Quad Tech Network QTN Series

A TECHNO-DIPLOMACY STRATEGY FOR TELECOMMUNICATIONS IN THE INDO-PACIFIC

SEPTEMBER 2021

Authors: Lisa Curtis and Martijn Rasser

Series Editors: Jennifer Jackett, William Stoltz and Rory Medcalf

Australian National University

Center for a New American Security

GRIPS 政策研究大学院大学 National Graduate Institute For Policy Studies

ORF

Australian Government

Department of Foreign Affairs and Trade

Published by the National Security College, The Australian National University, Acton ACT 2601, Australia

Available to download for free at nsc.anu.edu.au

Cover design and layout by Black Bear Creative.

About the Quad Tech Network Series

The Quad Tech Network (QTN) is an Australian Government initiative to promote Track 2 research and public dialogue on cyber and critical technology issues relevant to the Indo-Pacific region.

As part of the initiative, research institutions in Australia (the National Security College at The Australian National University), India (the Observer Research Foundation), Japan (the National Graduate Institute for Policy Studies) and the United States (Center for a New American Security) have commissioned papers on key issues facing the region.

These papers – together, the QTN series – offer analysis and recommendations on shared challenges facing Australia and Indo-Pacific partners in the cyber and technology environment.

The QTN is managed by the National Security College at The Australian National University, with the support of the Australian Department of Foreign Affairs and Trade.

About the Series Editors

Rory Medcalf is Head of the National Security College at The Australian National University. Professor Medcalf's professional background spans diplomacy, journalism, think thanks and intelligence analysis, including as founding Director of the International Security Program at the Lowy Institute from 2007 to 2015. Professor Medcalf has been recognised as a thought leader internationally for his work on the Indo-Pacific concept of the Asian strategic environment, as articulated in his 2020 book *Contest for the Indo-Pacific* (released internationally as *Indo-Pacific Empire*).

William Stoltz is the Senior Adviser for Public Policy at the National Security College. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates. Dr Stoltz joined the NSC after working across Australia's defence, intelligence, and law enforcement communities, including strategic intelligence and advisory roles within the Department of Defence, the Australian Federal Police, the Royal Australian Air Force (Reserve), and the National Intelligence Community.

Jennifer Jackett is a Sir Roland Wilson Scholar and PhD candidate at the National Security College. Her research examines US-China competition for leadership over emerging technologies and the implications for US allies and partners including Australia. She is currently on leave from the Australian Government where she held roles across the national security community advising government on issues such as critical infrastructure security, foreign interference, counter-terrorism, and international defence engagement.

About the Authors

Lisa Curtis is a Senior Fellow and Director of the Indo-Pacific Security Program at the Center for a New American Security (CNAS). She is a foreign policy and national security expert with over 20 years of service in the US government, including at the NSC, CIA, State Department, and Capitol Hill. Ms. Curtis served as Deputy Assistant to the President and NSC Senior Director for South and Central Asia from 2017-2021 under three successive National Security Advisors. She received a Bachelor of Arts degree in Economics from Indiana University.

Martijn Rasser is a Senior Fellow in the Technology and National Security Program at the Center for a New American Security (CNAS). Mr. Rasser served as a senior intelligence officer and analyst at the Central Intelligence Agency. Upon leaving government service, he was Chief of Staff at Muddy Waters Capital, an investment research firm. More recently, he was Director of Analysis at Kyndi, a venture-backed artificial intelligence startup. Mr. Rasser received his BA in anthropology from Bates College and his MA in security studies from Georgetown University.

Contents

Executive Summary

The countries in the Quadrilateral Security Dialogue (the Quad) – Australia, India, Japan, and the United States – have the opportunity to shape the telecommunications ecosystem in the Indo-Pacific so that key 5G and undersea cable infrastructure is more secure, resilient, and open. There are six lines of effort the Quad should pursue:

1. ***Public Diplomacy.*** The Quad members should have consistent messaging on the geopolitical risks of using technology from autocratic states.
2. ***Industry Collaboration.*** The Quad members should pool resources to provide financial incentives for private sector R&D, standard-setting, and digital infrastructure development. The four governments should also work with the private sector to craft an undersea cable strategy that addresses the risks associated with Chinese firms and cable landing sites in China.
3. ***Countering Coercion.*** The Quad members should provide financial or diplomatic support to any Indo-Pacific country that Beijing targets in response to forgoing Chinese technology purchases.
4. ***Government Financing.*** The Quad members should create new infrastructure financing mechanisms for telecommunications infrastructure development throughout the Indo-Pacific to provide a sustainable alternative to China's Belt and Road Initiative.
5. ***Monitoring and Security.*** The Quad members should set up a joint monitoring system to safeguard the integrity of the region's subsea cable network.
6. ***Strengthening Legal Frameworks.*** The Quad members should contribute to strengthening international laws to help prevent both physical damage and cyberattacks on telecommunications networks, particularly subsea cables.

Introduction

China's rapidly expanding role in the development of telecommunications technology and infrastructure across the Indo-Pacific raises concerns about the future security of regional digital ecosystems; the coercive power China will gain by controlling these networks; and the impact on broader political trends in the Indo-Pacific region.

There is growing recognition that a multilateral approach is required to deal with the challenges stemming from China's growing digital influence.

The Quadrilateral Security Dialogue between Australia, Japan, India and the United States (the Quad) is well placed to find solutions to these complex geo-technological problems because of each country's strong commitment to maintaining an open, free, transparent and rules-based order in the Indo-Pacific and the Quad's constructive approach to finding practical multilateral solutions to international security challenges. As the Quad leaders prepare to meet for the second time in 2021, it is clear that dealing with the technology challenges from China should be high on their agenda.

While there is a need for the Quad to examine the development of emerging technologies – such as artificial intelligence, quantum computing, 6G wireless technology, and biotechnology – this paper explores opportunities for Quad cooperation specifically on 5G wireless technology and subsea fibre-optic cables. The authors chose to focus on 5G and subsea cables as these are sectors on which the Quad countries have already begun collaboration and that provide immediate prospects for tangible Quad cooperation.

Enhancing Quad cooperation on emerging technologies requires building industry partnerships among the four nations.

Bringing the public and private sectors of one country together to identify technology solutions is a challenge in and of itself. Managing to establish industry partnerships among four different countries will be more challenging still. Yet bringing private industry from the four countries together to hammer out innovative, efficient, and democratic solutions for maintaining free and open technology ecosystems is urgently needed.

In addition to Quad coordination on critical technology issues, the European Union, United Kingdom, and technologically advanced nations and partners like South Korea and Taiwan will also play a role in identifying, developing, and implementing solutions. This paper, however, focuses specifically on the Quad nations and how they can create public-private partnerships aimed at protecting 5G infrastructure and undersea fibre-optic cables. The recommendations in this paper may serve as a template for how to approach challenges with other critical and emerging technologies.

The 5G Challenge

Communications networks are the central nervous system of modern society. The advent of 5G – fifth generation wireless networks – will make these technologies ever more essential and prevalent. Higher data throughput and very low latency will make a true Internet-of-Things feasible, connecting millions of devices – from self-driving cars, thermostats, streetlights, wearable devices and much more.[I] Connected devices will be woven into the daily fabric of society meaning that opportunities for economic growth and societal benefits will abound in a new digital reality.

Where there is opportunity, there is also risk. With 5G, there are concerns over the ability of China's authorities to conduct espionage and data exfiltration via the equipment of Chinese firms on networks in third countries. China has numerous laws that compel Chinese firms to assist the government's security and intelligence efforts, including the 2015 National Security Law and the 2021 Data Security Law.[1] This is often the primary argument for not having equipment from untrusted vendors such as Chinese telecommunications firm Huawei on 5G networks. Such concerns are not abstract worries, they are grounded in technical reality.

In April 2021, the Dutch newspaper *De Volkskrant* reported on a risk assessment on Huawei commissioned in 2010 by KPN, the largest telecommunications operator in the Netherlands. The report's findings were so damning that KPN avoided releasing them for fear that the company wouldn't survive. Investigators of the firm CapGemini, whom KPN commissioned to conduct the assessment, determined that Huawei personnel had unfettered access to KPN's network, could eavesdrop on all conversations, knew which numbers were monitored by Dutch police and intelligence services and had accessed the network core from China.[2] Even more significantly, 5G networks are rapidly becoming part of critical infrastructure by supporting most countries' ability to supply power, clean water, and transportation. The capacity of Chinese authorities to shut down a 5G network means having the capability to cripple infrastructure needed for the basic functioning of a society.[3] This is not a threat that can be diminished. In assessing the threat posed by Huawei's presence on Australian communications networks the Australian Signals Directorate, determined that even if it had "full and sole access to the source code, full access to hardware schematics" and updates done only in Australia, it could not fully mitigate the risk of shutdown by Huawei.[4]

Viable 5G Options: Traditional Trusted Vendors and Open-RAN

Excluding Huawei and other untrusted vendors[II] from supplying 5G network components leaves two alternatives.

Option one is buying equipment from the other established hardware providers: Nokia of Finland, Ericsson of Sweden, and Samsung of South Korea. There is appeal in doing so in that the firms offer proven technology and have experience building out and maintaining network infrastructure. A major drawback, however, is the inefficiencies of the telecom hardware industry: the limited vendor pool constrains the ability of vendors to negotiate on price and the general lack of interoperability between equipment made by the three companies means that an operator has "vendor lock-in". Once you commit to one vendor it is typically prohibitively expensive to change vendors within an equipment generation (about 10 years).

Option two is adopting a technology alternative to hardware-dominant 5G networks. This approach is wireless infrastructure built on a modular architecture with open interfaces, often referred to as open radio access networks (open-RAN). With this model, many of the functions currently done by RAN hardware is conducted by software, a process called network virtualisation. There are several distinct advantages: greater vendor diversity, better interoperability, supply chain resiliency, improved security, and probable cost savings.[5]

Because the software industry's barriers to entry are lower, new entrants can be expected to enter the 5G service market, which is projected to exceed $85 billion by 2024 at 31.9 percent compound annual growth rate.[6] On a virtualised network, interoperability will be vendoragnostic because every hardware and software component must be compatible to function.

Greater vendor diversity and interoperability enhances the overall resilience of the supply chain.

Security also benefits because the transparency associated with open interfaces makes it easier to verify and monitor software security compared to the traditional hardware that are "black boxes" to its operators. Finally, greater competition and lower software development costs should translate into lower prices.[7]

I. Latency is the amount of time it takes for a data packet to travel from sender to receiver and back.

II. While the term 'untrusted vendor' is often used by American government officials, the 2018 joint statement by Australian officials on the trustworthiness of telecommunications vendors stated it thusly: "The government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference."

Some analysts caution that the timing and extent of these advantages is not yet known. There is merit to some of these arguments, particularly how significant the cost savings may be. Furthermore, because open-RAN solutions are still coalescing, security measures still need to be defined and agreed upon. Improvements in energy efficiency and performance in areas of high user density (urban areas) are also needed to support large-scale rollouts.[8]

Quad 5G Open-RAN: Strengths and Challenges

The Quad countries are well-positioned to build and promote 5G open-RAN deployments in the Indo-Pacific and around the world. Companies in Australia, India, Japan, and the United States each bring to bear relevant capabilities and expertise. Japanese and American firms in particular have the requisite technologies and know-how. When combined with governmentled investment mechanisms, the Quad could offer sustained support for the development of secure, resilient, and open digital infrastructure throughout the Indo-Pacific.[9]

Australia

Of the four countries, Australia has the least to offer from a technology standpoint at present. While the country has a mature telecommunications market, few homegrown companies produce equipment needed to build out networks. What Australia does bring to the table is experience: a majority of Australians enjoy 5G coverage provided by the country's three main carriers.[10] The Australian experience with urban and rural rollouts will help to inform best practices for 5G open-RAN rollouts in the region, particularly in remote and geographically complex areas of the Pacific. Australia also brings important cybersecurity testing expertise to bear that can be used to address vulnerabilities associated with growing network virtualisation.[11]

A further advantage Australia has is vast stretches of sparsely populated land. These provide ideal test areas for remote-sensing and remote-control applications of 5G networks.[12] Australian firms could therefore take a leading role in developing solutions in areas such as weather, forestry, agriculture, and biodiversity that would benefit less affluent countries in the Indo-Pacific.

India

India has potential to become a global technology leader in telecommunications. While India lags its Quad peers in rollouts of commercial 5G networks – the first will begin by early 2022 – Indian telecommunications companies are keen to incorporate open-RAN solutions.[13] India's Department of Telecommunications allocated a swath of spectrum in early June 2021 for Indian firms to partner with non-Chinese firms on 5G trials.[14] This momentum and the country's world-class software industry prime it for opportunities in developing open-RAN solutions. Several collaborations with companies from Quad countries are underway.

The telecommunications services company Bharti Airtel is developing 5G network technologies, traditional and open-RAN, independently and in partnership with Indian, American and Japanese firms.[15] Reliance Jio Platforms teamed up with US firm Qualcomm Technologies to develop an open-RAN compliant 5G architecture for network infrastructure in India.[16] Expertise and experience gained during these collaborations can contribute to Indian firms' efforts to become globally competitive in the sector. To do so, however, India must alter its autarkic and protectionist policies.

Prime Minister Modi's economic philosophy Atamanirbhar Bharat – typically translated as selfreliant India – is centered on the premise of limiting foreign firms' access to India's domestic market while at the same time boosting domestic manufacturing and services, and exports of Indian products. Beyond the inherent contradictions in the two basic goals, this philosophy is at odds with the kind of multilateral collaboration between governments and private industry that is needed to craft and execute an effective Quad strategy on 5G.

Japan

Japan is at the forefront of 5G open-RAN deployments. The company Rakuten is spearheading the world's largest open-RAN network and was on track to provide coverage to over 90 percent of Japan's population by mid-2021.[17] Lessons learned from this network rollout will provide valuable insight into opportunities, challenges, and risks with widespread deployments elsewhere. Other firms provide important expertise and connections as well. NEC Corporation is a leading provider of open-RAN compliant equipment and has launched a project with the UK government.[18] Japanese operator NTT DoCoMo is part of a 12-company international partnership to accelerate open-RAN deployments.[19] Leveraging such existing relationships could jumpstart a comprehensive Quad-centered effort.

The United States

US companies are among the world leaders in open-RAN technologies and would likely be the cornerstone of a broader Quad strategy.[20] American firms are already partnering with operators around the world to develop and deploy relevant infrastructure. Logically, these companies would be central to a burgeoning Quad effort to address the digital divide in the Indo-Pacific. Technological innovation by these firms to address concerns about current open-RAN capabilities, such as for capacity and performance in high user-density areas, will also be key. For example, the firm Parallel Wireless claims it has developed technology suitable for urban networks.[21]

Addressing Digital Entanglement with China in the Indo-Pacific

The Quad needs to create a 5G strategy with the goal of promoting secure and digital infrastructure throughout the Indo-Pacific. This requires making high-quality 5G networks available at competitive prices and with greater vendor diversity. Networks based on open-RAN architecture provide such flexibility. To make such equipment affordable, government-backed investment offerings and public-private partnerships will be needed.

Beyond competitive upfront pricing, an important value proposition is providing jobs and training for the local population. Not only does this give the customer country a larger vested interest in the infrastructure investment, it offers the Quad the opportunity to ensure that the applications these communications networks enable, such as surveillance and smart cities, are used in ways that comport with liberal democratic norms and values. The Quad could use its nascent emerging technologies working group as the initial forum to finetune the details for this strategy.

5G Collaboration Beyond the Quad

A Quad 5G telecommunications strategy should also feature a broader multilateral engagement component. A larger group of stakeholders would mean access to more technology, know-how, and resources, and provide increased appeal and legitimacy to efforts to disentangle the Indo-Pacific from Chinese technology offerings. The European Union, South Korea, and the United Kingdom would be common-sense partners for the Quad. Each has distinct interests in the region and the European Union and United Kingdom have specific regional strategies, both emphasising the kind of sustainable development that trustworthy digital infrastructure investments bring.[22]

They each also feature growing support within government and industry for open-RAN offerings for 5G. Five of Europe's largest mobile operators announced large-scale open-RAN rollouts for 2022 and Nokia, one of the leading trusted vendors of telecommunications equipment, is producing open-RAN compliant equipment.[23] Similarly in South Korea, Samsung is providing equipment compliant with open interfaces to Japanese operator NTT DoCoMo, while Prime Minister Moon concluded an agreement with US President Biden in May 2021 to jointly develop 5G and 6G network architectures using open-RAN technologies.[24] Open interfaces feature prominently in the UK government's 5G supply chain diversification strategy and its leading operator Vodafone is an advocate for open-RAN deployments in Europe.[25]

The Quad and Undersea Cables

The Quad's approach to terrestrial 5G networks should mesh with its strategy for other critical global communications infrastructure. Seabed cables are key links and of increasing importance in the Indo-Pacific as parts of the region are becoming more integrated. Beijing recognises the centrality of these cables and is expending considerable resources to gain global market share.

China is aggressively pursuing undersea cable construction across the globe to facilitate its ability to gain control over increasing amounts of global data and information flows.

Nearly 95 percent of intercontinental global data transmissions rely on undersea cables. With global bandwidth demand growing exponentially and expected to nearly double every two years, the demand for undersea cable construction will also rise accordingly.[26] While American companies like Google, Facebook, Microsoft, and Amazon currently own or lease nearly half of the global undersea bandwidth, China's Huawei Marine has built or repaired nearly 100 of the world's 400 undersea cables, including dozens in Southeast Asia in the last few years.[27] In 2020, following US sanctioning of Huawei Technologies, the company divested Huawei Marine, which is now majority-owned by another Chinese firm, Hengtong Optic-Electric. Despite the divestment scheme, Huawei Marine is still listed in the US Department of Commerce "Entity List," which restricts the sale of US goods and technology to the company.[28]

In addition to restricting Huawei Marine's access to US technology, the United States is discouraging US companies from constructing subsea cables links to China. While the most common reason for subsea cable disruption remains fishing-related activities near coastlines, there is growing concern about the potential for state actors to target the cables for malicious activity. Last year, US Federal Communications Commissioner Geoffrey Starks raised concerns about Chinese control over subsea cables, especially those connecting the United States and China, and cables that are partially owned by Chinese state-owned companies.[29] Starks indicated a need to ensure subsea telecommunications infrastructure is trustworthy and that adversaries of the United States are unable to sabotage the cables or intercept the information and data being transmitted through them. Due to US government pressure, Facebook backed out of a project to construct an undersea fibre-optic cable from California to Hong Kong earlier this year. In September 2020, Facebook withdrew from two other undersea cable projects that would have connected the United States to Hong Kong.[30] The US Department of Justice had recommended to the Federal Communications Commission against the connections, given Beijing's recent crackdown in Hong Kong and last year's implementation of the Hong Kong National Security Law, which gives China sweeping powers to tighten its grip on the region.

One of China's most high-profile undersea cable projects, the Pakistan and East Africa Connecting Europe (PEACE) cable, is set to run over 9,000 miles from the Gwadar Port in Pakistan to landing sites in Djibouti, Kenya, Seychelles, South Africa, and Marseille, France.[31] Another project, 2Africa, will connect 23 countries in Africa, the Middle East, Europe, and Asia and is being run by a consortium made up of China Mobile International, Djibouti Telecom, Facebook, MTN GlobalConnect, Orange, Saudi Telecom Company, Telecom Egypt, Vodafone, and West Indian Ocean Cable Company. This cable, which is expected to be completed by 2024, will run nearly 23,000 miles with 21 landing sites in 16 African countries.[32]

There is concern about the expanding role of China in subsea cable construction, particularly when it comes to protecting the sovereignty and resilience of those Indo-Pacific countries with less developed critical infrastructure. For this reason, the Quad countries are competing with China to meet expanding demand for bandwidth through new construction of undersea cables in the Pacific Islands. In January 2018, Australia took control of a project, originally led by Huawei Marine, to build a cable from Australia to the Solomon Islands.[33] The United States worked with Australia and Japan in October 2020 to finance a submarine internet cable spur to the Pacific Island nation of Palau. This cooperation was possible under a Memorandum of Understanding the three countries signed in 2018, enabling the US Development Finance Corporation, the Japan Bank for International Cooperation, and Australia's Department of Foreign Affairs and Trade and Export Finance and Insurance Corporation to work together to mobilise private capital to support major infrastructure projects in the region. In late February, the Pacific Island nations of Micronesia, Kiribati, and Nauru cancelled bidding for another undersea cable project, for which Huawei Marine was competing, after the United States raised concerns about the security of the project.[34] More recently in mid-June, in a new bidding process for the Pacific Islands cable project, the World-Bank led consortium declined to award the contract to any bidder when Huawei Marine submitted a bid more than 20 percent below rivals Alcatel's Submarine Networks and Japan's NEC bids. The World Bank has indicated it was working with the Pacific Island governments to map out next steps.[35]

Each Quad country brings an individual strength to the subsea cable issue.

Between the two of them, US SubCom and Japan's NEC account for about 70 percent of the submarine fibre-optic cable market. Australia, for its part, has been a leader in creating regulatory frameworks for the protection of undersea cables.[36] And India is set to be a key landing point for undersea cables transiting the Indian Ocean. At least eight new subsea cable systems that will have landing stations in India are currently under consideration. In addition, Japan's NEC recently laid an undersea fibre-optic cable to connect mainland India to its Andaman and Nicobar Islands. The project received support from both the Indian and Japanese governments.

Implications and Recommendations

The developments with open-RAN show how private sector collaboration, with nudges by national-level governments, can set the stage for transformative possibilities in relatively short order. In early 2019, virtually no policymaker in any of the Quad countries had considered open interfaces for telecommunications networks. By late 2020, open-RAN had become the main topic among lawmakers when thinking about shaping a secure 5G future. The technodemocracies will need to take similar steps regarding construction of undersea fibre-optic cables.

While dealing with the subsea cable challenge may not be as complicated or costly for the Quad governments as handling the 5G challenge, the need for multilateral action on the issue is urgent. Chinese companies are still behind American, Japanese, and French companies in the subsea cable construction business, so managing China's new encroachment in the industry is likely manageable. Japan-based NEC, US-based SubCom, and France-based Alcatel Submarine Networks hold more than 90 percent of the market share of the subsea cable industry. China's goal to try to capture 60 percent of the world's fibre-optic communications market by 2025 may seem far-fetched, however, given how quickly non-Chinese companies fell behind in the 5G race, nothing should be taken for granted. Protecting subsea cables from potential Chinese espionage and/or sabotage does not require restructuring the industry in fundamental ways as is the case with 5G.

However, from the private sector perspective, it will be burdensome to restructure their undersea cable investments to avoid Chinese involvement. Subsea cables cost hundreds of millions of dollars, usually involve multiple international investors, and can operate for up to 25 years,[37] so if a consortium member changes course on its investment mid-stream, there will be implications for the market. Some argue that ensuring different subsea cable systems and landing stations connect seamlessly with one another is critical to overall connectivity and internet performance. Trying to segregate Chinese companies from the construction, operation, and maintenance of certain subsea cable projects, they say, would be detrimental to the goal of maintaining open and connected societies. If US companies avoid building subsea cables with landing sites in or near the Chinese mainland, the world will likely head toward a "splinternet" that could contribute to further political divisions and diplomatic misunderstandings among nations. Because of these questions and uncertainties, a public-private dialogue among likeminded democratic partners and industry leaders is essential.

Building on the respective strengths they bring to the open-RAN and subsea cable issues, the Quad members should work together along six main lines of effort:

- ***Public Diplomacy.*** The Quad countries should pursue a clear and consistent effort to inform the publics of the Indo-Pacific countries about the risks of using technology from techno-autocracies, such as China. These efforts should also include helping governments in the region to build systemic mechanisms to factor geopolitical risks in policy decision making.
- ***Industry Collaboration.*** The Quad members should provide incentives such as tax credits to encourage more and deeper collaboration, particularly for R&D, standardsetting, and infrastructure development in third countries. For undersea cables, the private sectors of each Quad nation must also discuss the implications for the market and overall connectivity and internet performance of segregating Chinese companies in subsea cable construction and in avoiding landing sites on or near mainland China.
- ***Countering Coercion.*** The Quad members should provide financial or diplomatic support to any Indo-Pacific country that Beijing targets in response to forgoing Chinese technology purchases. Ensuring a united front on this matter will demonstrate to the region that Beijing cannot exert its will in the region unfettered. Numerous scholars have proposed ideas for countering Chinese economic coercion that could serve as the model for such an effort.[38]
- ***Government Financing.*** The US-Japan-Australia joint project to finance the subsea cable to Palau is a good example of multilateral cooperation to compete against Chinese efforts to dominate subsea cable construction in the Pacific Islands, where demand for bandwidth and connectivity is rapidly increasing. The US International Development Finance Corporation's loan of $500 million to a consortium of companies to develop a mobile network in Ethiopia could serve as a template for 5G projects.[39]

  Future efforts to pool financing for subsea cable projects in the Indo-Pacific region with strategic benefits for all four Quad members should also involve India. While India has not traditionally engaged in this type of multi-country project financing, its participation in such initiatives would send a strong signal about the strength and impact of the Quad as a part of the regional architecture.
- ***Monitoring and Security***. With an increased number of Chinese oceanographic research and survey vessels transiting the Indian Ocean Region, it is important for the Quad nations to set up a system to monitor the movements and activities of the Chinese vessels and guard against sabotage and espionage of the subsea cable network. Similarly, regular information exchanges between the Quad governments on Chinese digital infrastructure investments will streamline cooperative action by the Quad on efforts to counter and mitigate those developments.

- ***Strengthening Legal Frameworks.*** The Quad members can contribute to strengthening international laws to help prevent both physical damage and cyberattacks on telecommunications networks, particularly subsea cables. The UN Convention on the Law of the Sea recognises the freedom of states to lay and protect cables within their Exclusive Economic Zones and to lay cables on the continental shelf, yet there is no existing treaty to protect against cyber warfare on subsea cables.[40] The International Cable Protection Committee, an international non-governmental organisation that promotes undersea cable protection, could serve as a valuable resource for the Quad governments as they consider developing and promoting specific international standards and regulations to maintain security of undersea cables.

Conclusion

The governments of the Quad countries have the potential to set the Indo-Pacific on course to achieve a digital future that is secure, resilient, reliable, and beneficial. Doing so will require coordinated policies on countering the diffusion of techno-authoritarianism and digital entanglement with China in the region. This means making trusted technology alternatives available, assuring their affordability by providing sustainable financial support, providing safeguards against economic coercion attempts by Beijing, and countering high-tech illiberalism. Australia, India, Japan, and the United States have the collective heft, capabilities, and financial resources to achieve this if they act in concert, especially when in partnership with other tech-leading democracies.

A concrete techno-diplomatic strategy for telecommunications will be key to assuring the Indo-Pacific's future is free and open.

Endnotes

1. "National Security Law of the People's Republic of China," People's Republic of China, July 1, 2015, https://chinacopyrightandmedia.wordpress.com/2015/07/01/national-security-law-of-the-peoples-republic-of-china/; Abby Chen, "A Close Reading of China's Data Security Law, in Effect Sept. 1, 2021," China Briefing, July 14, 2021, https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/
2. Huib Modderkolk, "Huawei kon alle gesprekken van mobiele KPN klanten afluisteren," Volkskrant, April 17, 2021, https://www.volkskrant.nl/nieuws-achtergrond/huawei-kon-alle-gesprekken-van-mobiele-kpn-klanten-afluisteren-inclusief-die-van-de-premier~bd1aece1/
3. Martijn Rasser and Ainikki Riikonen, "Open Future: The Way Forward on 5G", Center for a New American Security, July 28, 2020, https://www.cnas.org/publications/reports/open-future.
4. Peter Hartcher, "China could have ordered Huawei to shut down Australia's 5G", The Sydney Morning Herald, May 21, 20121, https://www.smh.com.au/politics/federal/china-could-have-ordered-huawei-to-shut-down-australia-s-5g-20210520-p57trn.html
5. Martijn Rasser and Ainikki Riikonen, "Open Future: The Way Forward on 5G", Center for a New American Security, July 28, 2020, https://www.cnas.org/publications/reports/open-future.
6. Market Research Future (MRFR) "5G Service Market to Witness Upsurge by 31.9% CAGR by 2023", Globe Newswire, July 30 2019 https://www.globenewswire.com/news-release/2019/07/30/1893828/0/en/5G-Service-Market-to-Witness-Upsurge-by-31-9-CAGR-by-2023-Upsurge-in-Ultra-Latent-Connectivity-to-Foster-5G-Service-Market-Growth.html.
7. Martijn Rasser and Ainikki Riikonen, "Open Future: The Way Forward on 5G" (Center for a New American Security, July 28, 2020), https://www.cnas.org/publications/reports/open-future.
8. See for example, John Strand, "Fact vs Fiction: The 10 Parameters of OpenRAN," Strand Consult, April 30, 2021, https://strandconsult.dk/fact-vs-fiction-the-10-parameters-of-openran/; Dean Bubley, "Open RAN: The Future, not the Present," Strand Consult, 9 March, 2021, https://strandconsult.dk/blog/open-ran-the-future-not-the-present/; and Iain Morris, "Say hello the to the open RAN 'ecosystem,' or vendor lock-in 2.0," February 8, 2021, https://www.lightreading.com/open-ran/say-hello-to-open-ran-ecosystem-or-vendor-lock-in-20/d/d-id/767225
9. Martijn Rasser, "Networked: A Techno-Democratic Statecraft for Australia and the Quad", Center for a New American Security, January 19, 2021, https://www.cnas.org/publications/reports/networked-techno-democratic-statecraft-for-australia-and-the-quad
10. Juan Pedro Tomas, "The current state of 5G in Australia," RCR Wireless, December 29, 2020, https://www.rcrwireless.com/20201229/5g/the-current-state-5g-australia
11. Australian Trade and Investment Commission, "Cybersecurity," Australian Government, January 2017, https://www.austrade.gov.au/ArticleDocuments/1358/Cyber%20security%20ICR.pdf.aspx
12. Rajiv Shah, "Australia needs to take the lead on 5G again," The Strategist, September 17, 2020, https://www.aspistrategist.org.au/australia-needs-to-take-the-lead-on-5g-again/
13. Lok Sabha Secretariat "The Twenty-First Report of the Standing Committee on Information Technology (2020-21) on the Subject 'India's Preparedness for 5G' Relating to the Ministry of Communications (Department of Telecommunications," 8 February, 2021, http://164.100.47.193/lsscommittee/Information%20Technology/pr_files/Press%20Release%20on%2021st%20Report%20.pdf; https://www.zenger.news/2021/02/11/open-ran-technology-to-play-major-role-in-indias-5g-ambitions/#:~:text=Video-,Open%20RAN%20Technology%20To%20Play%20Major%20Role%20In%20India's%205G,billion%205G%20subscriptions%20in%202026.&text=MUMBAI%2C%20India%20%E2%80%94%20Global%205G%20adoption,leap%20forward%20from%20this%20year; Gandeep Kaur, "Indian telcos warm up to open RAN," Light Reading, September 23, 2020, https://www.lightreading.com/open-ran/indian-telcos-warm-up-to-open-ran/d/d-id/764125
14. Kalyan Parbat, "DoT allots 5G trial spectrum, paves way for development of use cases," ET Telecom, May 28, 2021, https://telecom.economictimes.indiatimes.com/news/dot-allots-5g-trial-spectrum-paves-way-for-development-of-use-cases/83027202
15. Danish Khan, "Airtel's dramatic strategy shift: Developing local 5G gear ecosystem via own R&D and US, Japanese partners," ET Telecom, 21 October, 2020, https://telecom.economictimes.indiatimes.com/news/airtels-dramatic-strategy-shift-developing-local-5g-gear-local-ecosystem-via-own-rd-and-us-japanese-partners/78774004
16. "Qualcomm and Reliance Jio Align Efforts on 5G," Qualcomm Press Note, October 20, 2020, https://www.qualcomm.com/news/releases/2020/10/20/qualcomm-and-reliance-jio-align-efforts-5g
17. Juan Pedro Tomas, "Rakuten Mobile receives approval to expand 5G via 1.7GHz band," RCR Wireless News, 15 April 2021, https://www.rcrwireless.com/20210415/5g/rakuten-mobile-receives-approval-expand-5g-via-1-7-band
18. "NEC participates in the UK Government-led 5G Open RAN trial program with the NeutrORAN testbed," NEC Press Release, November 30, 2020, https://www.nec.com/en/press/202011/global_20201130_02.html
19. Juan Pedro Tomas, "NTT DoCoMo aims for a 5G O-RAN ecosystem with 12 partners," RCR Wireless News, February 4, 2021, https://www.rcrwireless.com/20210204/asia-pacific/ntt-docomo-creates-5g-oran-ecosystem-12-partners
20. Stu Woo, "The U.S. Is Back in the 5G Game," Wall Street Journal, May 26, 2021, https://www.wsj.com/articles/us-5g-companies-11621870061
21. News Wire Feed, "Parallel Wireless touts urban open RAN," Light Reading, May 5, 2021, https://www.lightreading.com/open-ran/parallel-wireless-touts-urban-open-ran/d/d-id/769281
22. "EU Strategy for Cooperation in the Indo-Pacific," European Union, April 19, 2021, https://eeas.europa.eu/headquarters/headquarters-homepage_en/96740/EU; "Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy," Cabinet Office Policy Paper, March 16, 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

23. Alan Burkitt-Gray, "Big five mobile operators to start open RAN next year," Capacity, May 13, 2021, https://www.capacitymedia.com/articles/3828532/big-five-mobile-operators-to-start-open-ran-next-year; "Open RAN," Nokia, https://www.nokia.com/networks/portfolio/radio-access-networks-ran/open-ran/

24. Catherine Sbeglia, "Samsung to provide Open RAN-compliant solutions to NTT DoCoMo," RCR Wireless News, March 22, 2021, https://www.rcrwireless.com/20210322/5g/samsung-to-provide-open-ran-compliant-solutions-to-ntt-docomo; "U.S.-ROK Leaders' Joint Statement," The White House, May 21, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/u-s-rok-leaders-joint-statement/

25. "5G Supply Chain Diversification Strategy," Department for Digital, Culture, Media & Sport, December 7, 2020, https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy

26. Jonathan E. Hillman, "Securing the Subsea Network: A Primer for Policymakers," Center for Strategic and International Studies, March 9, 2021, https://www.csis.org/analysis/securing-subsea-network-primer-policymakers.

27. Nadia Schadlow and Brayden Helwig, "Protecting undersea cables must be made a national security priority," DefenseNews, July 1, 2020, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/.

28. Jonathan Barrett, "Exclusive: U.S. warns Pacific islands about Chinese bid for undersea cable project – sources," Reuters, December 17, 2020, https://www.reuters.com/article/us-china-pacific-exclusive-idUSKBN28R0L2; and Winston Qiu, "Global Marine Group Fully Divests Stake in Huawei Marine Networks," Submarine Networks, June 6, 2020, https://www.submarinenetworks.com/en/vendors/huawei-marine/global-marine-completes-sale-of-30-stake-in-huawei-marine-networks-for-85-million.

29. David Shepardson, "FCC commissioner calls for new scrutiny of undersea data cables," Reuters, September 30, 2020, https://www.reuters.com/article/usa-trade-china-telecommunications/fcc-commissioner-calls-for-new-scrutiny-of-undersea-data-cables-idINL1N2GR1DV.

30. Isobel Asher Hamilton, "Facebook killed off its 3rd U.S.-Hong Kong undersea internet cable project in 6 months, citing U.S. political pressure," Insider, March 11, 2021, https://www.businessinsider.com/facebook-kills-cable-project-california-hong-kong-americas-hka-2021-3

31. Brian Gicheru Kinuya, "How China is Winning the Subsea Internet Cable Competition in Africa," The Maritime Executive, March 22, 2021, https://www.maritime-executive.com/editorials/how-china-is-winning-the-subsea-internet-cable-competition-in-africa

32. "2Africa: Cable of Life," https://www.2africacable.com/.

33. "Solomon Islands Drops Chinese Tech Giant Huawei for Billion-Dollar Undersea Cable, Signs Australia," South China Morning Post, June 13, 2018, https://www.scmp.com/news/asia/diplomacy/article/2150616/solomon-islands-drops-chinese-tech-giant-huawei-billion-dollar.

34. Jonathan Barrett, "Exclusive: U.S. warns Pacific islands about Chinese bid for undersea cable project – sources," Reuters, December 20, 2017, https://www.reuters.com/article/us-china-pacific-exclusive/exclusive-u-s-warns-pacific-islands-about-chinese-bid-for-undersea-cable-project-sources-idUSKBN28R0L2

35. Jonathan Barrett and Yew Lun, "Pacific undersea cable project sinks after U.S. warns against Chinese bid," *Reuters*, June 17, 2021, https://www.reuters.com/world/asia-pacific/exclusive-pacific-undersea-cable-project-sinks-after-us-warns-against-chinese-2021-06-18/.

36. Parliament of Australia, "Telecommunications Legislative Amendment (Subsea Cable Protection) Bill 2013," Bills Digest no. 46, 2013-2014, February 27, 2014, https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/3022582/upload_binary/3022582.pdf;fileType=application/pdf

37. Jonathan E. Hillman, "Securing the Subsea Network: A Primer for Policymakers," Center for Strategic and International Studies, March 9, 2021, https://www.csis.org/analysis/securing-subsea-network-primer-policymakers.

38. See for example, Kristine Lee, Daniel Kliman, and Joshua Fitt, "Crossed Wires: Recalibrating Engagement with North Korea for an Era of Competition with China," December 18, 2019, https://www.cnas.org/publications/reports/crossed-wires; Peter Harrell, Elizabeth Rosenberg, and Eduardo Saravelle, "China's Use of Coercive Economic Measures," June 11, 2018, https://www.cnas.org/publications/reports/chinas-use-of-coercive-economic-measures; and Shin Oya, "Coping with China's economic threat," The Japan Times, July 28, 2020, https://www.japantimes.co.jp/opinion/2020/07/28/commentary/japan-commentary/coping-chinas-economic-threat/.

39. Manny Pham, "US bets $500M on Vodafone consortium in Ethiopia," Developing Telecoms, December 15, 2020, https://developingtelecoms.com/telecom-business/telecom-investment-mergers/10446-us-bets-500m-on-vodafone-consortium-in-ethiopia.html

40. Garrett Hinck, "Cutting the Cord: The Legal Regime Protecting Undersea Cables," Lawfare, November 21, 2017, https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables

About the National Security College

The National Security College (NSC) is a joint initiative of The Australian National University and Commonwealth Government. The NSC offers specialist graduate studies, professional and executive education, futures analysis, and a national platform for trusted and independent policy dialogue.

T +61 2 6125 1219

E national.security.college@anu.edu.au

W nsc.anu.edu.au

 @NSC_ANU

 National Security College

CRICOS Provider #00120C