Australian National University | National Security College

Taking a strategic view of telecom networks in the Indo-Pacific

Sameer Patil

Key points

- 5G (fifth-generation) represents a generational shift in wireless telecommunications, but it is not cheap, and developing economies have faced budgetary constraints in deploying it.
- Chinese telecom companies have stepped in to offer 5G technology at cheaper rates than their western competitors and captured new markets. Their market dominance not only creates cybersecurity and surveillance risks, but also enables Beijing to create new standards and shape digital economy narratives.
- These dynamics create an imperative for Quad partners to work together on countering Chinese telecom companies' dominance and secure Indo-Pacific telecom networks.

Policy recommendations

- Leverage the Quad's financial heft, innovation, and talent to push for cost-effective, secure, and trusted hardware; endorse "The Prague Proposals" for 5G networks.
- Promote the Quad's technology ecosystem to speak to each other and other like-minded partners.
- Expedite research efforts, commercialise and secure the Open-Radio Access Network (O-RAN), which is also important for 6G.
- Establish a regional consultative mechanism for developing new standards at the International Telecom Union; harmonise existing standards.

Introduction

The Indo-Pacific is home to some of the world's fastest-growing digital economies that are harnessing technology for national governance and economic development. Telecommunications connectivity – the internet and mobile penetration base – forms the backbone for these economies. Unsurprisingly, the telecom market in the region is witnessing an upgrade. By 2030, telecom companies are expected to invest US$259 billion in the development of networks in the region.[1] These investments will foster the expansion of the digital economy and act as catalysts for innovation, growth and prosperity, with 5G technology playing an indispensable role in this.

5G represents a generational shift in wireless telecommunications – anchored on higher data transfer speed and ultra-low latency. It holds the promise of revolutionising how people communicate and consume content on the internet and transforming edtech, telemedicine, precision agriculture, and the Internet of Things (IoT). However, 5G technology is not cheap, and developing economies have faced budgetary constraints in deploying it. Estimates suggest that an average baseline cost of a national 5G rollout is expected to be US$3-8 billion per country, with an additional 20-35 per cent investment required for extending coverage.[2] This is where the Chinese telecom companies have stepped in.

Chinese companies' hold over the regional market and its implications

Pioneering the development and commercialisation of 5G technology, companies such as Huawei, Zhong Xing Telecommunication Equipment (ZTE), and China Unicom are aggressively penetrating new markets by offering cheaper rates than their western competitors. This, combined with a forceful push from the Chinese government, has enabled Huawei and ZTE to corner 29 and 11 per cent of the total global 5G revenues.[3]

However, given the chequered past of Chinese tech firms working at the behest of their government, the expansion of Huawei and ZTE has worried policymakers in several countries – primarily Quad partners and European allies of the United States (US) – that China may be strategically pushing its companies to capture newer markets in the Indo-Pacific to create a vast eavesdropping network through backdoors. Notwithstanding these concerns, many countries in the Indo-Pacific have prioritised commercial considerations over security concerns and deployed Huawei and ZTE equipment. In Southeast Asia, all countries, barring Vietnam, use Huawei for telecom connectivity. In Vietnam, its largest telecom provider, Viettel, has not used Huawei equipment nationally, even though its local subsidiaries in Cambodia and Laos have used it in deploying 4G and 3G networks.[4] [5]

The Chinese telecom companies' expanding market share has not only enabled Beijing to maintain its dominant position as a telecommunications leader, but allowed it to use that heft in other ways. For instance, Huawei has proposed replacing the US-invented Transmission Control Protocol/Internet Protocol (TCP/IP) with a new IP standard that it claims is faster than the existing protocol. Likewise, the company has utilised its market presence to shape critical conversations in the digital economy. In Thailand, for instance, it has worked with the Thai government to write a white paper on the digital roadmap for ageing society, agriculture and tourism.[6]

Beyond the surveillance risk, the dominance of Chinese 5G companies also creates a further cybersecurity risk, particularly for those companies that have chosen non-Chinese telecom equipment. Chinese state-sponsored hacking groups are known to execute attacks targeting critical infrastructure, primarily for disruption and data harvesting purposes. A similar threat extends to telecom networks, which are an important part of critical national infrastructure. In June 2022, US government agencies flagged that China-backed threat actors had exploited vulnerabilities in telecommunications companies and network service providers to steal credentials and harvest data.[7]

Collaborating to secure telecom networks

These dynamics create an imperative for the Quad partners to work together in countering Chinese telecom companies' dominance and securing Indo-Pacific telecom networks. The Quad Principles on Technology Design, Development, Governance, and Use have emphasised "trust, integrity, and resilience" and "safety and security-by-design approaches".[8] To achieve this, the Quad members must work together to encourage the use of secure and trustworthy hardware, create partnerships across their national technology ecosystems and mobilise developing economies of the Indo-Pacific in standard-setting exercises.

- Secure and trustworthy hardware: To encourage wide adoption of secure and trustworthy telecom hardware in the Indo-Pacific, Quad members must leverage their financial heft, innovation and talent to push for cost-effective and trusted hardware. They can potentially provide financial incentives to developing economies through development financing mechanisms. These financial incentives must be combined with the creation of whitelisted trusted vendors/sources that meet the necessary security

criterion and are interoperable. In addition, the Quad leaders can endorse "The Prague Proposals", which recommend a cybersecurity framework for 5G mobile networks and connectivity.[9]

- **Linking national technology ecosystems**: Quad members can also promote their technology ecosystem to speak to each and with like-minded partners. For instance, Indian, Japanese, US and Australian major telecommunication companies, system integrators and operators can converge on a platform or forum to discuss challenges they face in operating their network and equipment.
- **Open Radio Access Network**: Moreover, the Quad must expedite research efforts, commercialise, and secure the O-RAN, which is also important for 6G. Here, the focus should be on creating an O-RAN resilience framework to address cybersecurity and supply chain security concerns. The Quad has already announced plans to work with the government of Palau to deploy O-RAN capabilities.[10]
- **Standard-setting exercise**: For the development of new standards at the International Telecom Union, Quad members must utilise the Quad-plus formula and establish a regional consultative mechanism. A particular emphasis should be on bringing the private sector on board to make it a genuinely multi-stakeholder process. These standards must be based on the principles of security, individual control and rights, integrity and data minimisation. Simultaneously, this process should also emphasise harmonising existing standards, rather than creating overlapping and fragmented standards across different geographies.

The rapidly expanding telecommunications market in the Indo-Pacific offers an opportunity for the Quad partners to deepen their tech engagement. A collaborative Quad effort designed to safeguard telecommunication infrastructure across the region will substantially contribute to tackling China's growing digital trajectory and footprint in the strategically important region.

About the author

Sameer Patil is a Senior Fellow with the Centre for Security, Strategy and Technology at the Observer Research Foundation, India. The views expressed are his own.

About this paper

The ANU National Security College (NSC) is a joint initiative of The Australian National University and the Commonwealth Government. NSC is independent in its activities, research and editorial judgment and does not take institutional positions on policy issues. Accordingly, the authors are solely responsible for the views expressed in this publication, which should not be taken as reflecting the views of any government or organisation. NSC's publications comprise peer-reviewed research and analysis concerning national security issues at the forefront of academic and policy inquiry. This paper has been written for the Quad Tech Network Dialogue, held in September 2023 as part of the Quad Tech Network initiative.

About the Quad Tech Network

The Quad Tech Network (QTN) is an initiative of the NSC, delivered with support from the Australian Government. It aims to establish and deepen academic and official networks linking the Quad nations – Australia, India, Japan, and the United States – in relation to the most pressing technology issues affecting the future security and prosperity of the Indo-Pacific.

Contact

national.security.college@anu.edu.au

nsc.anu.edu.au

NSC_ANU

ANU National Security College

CRICOS Provider #00120C

TEQSA Provider ID: PRV12002 (Australian University)

Notes

[1] A Kumar, "Telcos in APAC set to invest $259 bn on networks by 2030, mostly on 5G: GSMA", *ETTelecom*, 24 July 2023, accessed 24 July 2023, https://telecom.economictimes.indiatimes.com/news/industry/telcos-set-to-invest-259-bn-on-networks-between-by-2030-mostly-on-5g-gsma/102080499

[2] ET Bureau, "India's 5G rollout cost to be highest among 15 emerging nations: study", *The Economic Times*, 26 November 2022, accessed 19 July 2023, https://economictimes.indiatimes.com/industry/telecom/telecom-news/indias-5g-rollout-cost-to-be-highest-among-15-emerging-nations-study/articleshow/95773987.cms

[3] Bevin Fletcher, "Huawei still dominates telecom equipment market", *Fierce Wireless*, 16 December 2021, accessed 19 July 2023, https://www.fiercewireless.com/wireless/huawei-still-dominates-telecom-equipment-market

[4] Blomberg, "Vietnam shuns Huawei as it seeks to build Southeast Asia's first 5G network", *South China Morning Post*, 27 August 2019, accessed 27 July 2023, https://www.scmp.com/news/asia/southeast-asia/article/3024479/vietnam-shuns-huawei-it-seeks-build-aseans-first-5g

[5] Raymond Zhong, "Is Huawei a Security Threat? Vietnam Isn't Taking Any Chances", *The New York Times*, 18 July 2019, https://www.nytimes.com/2019/07/18/technology/huawei-ban-vietnam.html

[6] Ministry of Digital Economy and Society, "Insights on Digitalization of Thailand Industry: Digital Roadmap for Aging Society, Agriculture, and Tourism", Ministry of Digital Economy and Society, February 2017, accessed 19 July 2023, https://www-file.huawei.com/-/media/corporate/pdf/market-trends/thailand_digitalization_whitepaper_en_new.pdf

[7] Cybersecurity and Infrastructure Security Agency, "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices", US Government, 10 June 2022, accessed 19 July 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a

[8] The White House, "Quad Principles on Technology Design, Development, Governance, and Use", US Government, 24 September 2021, accessed 19 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/

[9] Prague 5G Security Conference, "The Prague Proposals", 3 May 2019, accessed 27 August 2023, https://www.praguecybersecurityconference.com/prague-proposals/

[10] The White House, "Quad Leaders' Summit Fact Sheet", 20 May 2023, accessed 18 August 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/