Policy Brief
January 25, 2024

The Quad and Submarine Cable Protection in the Indo-Pacific: Policy Recommendations

Brendon J. Cannon and Pooja Bhatt

Photo credit: Korn Sriwawan / Shutterstock

This policy brief analyzes the Quadrilateral Security Dialogue (Quad) initiative on submarine cables in the Indo-Pacific and offers a timely roadmap as to how best to protect them. It first locates the significance of submarine cables for global connectivity and security, and then contextualizes the perception of threats to cables from malicious state or state-supported actors at a time of rising global tensions. Because of the unique challenges posed by cable vulnerabilities, to include sabotage and espionage, the brief focuses on the impact of disruptions within the evolving geopolitical landscape as well as their recent securitization and provides actionable rather than aspirational recommendations for the Quad. These include leasing cable repair ships, prioritizing existing subsea cable arrangements and collaborating with local operators to meet specific regional needs, and for the Quad to focus on achievable, collective maritime security initiatives rather than the pursuit of complex technology sharing at this stage. The aim is to recommend near-term, reachable goals that can demonstrate cooperation without straining the sensitive dynamics between Quad members, other stakeholders, and like-minded states. In doing so, the policy brief contributes to the existing literature on the Quad's effectiveness, structure, and deterrent value.

Introduction

This policy brief reviews the aims, nature, and scope of the Quad's response to the protection of submarine communication cables in the Indo-Pacific. It suggests practical policy prescriptions for the quartet's members—Australia, India, Japan, and the U.S.—to engender cooperation despite a range of differences, strategic ambits, and structural and systemic limitations within and between individual states.

Enhancing the protection of submarine communication cables (variously known as subsea, subsurface, and undersea cables) is an emerging area of concern for states. Submarine cables lie several hundred meters under the seas and serve as crucial conduits for internet lines as well as oil and gas pipelines across continents. As digital connectivity and energy transportation are growing, several countries are opting for and relying on undersea infrastructure for their development. However, recent inci-

dents, including that involving the Chinese *Newnew Polar Bear* vessel, indicate that the damage to these cables, inadvertent or otherwise, can disrupt sensitive communications and economies for several days, if not weeks. Disruptions can be exacerbated depending on the capabilities available to certain states to protect this critical infrastructure. The repair of cables is both expensive and technical and involves a degree of expertise and the presence of specialized vessels in the high seas. Recognizing the nature of the problem and the growing threats to submarine cables within the context of rising global tensions, the Quad—Australia, India, Japan, and the U.S.—established a framework for cooperation on the protection of cables in the Indo-Pacific.

The policy brief offers timely analysis and grapples with very real and prescient opportunities and challenges associated with the 'Quad Partnership for Cable Connectivity and Resilience.' It identifies what the Quad can realistically, collectively achieve, given its members' different geographies, capabilities, legal and regulatory regimes, and perception of threats. It offers policy prescriptions and courses of actions that are both possible and advisable, and highlights others that are likely inadvisable given a range of unintended consequences. In doing so, our brief on the Quad and the protection of submarine cables adds to and refines existing literature related to the quartet's efficacy as a security grouping, its cohesiveness, its deterrent value, and its future trajectory in the Indo-Pacific.

"What has been largely the domain of private cable manufacturers and operators that supply our increasing demand for communication and information has become an object to be securitized, protected, and overseen by government ministries, regulations, and complex licensing and legal regimes.

Relevance of Submarine Cables in National Security Debate

Thin as a garden hose, there are approximately 500 operational submarine cables worldwide comprising 200 interconnected systems, extending over a million kilometers, and continually expanding. Whenever we read an email, share a video on social media, or search the internet, the information travels through these submarine fiber optic cables. So do daily online financial transactions that amount to more than $10 trillion through the SWIFT system, as well as many states' most sensitive secrets.

Despite their crucial role in supporting the global economy and our everyday activities, cables have remained "under the surface" and "out of sight" until recently. But a combination of great power competition, securitization, and an uptick in what appears to be malicious cable sabotage has led to drastic changes. In May 2023, the Quad, in an age of heightened geopolitical competition with China, announced an initiative to protect submarine communication cables, which they see as a new and dangerous undersea battleground with China.

What has been largely the domain of private cable manufacturers and operators that supply our increasing demand for communication and information has become an object to be securitized, protected, and overseen by government ministries, regulations, and complex licensing and legal regimes. This is by no means a storm in a teacup. Nevertheless, on certain levels, it seems that the alarmist rhetoric issued by policymakers, think tanks, and governments may have outpaced the reality of the threats to and vulnerabilities of submarine communication cables.

Range of Vulnerabilities

Since submarine cables are intrinsic to our financial transactions and communications, when they go down—regardless of the cause—downtime is measured in seconds. Submarine cables face a variety of unique challenges that are proliferating with time. These include natural hazards like sharks and earthquakes, and accidental damage that comes from ship anchors. Not surprisingly, instances of damage to submarine cables are relatively common, with an estimated 100 to 150 cables being severed each year, mostly from fishing equipment or anchors.[1]

The network is designed with a certain level of redundancy to handle such damage. Most countries are interconnected by numerous fiber-optic cables, allowing data to be rerouted seamlessly in the event of one or two cables being compromised. However, when more severe damage occurs, it can lead to significant inconveniences and financial losses, and repairing damaged cables is complex and costly, often resulting in days or weeks of downtime. The vast distances and isolation of the cable network make damage prevention and repair efforts daunting. While routine faults caused by hazards typically result in limited disruptions for advanced economies, developing economies with limited cable capacity face more severe consequences from accidental damage.[2]

The vulnerability of submarine cables also makes them theoretically vulnerable to attacks. Cables are often concentrated near each other, driven by cost considerations, and finding suitable landing sites. This is particularly true of "pressure points," or the concentration of the cable landings. A malicious actor could potentially damage or destroy several cables at the same time thus rendering rerouting more difficult or impossible.[3] Current satellite technology is insufficient to meet the communication needs of advanced states' digital economies and societies.

The narrative gaining traction since the *Nord Stream* pipeline sabotage in late September 2022 is that geopolitical rivals increasingly seek to exploit the importance and vulnerability of submarine cables to gain advantages over one another.[4] Russia certainly thinks so when former Russian Prime Minister Dmitry Medvedev stated there was no reason Moscow should not destroy its enemies' submarine cables.[5] Yet, the list of ostensible submarine cable attacks is still rather thin, albeit growing. In February 2023, for instance, cables were cut between Taiwan and the Taiwan-controlled Matsu Islands that lie just off the coast of China. While Taipei refrained from accusing China of severing the cables, the fact remains that the cables have been cut 27 times since 2018, as of mid-2023.[6] The only documented case of a cyber assault on submarine cables took place in April 2022 when the U.S. government disclosed its successful prevention of an attack on a submarine cable connecting Hawaii and the Pacific Region.[7] In early October 2023, a Chinese-owned ship *Newnew Polar Bear* reportedly dragged its anchor over 100 nautical miles across the Gulf of Finland and hit gas lines and submarine cables.[8] While malicious sabotage seems more likely than gross negligence, this incident highlights both the vulnerabilities of submarine cables and the difficulty of pinning blame on a specific actor or accurately identifying whether the incident was an accident or sabotage.

Securitization and Responses

In late November 2023 and in response to what London viewed as increasing attacks on submarine cables, the UK announced it would send seven naval vessels and a maritime patrol aircraft to take part in Joint Expeditionary Force (JEF)[9] patrols of areas with vulnerable submarine infrastructure.[10] A few months earlier, the Quad announced its Quad Partnership for Cable Connectivity and Resilience at the G7 Summit in Hiroshima in May 2023. It aims to bring together public and private sector actors to address gaps in the infrastructure and coordinate future cable routing, building, and operations.

The deployment of naval assets and the Quad's submarine cable partnership highlights the growing securitization of submarine cables. Securitization,

in brief, occurs when actors transform issues or objects into security threats through 'speech acts.' International Relations (IR) theory thus emphasizes the social construction of security concerns and the role of elite actors in framing certain issues or objects (like submarine cables) as requiring extraordinary security measures for protection. From the lens of securitization theory then—given the relative paucity of confirmed malicious attacks on cables—the measures taken by the UK and the Quad signify not so much the recognition of increased threats, but the perception of them. They also are part of a wider effort by governments to forecast the future and act proactively. It is the speech acts—the announcements of naval redeployments or policies—that securitize submarine cables. Yet now that the proverbial horse has left the barn, we need answers to questions like: What, after all, is the Quad? What does the Quad partnership actually mean for submarine cable protection? And what has been done thus far?

To answer the first question, the Quad is an informal intergovernmental organization, according to international relations and international organizations parlance. It is chiefly a mechanism of dialogue for self-described "like-minded countries;" it is formalized only in that meetings occur regularly, albeit with no set plans, few announcements, or locations. It is, therefore, not an alliance. Since its inception in 2007 and its recreation in 2017, the Quad has shown staying power and that it can act together when interests converge. Privileging an informal, club-like model means the Quad emphasizes areas of converging interests and downplays points of tension and disagreement. Such congeniality and avoidance of hard issues creates an impression of amity and sends strong signals to China that Australia, India, Japan, and the U.S. are up to something. This "something" has involved quadrilateral efforts aimed at addressing the COVID-19 pandemic, maritime domain awareness and, most recently, submarine cables.[11]

In terms of the Quad's cable protection initiative,

> ***"Cables are often concentrated near each other, driven by cost considerations, and finding suitable landing sites. This is particularly true of "pressure points," or the concentration of the cable landings. A malicious actor could potentially damage or destroy several cables at the same time thus rendering re-routing more difficult or impossible.***

Australia took the lead and established the new Indo-Pacific Cable Connectivity and Resilience Program in 2023. It did so simply because it was the host of the Quad leaders' summit last year.[12] This program will reportedly share best practices and provide technical assistance to Indo-Pacific governments. To that end, Australia tasked a small team at its Department of Foreign Affairs and Trade (DFAT), which reportedly sent delegations to India and Vietnam and consulted with Australia's embassies to coordinate future policies such as investing in submarine cable programs.[13] For its part, the U.S. is to provide technical assistance and capacity building on the security of submarine cable systems through its US$ 5 million CABLES program.

The Quad is once again seeking to leverage each member's unique capabilities and geographies. They aim to combine their expertise in designing, producing, installing, and maintaining secure submarine cable systems, ultimately enhancing internet connectivity, and bolstering regional resilience. The Quad's initiatives align with trilateral investments (US$ 95 million) from Australia, Japan, and the U.S. in submarine cable projects. For instance, a

new 2,250-kilometer subsea fiber-optic cable connecting Micronesia, Nauru, and Kiribati aims to improve internet access and counter potential Chinese influence. Japan's NEC Corp, a leading submarine cable vendor, will play a key role. These actions echo the Quad's commitment, as expressed by American officials, to support a free, open, and secure internet. The U.S. State Department emphasizes the importance of prioritizing security and privacy by excluding "unreliable suppliers" from various network components, including submarine cables.

U.S. efforts to hinder various Chinese submarine cable projects have also included, since 2019, tactics like providing millions of dollars in training grants to foreign telecom firms to disinvite Chinese cable companies from bidding processes.[14] Washington has also pressured American companies such as Google and Meta by withholding licenses for proposed private subsea cables that transited Hong Kong, which is Chinese sovereign territory.[15] The sum of these parts is the U.S.' Clean Network initiative that bans new cables directly connecting the U.S. to China or Hong Kong.[16] This has led to the rise of consortiums like Apricot, Bifrost, and Echo that push alternative cable routes through Singapore, Indonesia, the Philippines, and Guam, which is becoming a central hub for global data traffic.

The trilateral and unilateral moves within the Quad are telling. The submarine cable expertise and manufacturing rests squarely in Japan and the U.S. Australia, for its part, offers its strategic geography and links to Pacific Island states, which have found themselves the object of increased attention by Washington and Canberra as well as Beijing. These efforts that occur below the level of the Quad also shed light on what steps the four members can take collectively to protect submarine cables.

Policy Recommendations

We propose the following actionable policy prescriptions for the Quad. In doing so, we distinguish between the advisable and potentially inadvisable, i.e., *do this, not that*. These are meant to be purposely provocative and engender a lively debate within policy and academic circles to develop best practices for submarine cable protection. The analysis and below policy recommendations also contribute to the literature related to the Quad's effectiveness as an informal security organization, the chances for unity in a crisis, and ultimately its deterrent value within the context of great power competition and the prospect of Chinese hegemony in Asia.

Lease cable repair ships

The Quad members can collectively pool resources to lease cable repair ships in collaboration with industry. Cable repair ships play a vital role in submarine cable maintenance, using advanced tools like ROVs to locate and retrieve faults. They conduct repairs, install protective measures, perform routine inspections, deploy submersibles for deep-sea tasks, coordinate with cable stakeholders, and play a crucial role in emergency responses. These efforts contribute to the reliability of global communication networks. Currently, a consortium of owners and investors have contracted repair services to private third-party companies. These have the ships, staff, and resources to make repairs. Yet, there are only about 60 cable repair ships in service, either installing a new cable or repairing a cable.[17] The Quad can begin to lease ships like that leased by NEC Japan in 2022 when it signed a charter contract with UK-based Global Marine Systems Limited for an optical submarine cable-laying ship for approximately four years.[18]

Work with local operators and industry

Quad-inspired initiatives—unilateral, bilateral, trilateral, or quadrilateral—should prioritize existing subsea cable arrangements and address local needs. By working with local operators and industry, the smaller actors in the cable industry and the interests of local populations in small island states, for example, can better be addressed. When Google announced it would build a submarine cable to at least eight Pacific Island states under a joint U.S.-Australian deal, it was both welcomed and problematic.[19] The project should expand an

existing commercial project by Google in the region to the nations of Micronesia, Kiribati, the Marshall Islands, Papua New Guinea, the Solomon Islands, Timor-Leste, Tuvalu, and Vanuatu, but it has also caused headaches for local industry and interests, some of which had worked hard to find funding and support for certain cable routes stretching between two or more island states.

If this is the case, then Quad states need to work on ensuring redundancy but understand that these cables may be used by belligerents via neutral parties in the event of conflict. So, what's to be done? Perhaps look at space and the robust space capabilities of Japan, India, and the U.S. and the development of communication satellite infrastructure that can be used in the event of cable rupture.

Work with (and join) ICPC

The International Cable Protection Committee (ICPC) is an organization that promotes the safeguarding of submarine cables and facilitates collaboration among industry stakeholders, governments, and telecommunications companies to prevent damage to and enhance the reliability of submarine communication infrastructure. While Japan, Australia, and the U.S. are well-represented at the ICPC, India is currently only represented by Tata Communications Ltd. Australia's Department of Home Affairs and the U.S. Navy also have official representation in the ICPC.

> ***"The deployment of naval assets and the Quad's submarine cable partnership highlights the growing securitization of submarine cables. From the lens of securitization theory then—given the relative paucity of confirmed malicious attacks on cables—the measures taken by the UK and the Quad signify not so much the recognition of increased threats, but the perception of them.***

Our policy prescription is that ministries and industry partners from the four Quad member-states should be encouraged to join the ICPC. For example, greater Indian participation, as a rising great power, could play a vital political role given its history of non-aligned leadership, its status in the Global South, and its consistent approach to building inclusivity in multilateral fora.

Utilizing ICPC as a forum to address submarine cable resilience and security makes sense for three reasons. *First*, ICPC's role will be enhanced and provide a currently apolitical forum for discussions about best practices to avoid potential disruptions or malicious interference as well as matters such as addressing licensing delays. *Second*, participation in ICPC may further what has been a businesslike attitude towards cable building, repair, and maintenance. It could therefore provide the architecture for international standards and practices, setting expectations for secure and cooperative management of critical communication infrastructure. *Third*, industry representatives from Hong Kong and China are already members of ICPC as are those from a host of other states (but not Russia). ICPC can provide for exchanges and engagement that may help to prevent fragmentation in submarine cable governance.

Update (and join) UNCLOS

Quad states could work with other like-minded partners to update UNCLOS to clarify the legal regime and obligations of states. Article 113 of

UNCLOS requires that every State party to the convention enact domestic legislation making the willful or negligent "breaking or injury" of a submarine cable a punishable offense. As Green and Burnett advised: UNCLOS provisions regarding the freedom to operate, maintain, and repair international cables outside of territorial seas must be adhered to by all states.[20] To do this effectively, however, the U.S. must become a signatory, and this will be easier said than done.

Make submarine cables a global common

Compared to the U.S. and Australia, states like India and Japan can more effectively mobilize support in the "Global South" for something like a "Protect Our Cables" campaign. Such a campaign would attempt to make cables a global common akin to the oceans themselves. This normative angle could develop basic ground rules that mirror some of Japan's new "free and open Indo-Pacific" or FOIP.[21] In essence, the message would be: "Malicious cable attacks harm us all."

Countering espionage

With increasing tensions between rivals in the Indo-Pacific, the threat of espionage through cables remains a clear danger to national security. Submarine cables are vulnerable to communication interception. Tapping into cables could allow unauthorized access to sensitive communications, including government and military communications within the Quad countries. Espionage activities may also extend beyond physical cable tapping to cyber operations targeting the data transmitted through the cables. Cyberattacks could compromise the security of communication systems and networks.

Justin Sherman noted that the tussle over submarine communication cables is about China or the U.S. gaining espionage advantage over the other.[22] Private firms overseeing Internet infrastructure play a role in state espionage, with greater concerns when the overseeing entity is state-controlled. This is especially evident in countries like China, where authoritarian surveillance practices, distinct from those in the U.S., increase the likelihood of Beijing exploiting influence over submarine cable infrastructure for espionage purposes. Indeed, a recent report outlined the growing role of Chinese state-owned enterprises as cable owners and providers, which is "increasing China's ability to manipulate, surveil and interfere with worldwide data flows." [23]

Given the threat of espionage, which seems much more pronounced than the more lurid threat of submarines snipping cables on the ocean floor, Quad governments should encrypt their communications to mitigate this threat. This is already being done in the case of the U.S. and Australia and their FVEYs intelligence sharing framework, but this is less obvious in the cases of India and Japan. Pooling resources or, less sensitive, sharing basic "best practices" in cybersecurity policy, operations, and encryption may be a critical first step with an understanding that work on counter espionage will move forward on the unilateral or bilateral front (U.S.-Australia) rather than quadrilaterally.

Quad Maritime Security Efforts and Cable Protection: A Non-Starter

A recent report advised the Quad to pursue a collective maritime security strategy across five high-priority areas: *maritime domain awareness; anti-submarine warfare; maritime logistics; defense industrial and technological cooperation*; *and maritime capacity building*.[24] The authors offered compelling reasons to do so, and on the surface, both the policy recommendations and linking these with the Quad's submarine cable initiative make sense.

We advise against pursuing these initiatives at this stage, however, for the simple logic that they are entirely aspirational and out of reach for the Quad as it is currently constituted. As noted, the Quad is purposely designed to be highly informal. It is the only workable format for India and the U.S. to work together at present. Intelligence sharing and defense industrial and tech cooperation on a limited basis are possible, but these can only be purposively pursued at the bilateral level—the

U.S. and Australia, for example, or relatedly as Australia-UK-U.S. (AUKUS). Cable protection is no different. Developing the capabilities of cutting edge underwater autonomous vehicles (UAVs) to protect submarine cables on even a rudimentary basis is chockful of sensitive national security-related technology and secrets. Sharing the eventual "security umbrella" offered by such technologies may be possible as the U.S. underwater surveillance systems did for Japan during the Cold War, but the technologies will not be shared.

Our policy recommendation is, therefore, that the Quad focuses on what is achievable and has the most impact today vis-à-vis cable protection rather than attempting to implement technology sharing and research and development in sensitive arenas prior to the evolution of the Quad into something resembling a theoretical military alliance. This is an unlikely eventuality at this point and rests entirely on the level of threat perceived by each member-state from China. In short, the Quad's efficacy to each member is directly inverse to the China threat.

Fund cables and expand U.S.-led cable initiative

The U.S. has employed various tactics since 2019, as noted, including financial incentives and pressure on American companies like Google and Meta to obstruct Chinese involvement in submarine cable projects under the Clean Network initiative. This bars direct connections between the U.S., China, or Hong Kong and has prompted the creation of alternative cable consortiums. This seems to have been quite successful and reports that China is building a separate "Chinese" cable network appear exaggerated at this point. The reality is that the majority of data flowing across the world's cables occurs on non-Chinese cables. American, French, and Japanese dominance in cable supply and installation makes it challenging for China to establish its network.[25]

Any Quad actions that bolster Washington's Clean Network initiative may further diminish the likelihood of a distinct Chinese cable network in the future. Yet in doing so, the Quad may create trouble of its own making. As the aforementioned instance of Google announcing a new subsea cable in the Pacific between small island states shows, private operators and local interests may take a beating. As such, we recommend that the Quad prioritize feasibility studies where new cable work has been planned so as to engage with local companies and reflect the interests and priorities of Pacific Island states, for example. Entities like Google that plan to build new cable networks could also subcontract work to local entities.

> ***"Quad-inspired initiatives—unilateral, bilateral, trilateral, or quadrilateral—should prioritize existing subsea cable arrangements and address local needs. By working with local operators and industry, the smaller actors in the cable industry and the interests of local populations in small island states, for example, can better be addressed.***

Stop securitizing rhetoric

The securitization of cables is a two-edged sword. On the one hand, it does seem that there is a slight rise in malicious cable attacks by state actors (or state-supported actors). On the other hand, the rhetoric seems to have outpaced the reality. Malicious attacks against cables have not been well-cataloged. This is partly because they have been few and far between, and partly because interest in cables has only recently grown across the globe. This may be a chicken and egg scenario in that we can no longer decide which came first: malicious attacks

against cables or the speech acts that securitize cables. Nevertheless, the results of securitizing what has been a robust industry largely in private hands (outside China) may have more negative than positive consequences.

In addition, the ongoing securitization of cables by the Quad, academia, and policymakers is spreading to third countries such as Indonesia that see both an opportunity and a threat in terms of protecting cables.[26] In another case, cables are increasingly being designated as the property of states. What were previously cables laid by a private company, NEC Japan, and managed by a host of telecommunication firms may now be seen as more tempting "Japanese" targets by competitor states.

For this reason, while we applaud the Quad's Undersea Cable initiative for the deterrence that may come from being proactive and demonstrating its members' collective, written resolve to protect submarine cables, we also assess that such a move unnecessarily calls attention to cables for adversaries as objects to be attacked. This is not to say that the announcement in Hiroshima in May 2023 led Beijing to see an opportunity they had not thought of before. No, instead the Quad has announced a resolve to act and commit resources to protect cables in a manner that may be nigh impossible to fulfil.

While we applaud the Quad's Undersea Cable initiative for the deterrence that may come from being proactive and demonstrating its members' collective, written resolve to protect submarine cables, we also assess that such a move unnecessarily calls attention to cables for adversaries as objects to be attacked.

Unilaterally develop cable regimes

Australia's lead in the protection of submarine cables by robust legal, regulatory and policy measures has given it a "gold standard." However, Australia's geography gives it opportunities to do so that may not exist for other quartet members. In the Bay of Bengal, particularly around the eastern Andaman and Nicobar Islands, India's claims need more clarity vis-vis its EEZ. Clarifying the matter may assist India in developing a similar "gold standard," but New Delhi will certainly be required to discuss the issue with its littoral neighbors for continuing trust and transparency.

For these reasons, we argue that Quad states may wish to reference Australia's "gold standard" but develop individual cable protection regimes that fit with their geographical remit, their public-private frameworks, and their legal regimes.

Single point of contact

Develop a single point of contact for reporting incidents in each member-state, as other experts have suggested.[27] The Quad should designate its nodal agencies for cooperation on submarine cable protection. Currently, the submarine cables-related regulation lies largely with the telecom ministries of the Quad countries with the involvement of respective security agencies for the protection of data.

However, in India's case the National Critical Information Infrastructure Protection Centre (NCIIPC), which is the national nodal agency, does not have subsea cables under its list of sectors. Focusing on granular issues such as these is needed to streamline commitments towards cable protection. Inter-agency cooperation makes it easier for quicker resolution of incidents but also

builds a robust and efficient regional framework by developing Standard Operating Procedures to be followed amongst the partners.

Policies for Today's Submarine World

While submarine cables have been around for some time, the threat to them has been revisited under the securitization debate of the Quad framework. The private industries' onus on cable laying and transmitting of data makes them as much a party to the debate about cable protection as national governments. Therefore, the state's role in the protection of submarine cables should remain limited, albeit required. In this situation, protection of the transnational submarine cables in the high seas requires closer introspection amongst the collaborating partners about what they can do, but more importantly, admit to what they cannot or should not do.

The Quad's response to protecting submarine communication cables in the Indo-Pacific reflects the increasing securitization of undersea infrastructure. The Quad's initiative recognizes the vital role of submarine cables in global connectivity and national security and aims to address emerging threats. Nevertheless, this policy brief emphasizes the importance of distinguishing realistic goals within and among the Quad's diverse members, geopolitical landscapes, and perceptions of threats. It has accordingly cataloged and prioritized current threats to submarine cables such as espionage and offered policy recommendations that are geared towards collectively addressing them. The Quad's informal structure places limits on what it can and cannot hope to achieve not just vis-à-vis submarine cable protection but a host of other threats. As such, this brief is useful in that it adds to and refines existing literature related to the quartet's efficacy as a security grouping, its cohesiveness, its deterrent value, and its future trajectory in the Indo-Pacific.

Authors –

Dr. Brendon J. Cannon *is an Assistant Professor at Khalifa University in Abu Dhabi, UAE, and an Associated Research Fellow at ISDP. His research is at the nexus of international relations, security studies, geopolitics, and emerging technologies in the Indo-Pacific.*

Dr. Pooja Bhatt *is an author and researcher in maritime security and governance issues based in New Delhi. Previously, she was a Consultant at the Ministry of External Affairs.*

For feedback, the authors can be reached at brendon.cannon@ku.ac.ae and poojabhatt.jnu@gmail.com

Disclosure statement –

Some of the ideas and analysis in this brief were presented at and emanated from the Undersea Cables, Geoeconomics, and Security in the Indo-Pacific: Risks and Resilience conference hosted by the Center for Indo-Pacific Affairs (CIPA) at the University of Hawai'i at Mānoa, October 26–27, 2023.

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

www.isdp.eu

Endnotes

1 "Why the undersea cables that connect the world are a subject of concern," *The Week*, February 18, 2022, https://www.theweek.co.uk/news/technology/955812/undersea-cables-connect-world-subject-concern.

2 Ash Rossiter, "Undersea cables in an age of geopolitical competition," Trends Research, February 19, 2023, https://trendsresearch.org/research.php?id=68&title=Undersea_cables_in_an_age_of_geopolitical_competition.

3 Robert Meyer and Nicole Starosielski, "Managing Risks for the World's Undersea Cable Network," Knowledge at Wharton, November 2, 2015, https://knowledge.wharton.upenn.edu/podcast/knowledge-at-wharton-podcast/managing-risks-for-the-worlds-undersea-cable-network/.

4 Insikt Group, "The Escalating Global Risk Environment for Submarine Cables," Recorded Future, June 27, 2023, https://www.recordedfuture.com/escalating-global-risk-environment-submarine-cables. See also, James Coker, "Submarine Cables at Growing Risk of Cyber-Attacks," Infosecurity Magazine, June 27, 2023, https://www.infosecurity-magazine.com/news/submarine-cables-risk-cyber-attacks/.

5 Guy Faulconbridge, "Russia now has free hand to destroy undersea communications cables, Putin ally says," *Reuters*, June 14, 2023, https://www.reuters.com/world/europe/russias-medvedev-says-moscow-now-has-free-hand-destroy-enemies-undersea-2023-06-14/.

6 Xiaoshan Xue and Adrianna Zhang, "Tensions With China Emerge Over Undersea Cables Carrying Internet Traffic," *VOA News*, March 29, 2023, https://www.voanews.com/a/tensions-with-china-emerge-over-undersea-cables-carrying-internet-traffic/7027809.html.

7 Dina Temple-Raston and Sean Powers, "Who tried to hack Hawaii's undersea cable?" The Record, April 27, 2022, https://therecord.media/who-tried-to-hack-hawaiis-undersea-cable.

8 Eric Tegler, "Investigating the Chinese Ship That 'Accidentally' Hit Undersea Lines," *Forbes*, November 28, 2023, https://www.forbes.com/sites/erictegler/2023/11/28/investigating-the-chinese-ship-that-accidentally-hit-undersea-lines/?sh=45b7cf7e40bf.

9 The Joint Expeditionary Force (JEF) is a United Kingdom-led expeditionary force which consists of Denmark, Finland, Estonia, Iceland, Latvia, Lithuania, the Netherlands, Sweden, and Norway.

10 "Britain to send seven Royal Navy ships to patrol areas with undersea cables," *Reuters*, November 30, 2023, https://www.reuters.com/world/uk/britain-send-seven-royal-navy-ships-patrol-areas-with-undersea-cables-2023-11-30/.

11 B. J. Cannon, and A. Rossiter, "Locating the Quad: informality, institutional flexibility, and future alignment in the Indo-Pacific," *International Politics* (2022): 1-22.

12 The 2023 Quad leaders' summit in Sydney was cancelled on account of U.S. President Joe Biden's absence. Instead, it was held on the sidelines of the G7 summit in Japan. See Lewis Jackson and Kirsty Needham, "Australia cancels Quad meeting in Sydney after Biden postponement," *Reuters*, May 17, 2023, https://www.reuters.com/world/asia-pacific/australia-pm-says-govt-talking-with-japan-india-quad-meet-after-biden-cancels-2023-05-16/.

13 Online interview with Indian analyst and maritime professional, October 12, 2023.

14 J. Brock, "U.S. and China wage war beneath the waves – over internet cables," *Reuters*, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

15 Ibid.

16 U.S. Department of State, "The Clean Network," https://2017-2021.state.gov/the-clean-network/.

17 Phil Gervasi, "Diving Deep into Submarine Cables: The Undersea Lifelines of Internet Connectivity," Kentik, March 28, 2023, https://www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/.

18 NEC, "NEC signs long-term charter contract with Global Marine Systems Limited for optical submarine cable-laying ship," Ocotber 17, 2022, https://www.nec.com/en/press/202210/global_20221017_01.html.

19 Amanda H A Watson, "Questions about Pacific cable announcement," DevPolicy Blog, November 10, 2023, https://devpolicy.org/questions-about-pacific-cable-announcement-20231110/.

20 Mick P. Green and Douglas R. Burnett, "Security of International Submarine Cable Infrastructure: Time to Rethink?" ICPC Ltd, https://www.iscpc.org/documents/?id=2974.

21 K. Hakata, and B. J. Cannon, "Japan's new Indo-Pacific: A guiding perspective to shape worldviews," ORF, May 3, 2023, https://www.orfonline.org/expert-speak/japans-new-indo-pacific-a-guiding-perspective-to-shape-worldviews.

22 Justin Sherman, "Cyber defense across the ocean floor: The geopolitics of submarine cable security," Atlantic Council, September 13, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.

23 James Coker, "Submarine Cables at Growing Risk of Cyber-Attacks," Infosecurity Magazine, June 27, 2023, https://www.infosecurity-magazine.com/news/submarine-cables-risk-cyber-attacks/.

24 Tom Corben, Ashley Townshend, Blake Herzinger, Darshana M. Baruah, and Tomohiko Satake, "Bolstering the Quad: The case for a collective approach to maritime security," United States Studies Centre, June 8, 2023, https://www.ussc.edu.au/bolstering-the-quad-the-case-for-a-collective-approach-to-maritime-security.

25 A. Mauldin, "The Subsea Cold War" [Conference presentation], September 28, 2023, Submarine Networks World, Singapore.

26 W. Y. Yee, "Indonesia Isn't Ready to Become Asia's Submarine Cable Hub," *Foreign Policy*, August 23, 2023, https://foreignpolicy.com/2023/08/31/indonesia-submarine-cable-internet-meta-google-us-china-competition/.

27 Mick P. Green and Douglas R. Burnett, "Security of International Submarine Cable Infrastructure: Time to Rethink?" ICPC Ltd, https://www.iscpc.org/documents/?id=2974.