washington, 2017. ⟨https://jsis.washington.edu/news/cybersecurity-implications-chinese-undersea-cable-investment/⟩ (Accessed 11 June 2025).
[40] J. Sherman, Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security, Atlantic Council, Washington, DC, 2021.
[41] K.F. Rauscher, ROGUCCI Study Final Report, IEEE Communications Society, 2010.
[42] M. Kajiwara, Maritime security and underwater surveillance technology: lessons from the cold war, Indo-Pac. Outlook 1 (2024) 1–9.
[43] J. Sherman, Improving Indo-Pacific cable security and resilience: investment, licensingg, and repair, Indo-Pac. Outlook (1) (2024).
[44] J. Panda, India's emerging undersea cable landscape: varied indo-Pacific partnerships to boost geopolitical ambitions? Mar. Policy 171 (2025) 1–10.
[45] B. Cannon, Undersea cable security in the Indo-Pacific: enhancing the quad's collaborative approach, Mar. Policy 171 (2025) 1–6.
[46] H. Channer, Improving public-private partnerships on undersea cables: lessons from Australia and its partners in the Indo-Pacific, Indo-Pac. Outlook (1) (2024).
[47] C. Mims, Google, Amazon, meta and microsoft weave a fiber-optic web of power, Wall Street J., 2022.
[48] Interviews with Cable Industry Industry Representatives, 27 October, 2023.
[49] L. Gjesvik, Private infrastructure in weaponized interdependence, Rev. Int. Political Econ. 30 (2023) 722–746.
[50] S. Kuszynski, The Geopolitics of Undersea Cables: Underappreciated and Under Threat, London Politica, London, 2019.
[51] N. Schadlow, B. Helwig, Protecting Undersea Cables Must be Made a National Security Priority, DefenseNews, 2020.
[52] S. Patil, P. Gupta, The Digital Silk Road in the Indo-Pacific: Mapping China's Vision for Global Tech Expansion, Observer Research Foundation, New Delhi, 2024.
[53] A. Beattie, Can Globalisation Survive the US-China Rift, The Financial Times, 2024.
[54] Prime Minister of Australia, Joint statement from the leaders of Australia, India, Japan, and the United States, 2024. ⟨https://www.pm.gov.au/media/joint-statement-leaders-australia-india-japan-and-united-states⟩ (Accessed 11 June 2025).
[55] C. Morel, The Pacific Caught in the World Wide Web? Geopolitics of Submarine Cables in Oceania, French Institute of International Relations, Paris, 2022.
[56] White House, Quad Leaders' Summit Fact Sheet, 2023. ⟨https://web.archive.org/web/20250116064633/https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/⟩ (Accessed 11 June 2025).
[57] J. Brock, US and China Wage War Beneath the Waves - Over Internet Cables, Reuters, 2023.
[58] T. Suruga, Asia's Internet Cable Projects Delayed by South China Sea Tensions, Nikkei Asia, 2023.
[59] R. Tan. Escalating Contest over South China Sea Disrupts International Cable System, The Washington Post, 2024.
[60] US Embassy and Consulates in Brazil, Fact Sheet: The Clean Network Safeguards America's Assets, 2020. ⟨https://br.usembassy.gov/the-clean-network-safeguards-americas-assets/⟩ (Accessed 11 June 2025).
[61] J. Zhang, Heading in the direction of bifucated networks: Hong Kong's evolution amidst the global submarine cable system, Asian Rev. Political Econ. 3 (2024) 1–24.
[62] Y. Hirose, N. Toyama, Chile Picks Japan's Trans-Pacific Cable Route in Snub to China, The Financial Times, 2020.
[63] K. Takeda, M. Ban, More subsea cables bypass China as Sino-US tensions grow, Nikkei Asia, 2024.
[64] D. Woods, J. Li, Dangerous depths of bifurcation: the rise of "international security narcissists" and undersea cable (dis) connections, Asian Secur. 20 (2024) 106–128.
[65] J.-M. Desurmont, Territorial Claims and Subsea Cables: The Geopolitics of Invisible Lines in the South China Sea, Bloomsbury Intelligence and Security Institute, 2024. ⟨https://bisi.org.uk/reports/territorial-claims-and-subsea-cables-the-geopolitics-of-invisible-lines-in-the-south-china-sea⟩ (Accessed 11 June 2025).
[66] B. Tukamuhabwa, M. Stevenson, J. Busby, M. Zorzini, Supply chain resilience: definition, review, and theoretical foundations for further study, Int. J. Prod. Res. 53 (2015) 5592–5623.
[67] Congressional Research Service, Protection of Undersea Telecommunication Cables: Issues for Congress, Congressional Research Service, Washington, DC, 2023.

[68] J. Tan, Securing the Backbone: Security Challenges to and Governance of Submarine Cables in the Indo-Pacific, Melbourne Asia Review 2024, 2024. ⟨https://www.melbourneasiareview.edu.au/securing-the-backbone-security-challenges-to-and-governance-of-submarine-cables-in-the-indo-pacific/⟩ (Accessed 11 June 2025).
[69] International Cable Protection Committee, Cableships of the World, 2025. ⟨https://www.iscpc.org/information/cableships-of-the-world/⟩ (Accessed 11 June 2025).
[70] D. Swinhoe, The cable ship capacity crunch, 2022. ⟨https://www.datacenterdynamics.com/en/analysis/the-cable-ship-capacity-crunch/⟩ (Accessed 11 June 2025).
[71] T. Davenport, The high seas freedom to lay submarine cables and the protection of the marine environment: challenges in high seas governance, AJIL Unbound 112 (2018) 139–143.
[72] Centre for International Law, National University of Singapore and International Cable Protection Committee, Co-Chairs' Provisional Report, Workshop on the Protection of Submarine Cables, National University of Singapore, Singapore, 2011. ⟨https://cil.nus.edu.sg/wp-content/uploads/2011/02/Workshop_Report_21_April_2011.pdf⟩ (Accessed 11 June 2025)
[73] J. Kraska, Submarine Cables in the Law of Naval Warfare, Lawfare, 2020. ⟨https://www.lawfaremedia.org/article/submarine-cables-law-naval-warfare⟩.
[74] U.K. Raha, K.D. Raju, Submarine Cables Protection and Regulations: A Comparative Analysis and Model Framework, Springer, Singapore, 2021.
[75] C. Kavanagh, Cyber Stability Conference: Protecting Critical Infrastructure and Services Across Sectors, United Nations Institute for Disarmament Research, Geneva, 2022.
[76] L. Gordon, K. Jones, Global Communications Infrastructure: Undersea and Beyond, Center for Space Policy and Strategy, The Aerospace Corporation, 2022.
[77] D. Temple-Raston, S. Powers, Who tried to hack Hawaii's undersea cable?. The Record, 2022. ⟨https://therecord.media/who-tried-to-hack-hawaiis-undersea-cable⟩ (Accessed 11 June 2025).
[78] K. Govella, Strengthening Economic Resilience and Security through US-Japan Cooperation on Undersea Cables, The Japan Forum on International Relations, 2025. ⟨https://www.jfir.or.jp/en/studygroup_article/4628/⟩ (Accessed 11 June 2025).

Kristi Govella[1]
Nissan Institute of Japanese Studies, Oxford School of Global and Area Studies, University of Oxford, Oxford, United Kingdom
E-mail address: kristi.govella@nissan.ox.ac.uk.

[1] ORCID: 0000-0002-0579-0748