Quad Tech Network QTN Series

THIS CONNECTION IS SECURE: A 5G RISK AND RESILIENCE FRAMEWORK FOR THE QUAD

SEPTEMBER 2021

Authors: Andreas Kuehn and Trisha Ray

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

Andreas Kuehn is a Senior Fellow at the Observer Research Foundation America where he leads research on international cybersecurity cooperation within ORF America's Cyberspace Cooperation Initiative. His work focuses on the new risks and challenges in international security at the intersection of emerging technology, cybersecurity, and technology governance.

Trisha Ray is an Associate Fellow at the Centre for Security, Strategy and Technology at the Observer Research Foundation. Her research focuses on geopolitical and security trends in relation to emerging technologies, AI governance & norms and lethal autonomous weapons systems. Trisha is a member of UNESCO's Information Accessibility Working Group, as well as a Pacific Forum Young Leader. She completed her MA in Security Studies from the Walsh School of Foreign Service at Georgetown University.

Contents

Introduction

5G will be a game changer for the Indo-Pacific, which is home to the most rapidly growing digital economies in the world. The internet economy in Southeast Asia was valued at US$100 billion in 2019, growing at a compound annual growth rate of 33% between 2015-19.[1] India's digital economy alone contributed US$200 billion in economic value.[2] Securing the ICT infrastructure, including 5G networks, that underpins these massive economic and social benefits is critical to economic and national security, especially against the backdrop of growing concerns over the exploitation of 5G vulnerabilities and supply chain dependencies by foreign powers. Yet countries in the region have adopted divergent stances on high-risk vendors, state- versus private-led 5G deployments, and global partnerships. They also vary greatly in their capability and capacity to manage emerging digital technologies and absorb the benefits of the digital transformation, as well as the degree of their economic and political closeness to China. There is a need to develop common frameworks for managing risks and fostering resilience.

The Quad provides an ideal testbed for a shared 5G risk and resilience framework that can be expanded to the broader Indo-Pacific.

In the past three years, there has been a growing global body of research on what constitutes 'technical risk' in the realm of 5G.[3] The Quad countries – Australia, India, Japan, and the United States – have been proactive in identifying and acting upon risks to secure their 5G ecosystems at home and abroad. Security measures have ranged from soft bans to hard blocks implemented through a varying combination of public statements from political leadership, and statutory, regulatory, administrative, and technical measures. These include the US 5G Clean Network initiative under the Trump Administration; Australia's two-pronged trust challenge – external, relating to vendors, as well as internal, relating to consumers reacting to misinformation; Japanese telcos building alliances and consortiums both amongst themselves and in the region; and India's ambitious bid for self-sufficiency.[4]

The 'secure 5G deployment' debate has been steered by concerns about technical security vulnerabilities that, when exploited by state or non-state actors, can put the confidentiality, integrity, and availability of communications networks at risk. In particular, the oligopolistic 5G market, in which Chinese companies hold a large share, has raised concerns among the US and its partners. The Chinese government is perceived as being able to exercise undue influence to coerce Chinese equipment manufacturers under its 2017 National Intelligence Law to provide access to data held by their customers, including foreign network operators, and even shut down 5G networks.[5] These concerns have been amplified by China's ambitions to shape its preferred digital environment through the Digital Silk Road and emerge as a high-tech superpower by 2049, as well as its use of emerging technologies to maintain authoritarian rule with disregard for human rights. The 5G security debate has also come amidst growing US-China geopolitical and trade tensions that led to an increased focus on the susceptibility of technology supply chain dependencies. The COVID-19 pandemic further illustrated the perils of supply chain dependencies, which are susceptible to being weaponised for short-term economic and long-term strategic gains. Similar contentions could become salient as the 5G build-out advances globally.

Given the global nature of innovation, development, manufacturing, and assemblage of emerging digital technologies, the Quad countries cannot effectively manage these challenges individually. When operating globally, businesses and governments need secure, resilient communications channels to ensure mission success (for example, the need for a company to have protected confidential communications when operating abroad; the need for armed forces to have secure communications to "operate through" networks in contested red or grey areas).[6]

A resilient 5G network is one that can withstand sustained cyber-attacks, technical failure, or natural disasters, and continue operating essential services in such circumstances.

A common framework can help Quad countries allocate efforts and resources. At the same time, such a framework must acknowledge that 5G risk assessments may be influenced by geopolitical and national interest considerations, and that Quad countries possess different capabilities and capacities to monitor and act upon risks.

This paper therefore proposes a common risk and resilience framework that includes building the capabilities and resilience to improve recovery and business continuation of 5G networks and associated supply chains. It also provides a set of actionable recommendations to inform future 5G risk and resilience measures.

Taking Stock: Policy Measures by Quad Countries

While Australia, Japan and India have opted for approaches along the spectrum of "a ban in everything but name", the United States has systematically named and excluded Chinese vendors Huawei and ZTE from its 5G communications networks, supplemented by a global campaign to get buy-in from its allies and partners to prevent deployment of Chinese 5G equipment in foreign networks.

Quad countries have effectively banned Chinese telecommunications equipment vendors through a combination of policy and regulatory measures.

Their varying implementations, however, reflect national idiosyncrasies regarding national security and economic interests as well as the ability to manage their relationship with China. The following section compares the approaches Quad countries have taken to secure their 5G deployments.

Blocking High Risk Vendors

The United States explicitly banned Chinese vendors. The May 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain prohibited the acquisition and use of ICT from a foreign adversary that poses an unacceptable risk to critical infrastructure and national security.[7] Additionally, the 2019 National Defense Authorization Act (NDAA) prohibited federal agencies from procuring certain Chinese telecommunications equipment and services, Huawei was put on the Commerce Department's entity list in 2020 due to alleged activities contrary to US national security and foreign policy interests, and the Federal Communications Commission designated Huawei and ZTE as threats to national security in 2021.[8]

The other Quad countries, in contrast, opted for a soft ban. The Australian government was the first mover to bar high risk vendors, implicitly targeting Huawei and ZTE, from its 5G networks in August 2018.[9] Australia's soft ban was preceded by a 2012 decision to block Huawei as a vendor from the national broadband network.[10] Japan was the next country within the Quad to exclude Chinese telecommunications vendors. In December 2018, the government revised its procurement rules with strict supply chain security requirements to effectively ban purchases from Huawei and ZTE, although the two companies were not explicitly mentioned.[11] The most recent addition to this list is India's June 2020 ban, barring state-owned telecom providers from using Chinese equipment by excluding them from planned 5G trials.[12] The Department of Telecommunications' (DoT) list of approved carriers for a six-month 5G trial, Airtel, Reliance Jio, Vodafone and MTNL, have all partnered with Ericsson, Nokia, Samsung or C-DOT, or, in the case of Jio, are conducting trials with indigenous technology.

The decision to exclude Chinese vendors from their national 5G networks build-out can be understood against the backdrop of commonly shared concerns about 5G technical security among the Quad. Importantly, growing geopolitical tensions and profound mistrust towards China, in particular fears over foreign interference due to China's 2017 National Intelligence Law, cyber espionage, intellectual property theft, and undue government subsidies to national champions are important factors to consider.

Each Quad country's decision to exclude vendors however also has its own history, and Beijing's miscalculations on how New Delhi, Tokyo and Canberra would respond to threats of retaliation have played a not-insignificant role. For example, Canberra's decision to bar Chinese vendors was part of a larger effort against covert foreign interference in its politics, started under the Turnbull administration.[13] Acting Minister for Home Affairs Scott Morrison noted in a 2018 press release that, vendors "subject to extrajudicial directions of a foreign government that conflict with Australian law" and that enable "unauthorised access or interference" would not be allowed to participate in Australia's 5G market. Similarly, India's decision to exclude Chinese vendors from its 5G networks came after years of equivocacy,[14] and growing tensions with China following deadly clashes along the Sino-Indian border in the Himalayan Galwan valley provided the final push.

Leveraging Procurement and Security Requirements

Changes in government procurement authorities and policies, in the form of strict cyber and supply chain security requirements, are among the central measures Quad countries have applied to mitigate third-party supply chain risk, especially from Chinese vendors. India's DoT for instance regularly notifies security requirements for TSPs and ISPs,[15] and in March 2021, mandated that public procurement gives preference to "Made in India" cybersecurity products. Japan's updated 2018 procurement guidelines prohibit the purchase of computing and communications equipment and services for government entities deemed to be security risks and require guidance from competent government authorities to mitigate supply chain risk.[16] In the US, the Federal Acquisition Supply Chain Security Act provides the government with new procurement authorities to regulate the purchase of technologies developed or supplied by entities which are subject to obligations to foreign governments, as well as other risk factors regarding their supply chain.

Imposing Carrier Security Obligations

Quad governments also imposed cybersecurity obligations on their telecommunications providers, for example, through regulatory telecommunications and critical infrastructure protection authorities. Australia's 2018 Telecommunications Sector Security Reforms require that TSPs secure their networks and infrastructure from foreign interference. Its 2020 Security Legislation Amendment (Critical Infrastructure) Bill, if passed, would further expand the scope of critical infrastructure, and introduce new cybersecurity obligations for providers. Japan's Ministry of Internal Affairs and Communication imposed new cyber and supply chain security obligations as an operating condition in exchange for free 5G

spectrum allocation. Japanese telecom carriers which used or tested Chinese 5G network equipment announced that they would replace these products moving forward. In India's case, the DoT mandated in March 2021 that licensed TSPs use only "Trusted Products" made by "Trusted Sources", as designated by the National Cyber Security Coordinator.[17] The criteria for "Trusted Sources" were communicated to TSPs and telecom vendors in a meeting from which Huawei and ZTE were reportedly excluded.[18]

Providing Financial Incentives to Industry for Secure 5G Deployments

Japan has taken a unique approach by providing financial incentives for the development of secure 5G. Its 2020 Tax Reform provides corporate tax incentives for 5G technology adoption, if certain government standards, such as safety and reliability, supply stability as well as "openness" (adherence to international standards) are met.[19] Similarly, the Ministry of Economy, Trade and Industry has instituted the "Program for Promoting Investment in Japan to Strengthen Supply Chains". Currently in phase 2, the program will provide subsidies of up to 10 billion yen to companies that take steps to diversify the supply of 5G components, which will also help Japan's industry to strengthen its position in the global 5G ecosystem.[20] The US has also created funds under the 2021 National Defense Authorization Act to support 5G research and promote alternative 5G equipment providers (Innovation Fund) and advance development of trusted communications technologies, strengthen supply chains and promote trusted vendors (Multilateral Telecom Fund) in the US and with foreign partners.[21]

Strengthening International Cooperation

The Quad countries have cooperation mechanisms amongst themselves and other trusted partners. Japan and India for instance signed a Memorandum of Understanding (MoU) on ICT cooperation in January 2021, covering 5G technologies and telecom security, among other issue areas.[22] The two also finalised a cybersecurity cooperation agreement for 5G, Internet of Things, and artificial intelligence during a meeting of their external affairs ministers in October 2020.[23] The four countries also collaborated for the Quad Open RAN Forum in 2021, with key industry and government stakeholders participating in discussions over two days.[24]

5G Policy Responses by Quad Countries

The table below outlines policy actions of Quad countries in the 5G space. This is not a comprehensive table, but provides a quick summary of the range of actions and actors in this area:

	Australia	India	Japan	United States
Ban on Chinese Vendors	Yes (Implicit)	Yes (Implicit)	Yes (Implicit)	Yes
National Strategy	5G: Enabling the Future Economy	Making India 5G Ready	Beyond 5G Promoting Strategy	National Strategy to Secure 5G
Supply Chain Measures	Critical Technology Supply Chain Principles (Draft)[25]	Trusted Products and Trusted Sources Framework (2021)[26]	Program for Promoting Investment in Japan to Strengthen Supply Chains[27] Tax Reform (2020)[28]	Federal Acquisition Supply Chain Security Act
Guidelines for Telecom Service Providers	Security Legislation Amendment (Critical Infrastructure) Bill 2020	Trusted Products and Trusted Sources Framework (2021)[29]	Notified as part of the spectrum allocation policy (2019)[30]	Secure and Trusted Communications Networks Act (2019)
5G Standards	3GPP	3GPP 5Gi[32]	3GPP	3GPP
Relevant Agencies/ Bodies	Australian Signals Directorate Australian Communications and Media Authority, Department of Communications and the Arts	Department of Telecommunications, Ministry of Electronics and Information Technology National Cybersecurity Coordinator Telecom Regulatory Authority of India (TRAI)	Ministry of Internal Affairs and Communications National Center of Incident Readiness and Strategy for Cybersecurity	Cybersecurity & Infrastructure Security Agency[33] Federal Communications Commission Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector[34]
TSPs Ownership[35]	Private	Private and state-owned	Private and state-controlled	Private

5G Risk and Resilience

The actions taken by Quad countries indicate that a range of technical, organisational, and policy measures are necessary to effectively mitigate 5G technology, network deployment, and global supply chain security risks. A common view of 5G security risks and measures to strengthen security assurances, transparency, and accountability among Quad countries is therefore an important foundation to a shared risk and resilience framework. Each measure needs to be assessed on its merits and the contribution it makes to security and resilience over the long-term.[36]

The abilities of governments to mandate 5G security requirements depends on first, the capability and capacity of authorities to intervene and regulate the communications industry; and second, their ability to leverage international alliances or agreements to put forward a joint 5G security strategy.

While the 5G security discussion has largely been framed in terms of national security, strict measures such as bans may conflict with commercial and trade interests, as well as national targets for digital growth. They tend to be also only short-term fixes and could have dampening effects on innovation and cybersecurity in the long run, which remain understudied. A more holistic national interest approach, which considers security, economic and social factors, is required to strengthen risk and resilience of 5G networks.

The following is a risk and resilience framework for Quad countries that can be extended to the broader Indo-Pacific. The framework identifies three priority risk areas, which if addressed, provide a comprehensive strategy to securing country 5G networks:

- ***Technical Risk***, to address risk from 5G architecture and protocols.
- ***Supply Chain and Connectedness Risk***, to address risk from supply chain disruptions due to natural and man-made causes, including conflict, but also geopolitical pressures, complex supply chain interdependencies, and national powers to control national suppliers.
- ***Capability and Capacity Risk***, to address insufficient institutional capability and capacity, including in terms of expertise, institutional relationships, and personnel, to monitor and manage 5G security risks.

Technical Risk

5G security challenges identified in existing literature centre on threats relating to each of the three 'planes' of telecommunications architecture: compromised *user plane* integrity; added complexity in the 5G *control plane*; and security of the *management plane*.[37] For example, the large number of endpoints – including Internet of Things devices – could result in sudden spikes in network traffic. Signalling storms – generated by malware of apps – can similarly collapse the entire network. 5G roaming may also be difficult to secure if user security parameters are not updated when switching from one operator to another.[38]

In 5G, the distinction between the "core" and the "edge" networks has blurred. With edge computing, some core functions are moved to the edge of the network, closer to the end-user, enabling low latency by reducing the time it takes for endpoints to communicate with the server.[39] Therefore, policy measures to restrict untrusted vendors and technologies from the core in previous generations of communications are no longer effective in the case of 5G. Vulnerabilities and exploits in 5G products – either accidental or deliberate in nature – undermine the security of 5G communications. Vulnerabilities in previous generations of wireless technologies can also be inherited in the case of non-standalone (NSA) 5G architectures.[40] However, standalone (SA) 5G architecture may comprise yet unknown vulnerabilities.[41] Emerging solutions come with their own risks. With many countries rolling out NSA 5G networks, there is a risk of creating dependencies on a single vendor that could become long-term vulnerabilities. Open Radio Access Network (RAN) has been hailed as a way of avoiding this lock-in, by enabling interoperability and vendor diversity within a single network.[42] However, Open RAN's flexibility may create its own security vulnerabilities, as the patchwork of components and interfaces means that they may be more vulnerable than existing RAN architectures.[43]

All 5G technology choices are, therefore, accompanied by their set of technical risks. A range of technical and risk assessments about network architecture, protocols, and components, based on international standards and industry best practice, must inform policy and vendor choices as part of a broader 5G security strategy.

Supply Chain and Connectedness Risk

Global 5G supply chains are inherently a source of risk. Components for 5G networking technologies are designed, developed, manufactured, assembled, and distributed around the globe, with hundreds of vendors and subcontractors that deliver their components and services to 5G equipment manufacturers. The complexity of supply networks makes it challenging and costly to track and mitigate third-party risk from vendors and contractors, particularly when they are based in foreign and/or adversarial states. Hence, the ability to maintain oversight of third-party 5G equipment vendors and service providers is limited. In particular, tainted, counterfeit, and inherited software and hardware components in 5G technologies are difficult to identify and can introduce security vulnerabilities or hidden functions that threat actors can exploit.[44]

This risk is not limited to "untrusted vendors" or "untrusted products". Even the security of well-engineered, trustworthy components of trusted vendors can be compromised.[45] While some governments have banned 5G products manufactured by companies like Huawei and ZTE – that are subject to the laws of and potential interference by adversarial regimes – such a vendor-based approach is neither robust nor tenable. If the labels of "trusted solutions" and "trusted partners" are not based on transparent, international standards, it bears the risk that the security baseline for 5G is not sufficiently raised for all 5G manufacturers and operators. The breach of a "trusted supplier" can have a significant, potentially devastating impact. The 2020 SolarWinds hack demonstrated that point, when a "trusted supplier" became the target of a supply chain attack in which more than 18,000 customers download a malicious software update.,[46]

Bottlenecks in supply chains can result in disruptions or reduced supply. This may be caused by natural disasters or man-made conflict at a particular link or location in the supply chain, a surge in global demand of 5G products, or even unrelated products that use the same component in large numbers or rely on the same production capacity (e.g., semiconductor shortage across all sectors due to a surge in demand). Even a breakdown of the underlying logistics networks can lead to costly disruptions, illustrated by the 2021 Suez Canal blockage caused by a giant container ship.[47]

Finally, some states have sought to weaponise the 5G supply chain's complex interdependencies for strategic gains, for example in trade conflicts to exert pressure on trading partners.[48] A growing focus on innovation and industrial policy in liberal economies reflects concerns that current supply chain structures leave their markets vulnerable to the availability of critical ICT components. COVID-19 has also highlighted a growing trend toward protectionism. It is too early to tell whether similar dynamics will be at play, in which countries will restrict the sale of 5G components. Non-tariff barriers, such as export licenses, internal taxes, new certification and product quality requirements, as well as industrial policies and onshoring of critical goods could affect the availability of secure 5G components and delay the buildout of 5G networks globally.[49] The absence of a common view of 5G supply chain risk and response measures means states may introduce arbitrary restrictions that could dampen innovation and inhibit the development of diverse sources of globally competitive, high-quality 5G components.

Capability and Capacity Risk

While 5G brings advanced security functions (e.g., mutual authentication capabilities and enhanced subscriber identity protection) to the next generation of wireless communications networks, there remains a range of cybersecurity and policy risks to the deployment of 5G networks.[50] To manage and mitigate these risks effectively, capability and capacity across a range of government and industry areas are required, including institutions, infrastructure, resources, and personnel.

Deployment of 5G networks is not limited to traditional telecommunications service operators. Private entities, corporations, and universities can operate their own 5G networks and while large telecommunications service providers (TSPs) are able to follow industry best practices in securing their networks, smaller players may not have the operational maturity or resources to do so. [51]

Building capability and capacity to address 5G security threats[52] requires institutional arrangements similar to a national sector-specific Computer Emergency Response Teams (CERTs) as well as mechanisms and personnel to monitor networks for intrusions (e.g., the Einstein and Continuous Diagnostics and Mitigation programs in the US federal government).[53] Cooperation between government entities, TSPs, and industry is necessary to build and maintain these risk capabilities and capacities, in order to develop and manage baseline security controls, incident response plans, and joint exercises, for example. Additionally, network operators need to respond to 5G security incidents in close cooperation with industry partners and governments and share threat intelligence in a timely manner. Legal provisions to protect critical infrastructure, dedicated funds, or tax incentives, for instance, can be used to establish specific capabilities and capacities.

It is also worth noting that institutional capacity to address risks to 5G networks also requires political capital and diplomatic finesse. Monitoring and assessment must also be complemented by collaboration with trusted international partners, which requires the establishment of the necessary institutional "bridges", such as CERT-CERT cooperation, and cross-pollination of cybersecurity standards for 5G deployments at the technological level, as well as statecraft and cyber diplomacy at the international level. Coalescing around clear definitions of risk helps generate and sustain the political momentum needed to support technical and institutional capacity building. The following recommendations therefore propose a series of collaborative measures based on the three priority risk areas discussed in this section.

Recommendations

To address risk and resilience in the 5G build-up, a comprehensive framework is needed that can provide an objective and transparent basis for managing and mitigating threats and risks including those arising from certain types of equipment and suppliers.[54] Measures for which the Quad can take joint actions towards a shared risk and resilience framework are condensed into five central recommendations below. The three priority risk areas should be addressed through these recommendations. Quad countries' experiences and priorities will determine how the risk areas are weighted which is likely to evolve over time as the implementation of the recommendations progresses.[55]

Given that the Quad is increasingly aligned on the issue of common technology standards based on "shared interests and values",[56] they should:

1. ***Conduct joint risk assessments*** *of 5G supply chains, including scenarios for common threat vectors and define mitigation measures for vendors and operators; and*

2. ***Define common standards*** *for what "trustworthy" behaviour should look like for 5G vendors and equipment providers.*

At present, the four countries have their own individual sets of efforts,[57] including India's list of trusted vendors, under the supervision of the National Cybersecurity Coordinator;[58] Australia's review of existing requirements for telecommunications supply chains, under the Parliamentary Joint Committee on Intelligence and Security,[59] and the US' threat review under the Enduring Security Framework, part of the Critical Infrastructure Partnership Advisory Council.[60] Inconsistent standards create compliance burdens for vendors, and can dampen efforts to build internationally competitive alternatives. Therefore, India, Australia, US, and Japan should identify nodal agencies for a series of meetings to identify common criteria for trusted vendors, standards for network operators as well as threat scenarios. These meetings could lay out a series of voluntary measures, such as those laid out in the European Union's 5G cybersecurity toolbox.[61] Quad countries should also closely work with their respective national 5G industry players to implement recommendations 1 and 2. The US is home to leading chipmakers like Qualcomm, India is fostering its indigenous 5G technology development through Reliance Jio, and Japan has two domestic 5G equipment vendors – NEC and Fujitsu – which primarily serve its national market but have global ambitions.[62] The common standards that emerge from this process could then be extended to other like-minded states, under the 5G Resilience Alliance proposed in recommendation five in this section.

3. ***Establish a 5G Agenda*** *for the Quad Critical and Emerging Technologies Working Group.*

The newly-established Quad Critical and Emerging Technologies Working Group is one forum to develop shared practices around 5G.[63] Measures that the Working Group could encourage include sharing of 5G threat information, developing joint security requirements for 5G procurement, adapting a joint testing and evaluation scheme for 5G security (e.g., Network Equipment Security Assurance Scheme),[64] establish reciprocity for certification, coordinating standard setting activities, conducting joint 5G security exercises, and developing joint research agendas for 5G security and resilience.

4. ***Coordinate policy priorities*** *in international forums on ICT security and standard setting*

Irrespective of the capability and capacity to respond to 5G security risks, telecommunications networks will continue to be hotbeds for foreign intelligence activities due to the massive amount of data flowing through these networks. Technical security measures may raise the attacker's costs but will not deter sophisticated state actors.[65] Ultimately, stronger international cyber norms, capacity building efforts, and confidence-building measures built through the United Nations and regional security and economic organisations are needed to strengthen international norms for responsible behaviour in cyberspace and ensure the integrity of 5G infrastructure and supply chains.

For example, the 2021 report of the Group of Governmental Experts on Advancing responsible State Behaviour in Cyberspace reaffirmed an earlier 2015 supply chain security norm, declaring that "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."[67] Tampering with 5G network equipment that would systematically subvert security and substantially impair the stability of cyberspace is also strongly discouraged under the Global Commission on the Stability of Cyberspace's "Norm to Avoid Tampering".[68] Furthermore, technical 5G standards development in the ITU as well as 3GPP, GSMA, O-RAN, and other relevant 5G standard setting organisations and industry associations deserve close attention. Competent national authorities in the Quad should coordinate their positions and efforts. The Quad countries should develop a complementary, if not shared, agenda for such international forums.

5. ***Build a Multistakeholder 5G Resilience Alliance***

Actions to build a resilient global 5G ecosystem cannot be restricted to the Quad alone. In this vein, a multistakeholder 5G alliance with a mission to promote objective and transparent standards, with participation from key industry actors, as well as cybersecurity and other relevant experts would be a valuable addition to the ecosystem. The alliance need not duplicate efforts already underway elsewhere but rather leverage existing relations and agreements within and beyond the Quad such as the 2020 Japan-India agreement on ICT cooperation, and the 2020 India-UK 5G MoU, for instance.

Taking a multistakeholder approach, the 5G resilience alliance should not limit its activities to state-centric actions but rather develop security and resilience measures relevant to and in close cooperation with organisations within the ICT industry and the wider ICT ecosystem. Some possible measures at different levels are:

First, ***organisations*** that buy and operate 5G equipment should assess vendor third-party risk and their capacity to manage risk. This is to determine buyers' risk-informed 5G procurement requirements, which should make use of internationally accepted standards and best practice security controls. Buyers may require vendors to follow standards for secure development, ensure that services and software are delivered in secure configuration by default, and adhere to best practices for security vulnerability management.

Second, requirements for ***industry***, applicable to all 5G buyers and vendors, can be established through market-driven collective purchasing power. Tax incentives or dedicated funds could be leveraged to that end. Assurance, transparency, and accountability measures across the supply chain should be used to raise the security baseline for all industry participants. For example, transparency requirements for vendors to disclose their supply chain risk practices, including how they manage their relationships with subcontractors and suppliers, would provide insights into supply chain dependencies and potential threats across industry.

Third, as the ***ICT ecosystem*** transcends national borders, measures that benefit national as well as global 5G deployments are essential. A 5G alliance could start the work towards establishing regional transparency and testing centres for code inspection and 5G conformance programs. Such centralised functions, including agreed-upon testing protocols and certification schemes among Quad countries, would not only allow for cost-efficient testing and one-time accreditation and verification but also help shorten the 5G build-out timeline.

Endnotes

1. Google, Temasek Holdings, Bain & Company, "e-Conomy SEA 2019: Swipe up and to the Right: Southeast Asia's $100 Billion Internet Economy" (2019) https://www.blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf.
2. "India's Trillion Dollar Digital Opportunity", *Ministry of Electronics and Information Technology, Government of India*, February 2019. https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.
3. Security Risk Assessment for 5G Networks: National Perspective, https://ieeexplore.ieee.org/document/9170263; Security situation assessment for massive MIMO systems for 5G communications, https://www.sciencedirect.com/science/article/abs/pii/S0167739X19300731; Overview of 5G Security Challenges and Solutions, https://ieeexplore.ieee.org/document/8334918
4. Indo-Pacific 5G survey: Connections and conflict, https://www.orfonline.org/wp-content/uploads/2021/04/Indo-Pacific-Survey.pdf
5. China could have ordered Huawei to shut down Australia's 5G, https://www.smh.com.au/politics/federal/china-could-have-ordered-huawei-to-shut-down-australia-s-5g-20210520-p57trn.html
6. Cyberspace Operations, Joint Publication 3-12, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf; DOD 5G Strategy Implementation Plan, https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf
7. Executive Order on Securing the Information and Communications Technology and Services Supply Chain (Executive Order 13873), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain
8. 2019 National Defense Authorization Act (NDAA), Section 889, https://www.congress.gov/bill/115th-congress/house-bill/5515/text ; FCC Releases List of Equipment & Services That Pose Security Threat. March 12, 2021.
9. Government provides 5G security guidance to Australian carriers, *Parliament of Australia*, August 23, 2018; "Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018" https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf
10. David Ramli and Paul Smith, "China's ire deepens over Huawei NBN ban", *Australian Financial Review*, March 29, 2012. https://www.afr.com/politics/federal/china-s-ire-deepens-over-huawei-nbn-ban-20120329-j36k5
11. Japan government to halt buying Huawei, ZTE equipment: sources, https://www.reuters.com/article/us-japan-china-huawei-idU.S.KBN1O600X
12. "Bid to keep Huawei out of 5G trials", *Telegraph*, June 6, 2020. https://www.telegraphindia.com/business/bid-to-keep-huawei-out-of-5g-trials/cid/1783807
13. Tom Westbrook, "Australia, citing concerns over China, cracks down on foreign political influence", *Reuters*, December 5, 2017. https://www.reuters.com/article/us-australia-politics-foreign/australia-citing-concerns-over-china-cracks-down-on-foreign-political-influence-idU.S.KBN1DZ0CN
14. Anandita Singh Mankotia, "India unlikely to ban Huawei's 5G equipment", Economic Times, December 21, 2018. https://economictimes.indiatimes.com/industry/telecom/india-unlikely-to-ban-huaweis-5g-equipment/articleshow/67186519.cms?
15. "Circulars: Security", *Department of Telecommunications*. https://dot.gov.in/circular-and-notifications/2688
16. "IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ等について", *The National Center of Incident Readiness and Strategy for Cybersecurity*, December 2018. https://www.nisc.go.jp/conference/cs/dai21/pdf/21shiryou05.pdf
17. File No. 20-1236/2021-AS-1, Ministry of Communication, Department of Telecommunications, Access Services Wing, March 30, 2021. https://dot.gov.in/sites/default/files/2021%2003%2031%20UL%20Proc%20AS-I.pdf?download=1
18. Sonali Rautham "NCSC Finalizes the Criteria for Identifying Trusted Vendors: Details", *Telecom Talk*, March 29, 2021. https://telecomtalk.info/ncsc-finalizes-criteria-trusted-vendors/347969/
19. "令和２年度（２０２０年度） 経済産業関係 税制改正について"https://www.meti.go.jp/main/yosan/yosan_fy2020/pdf/zeiseikaisei.pdf
20. "サプライチェーン対策のための国内投資促進事業費補助金 2次公募につい", *Ministry of Economy*, Trade and Industry, Updated March 12, 2021. https://www.meti.go.jp/covid-19/supplychain/index.html; and "サプライチェーン対策のための 国内投資促進事業費補助金 概要説明資料（２次公募）", *Ministry of Economy, Trade and Industry*, March 3, 2021. https://www.meti.go.jp/covid-19/supplychain/pdf/summary.pdf
21. H.R.6395 - William M. Thornberry National Defense Authorization Act for Fiscal Year 2021. https://www.congress.gov/bill/116th-congress/house-bill/6395
22. "India and Japan Sign MoU to Enhance Cooperation in the Field of ICT", *Press Information Bureau*, January 15, 2021. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1688812
23. "Signing of the Memorandum of Cooperation in the field of Cybersecurity between India and Japan", *Press Information Bureau*, October 7, 2020. https://pib.gov.in/PressReleasePage.aspx?PRID=1662334
24. The Quad Open RAN Forum, https://www.openranpolicy.org/the-quad-open-ran-forum/
25. Critical Technology Supply Chain Principles, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/critical-technology-supply-chain-principles
26. "Launch of the 'Trusted Telecom Portal' for implementation of the National Security Directive on Telecommunication Sector", *Department of Telecommunications*, June 15, 2021. https://dot.gov.in/sites/default/files/Brief%20on%20launch%20of%20Trusted%20Telecom%20Portal-1.pdf?download=1

27. "サプライチェーン対策のための国内投資促進事業費補助金 2次公募につい", Ministry of Economy, Trade and Industry, Updated March 12, 2021. https://www.meti.go.jp/covid-19/supplychain/index.html; "サプライチェーン対策のための 国内投資促進事業費補助金 概要説明資料（2次公募）", *Ministry of Economy, Trade and Industry*, March 3, 2021. https://www.meti.go.jp/covid-19/supplychain/pdf/summary.pdf

28. Japan approves bill to help firms develop 5G and drone technologies, https://www.japantimes.co.jp/news/2020/02/18/business/tech/5g-drone/; "令和2年度（2020年度）経済産業関係 税制改正について", p. 13, https://www.meti.go.jp/main/yosan/yosan_fy2020/pdf/zeiseikaisei.pdf

29. "Launch of the 'Trusted Telecom Portal' for implementation of the National Security Directive on Telecommunication Sector", *Department of Telecommunications*, June 15, 2021. https://dot.gov.in/sites/default/files/Brief%20on%20launch%20of%20Trusted%20Telecom%20Portal-1.pdf?download=1

30. "第5世代移動通信システム（5G）の導入のための 特定基地局の開設計画の認定（概要）", April 31, 2019. p. 15 https://www.soumu.go.jp/main_content/000613734.pdf

31. H.R.4998 - Secure and Trusted Communications Networks Act of 2019. https://www.congress.gov/bill/116th-congress/house-bill/4998

32. https://thewire.in/tech/what-should-india-hope-to-get-out-of-its-5gi-standard-experiment

33. Note that the U.S. 2021 National Strategy to Secure 5G Implementation Plan lists 38 departments, agencies, and other federal entities. The lead entities are the National Economic Council and National Security Council.

34. Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, April 4, 2020. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-establishing-committee-assessment-foreign-participation-united-states-telecommunications-services-sector/

35. OECD Communications Outlook 2013, *OECD*, July 11, 2013. https://www.oecd.org/sti/broadband/oecd-communications-outlook-19991460.htm. See table Table 2.6. Government ownership of public telecommunication network operators, https://www.oecd.org/sti/broadband/2-6.pdf. Note that also restrictions for foreign ownership stakes apply.

36. Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk, https://www.eastwest.ngo/technationalism

37. *Data plane:* Carries all network user traffic and data packets; *Management plane:* The management plane of a networking device is the element within a system that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system; *Control plane:* Responsible for configuring how data is forwarded. "User Plane", Dialogic https://www.dialogic.com/glossary/user-plane; Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage et al, "Overview of 5G Security Challenges and Solutions", *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, MARCH 2018, doi: 10.1109/MCOMSTD.2018.1700063. https://ieeexplore.ieee.org/document/8334918

38. Jim Hodges, "Securing 5G Networks: Addressing Control Plane Challenges ", *5GExchange*, April 12, 2019. https://www.the5gexchange.com/author.asp?section_id=743&doc_id=751196

39. "EDGE VS. CORE - AN INCREASINGLY LESS PRONOUNCED DISTINCTION IN 5G NETWORKS", *Cybersecurity and Infrastructure Security Agency* (2020) https://www.cisa.gov/sites/default/files/publications/5g_edge-core-computing_508_1.pdf

40. NSA 5G rollouts make use of existing 4G infrastructure. Hannes Ekström, "Non-standalone and Standalone: two standards-based paths to 5G ", Ericsson, July 11, 2019. https://www.ericsson.com/en/blog/2019/7/standalone-and-non-standalone-5g-nr-two-5g-tracks

41. 5G standalone networks may have more vulnerabilities than you think, *TechRepublic* https://www.techrepublic.com/article/5g-standalone-networks-may-have-more-vulnerabilities-than-you-think

42. "What Is Open RAN (Radio Access Network)?", *sdx central*, February 1, 2021. https://www.sdxcentral.com/5g/ran/definitions/what-is-open-ran-radio-access-network/

43. Beryl Thomas, "Why Germany's investment in Open RAN will not solve its 5G problem", *ECFR*, April 6, 2021. https://ecfr.eu/article/why-germanys-investment-in-open-ran-will-not-solve-its-5g-problem/

44. NIST is developing technology that can detect corrupted hardware before it is put in use, see: A measurement-based approach to 5G supply chain security, https://www.nist.gov/programs-projects/measurement-based-approach-5g-supply-chain-security

45. SolarWinds, the vendor of the compromised SolarWinds Orion Platform in the Sunburst hack, was a "trusted vendor," After SolarWinds, the U.S. can trust no one, https://fortune.com/2021/01/29/solarwinds-cybersecurity-zero-trust-national-security-supply-chain-risk-vendors-clean-network

46. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor", *FireEye*, December 13, 2020. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

47. Suez Canal blockage could cost $6 billion to $10 billion in lost trade - Allianz, https://www.reuters.com/article/us-egypt-suezcanal-ship-costs/suez-canal-blockage-could-cost-6-billion-to-10-billion-in-lost-trade-allianz-idU.S.KBN2BI261

48. "China May Ban Rare Earth Tech Exports on Security Concerns", *Bloomberg*, February 19, 2021. https://www.bloomberg.com/news/articles/2021-02-19/china-may-ban-rare-earth-technology-exports-on-security-concerns; Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies, https://web.archive.org/web/20200517021459/https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts

49. Seul Lee and Divya Prabhakar, "COVID-19 Non-Tariff Measures: The Good and the Bad, through a Sustainable Development Lens ", *UNCTAD*, Research Paper No. 60, UNCTAD/SER.RP/2021/3, February 2021. https://unctad.org/system/files/official-document/ser-rp-2021d3_en.pdf

50. Securing the 5G Era, https://www.gsma.com/security/securing-the-5g-era/

51. 5G: The outsourced elephant in the room, https://berthub.eu/articles/posts/5g-elephant-in-the-room/

52. 5G Cyber Security: A Risk-Management Approach, https://rusi.org/sites/default/files/20200602_5g_cyber_security_final_web_copy.pdf

53. Einstein on the Breach: Surveillance Technology, Cybersecurity Organizational Change, https://econinfosec.org/archive/weis2013/papers/MuellerKuehnWEIS2013.pdf

54. Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk, https://www.eastwest.ngo/technationalism

55. For example, depending on the need of the Quad, recommendation 1 could emphasize technical risk and/or supply chain risk but should address capability and capacity risk. Addressing capability and capacity is of overall importance as it speaks to the institutional, resource, and otherwise foundational preconditions to manage technical and political 5G risk.

56. "Quad Critical and Emerging Technology Working Group", April 16, 2021. https://www.internationalcybertech.gov.au/node/137

57. The Japanese government issued a set of guidelines for public procurement of ICT infrastructure, as well as a system of tax incentives to service providers for secure 5G infrastructure. See: "IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ等について", *National Center of Incident Readiness and Strategy for Cybersecurity*, December 2018. https://www.nisc.go.jp/conference/cs/dai21/pdf/21shiryou05.pdf

58. File No. 20-1236/2021-AS-1, Ministry of Communication, Department of Telecommunications, Access Services Wing, March 30, 2021. https://dot.gov.in/sites/default/files/2021%2003%2031%20UL%20Proc%20AS-I.pdf?download=1

59. "Australian Government response to the House of Representatives Standing Committee on Communications and the Arts: 'The Next Gen Future'", Department of Infrastructure, Transport, Regional Development and Communication of the Government of Australia, November 2020. https://www.infrastructure.gov.au/department/ips/government_responses/government-response-next-gen-future.aspx

60. ""Potential Threat Vectors to 5G Infrastructure", May 2021. https://media.defense.gov/2021/May/10/2002637751/-1/-1/0/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF

61. Cybersecurity of 5G networks - E.U. Toolbox of risk mitigating measures, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

62. "Handed a 5G Lifeline by Trump, Japan Races to Catch Up to Huawei". *Bloomberg*, December 10, 2020. https://www.bloomberg.com/news/articles/2020-12-10/handed-a-5g-lifeline-by-trump-japan-races-to-catch-up-to-huawei

63. Quad Critical and Emerging Technology Working Group, https://www.internationalcybertech.gov.au/node/137

64. Network Equipment Security Assurance Scheme (NESAS), https://www.gsma.com/security/network-equipment-security-assurance-scheme/

65. Disrupting Nation State Hackers, https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce

66. Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

67. Advancing Cyber Stability, https://cyberstability.org/report/

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