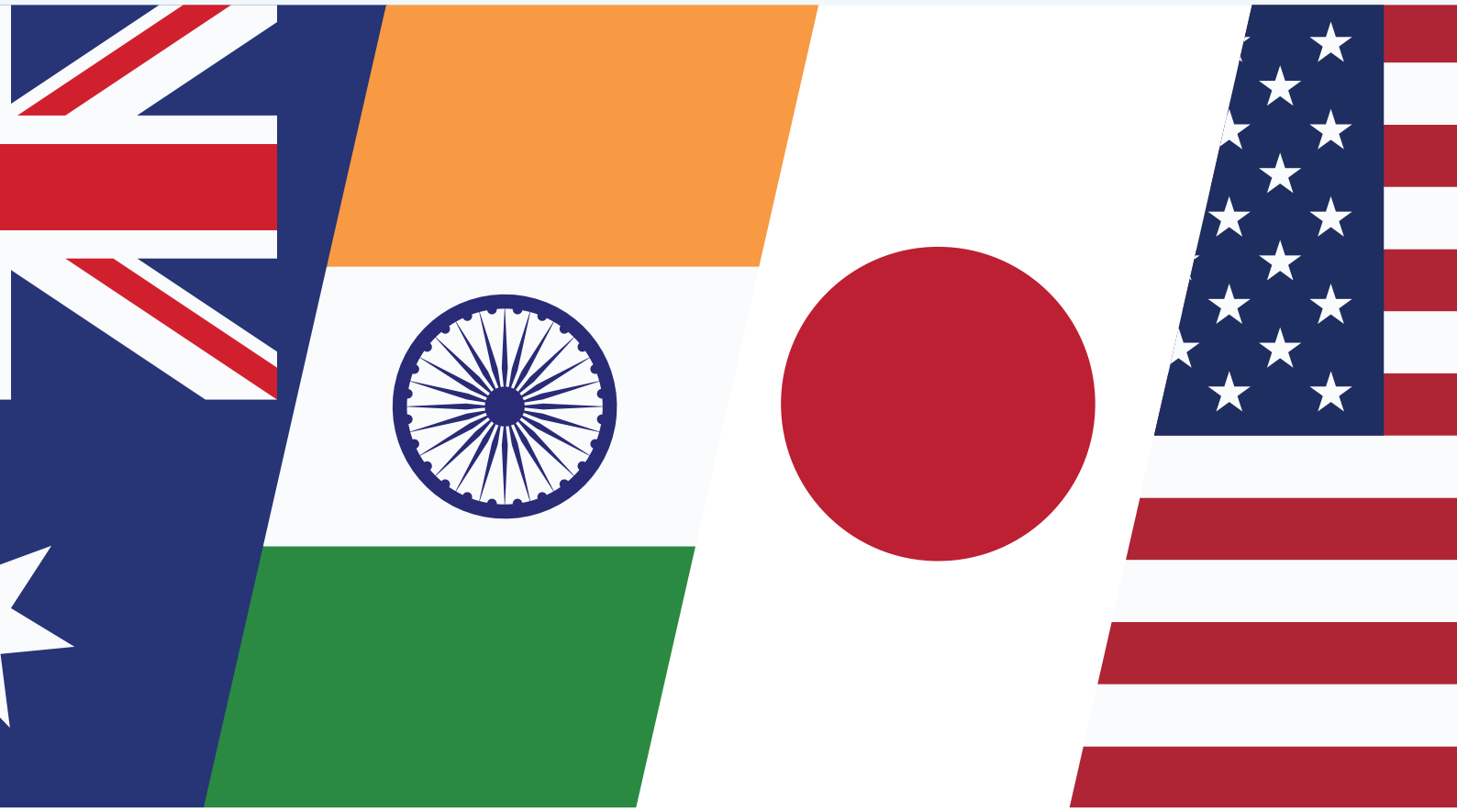
Quad Tech Network QTN Series

NETWORKED: TECHNO–DEMOCRATIC STATECRAFT FOR AUSTRALIA AND THE QUAD

FEBRUARY 2021

Author: Martijn Rasser

Series Editors: Katherine Mansted and Rory Medcalf



Australian National University

Center for a New American Security

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

ORF

About the Quad Tech Network Series

The Quad Tech Network (QTN) is an Australian Government initiative to promote regional Track 2 research and public dialogue on cyber and critical technology issues.

This paper is part of a series of papers by universities and think tanks 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).

The QTN series offers analysis and recommendations on shared challenges facing Australia and Indo-Pacific partners across four themes:

- international peace and security
- connectivity and regional resilience
- human rights and ethics, and
- national security.

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*).

Katherine Mansted is the Senior Adviser for Public Policy at the National Security College at The Australian National University, and a non-resident fellow at the Alliance for Securing Democracy at the German Marshall Fund of the United States. She regularly writes and presents to government and public audiences on technology and security policy. Ms Mansted holds a Master in Public Policy from the Harvard Kennedy School of Government, and a first-class degree in law and international relations.

This is a version of a report first published by the Center for a New American Security (CNAS) at https://www.cnas.org/publications/reports/networked-techno-democratic-statecraft-for-australia-and-the-quad

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.crawford.anu.edu.au

Cover design and layout by Black Bear Creative.

About the Author

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.

About The Center for a New American Security

The Center for a New American Security (CNAS) is an independent, bipartisan, nonprofit organization that develops strong, pragmatic, and principled national security and defense policies. Based in Washington D.C., CNAS engages policymakers, experts, and the public with innovative, fact-based research, ideas, and analysis to shape and elevate the national security debate. CNAS performs groundbreaking research and analysis to shape and elevate the national security and foreign policy debate in Washington and beyond. Our dynamic research agenda is designed to shape the choices of leaders in the U.S. government, the private sector, and society to advance U.S. interests and strategy.

For more information, please visit https://www.cnas.org.

Acknowledgments

The author thanks Kara Frederick, Elsa Kania, Megan Lamberth, Katherine Mansted, Rory Medcalf and Paul Scharre for their thoughtful feedback, suggestions and substantive contributions.

Thank you to CNAS colleagues Maura McCarthy and Melody Cook for their role in the review, production, and design of this report. Finally, thank you to JJ Zeng and Ainikki Riikonen for their assistance in finalizing the report.

Contents

Executive Summary

A new era looms. The fallout of the COVID-19 crisis is the accelerant for an array of trends causing remarkable volatility in geopolitics. An increasingly assertive and revisionist China and inconsistent leadership on the global stage by the United States are leading countries around to the world to reconsider and recalibrate their stances. Concerns over trade, supply chains, and economic dependencies have taken on new meaning and urgency. The tension between liberal democratic values and authoritarian priorities is growing as illiberal values proliferate more readily. Handwringing over the erosion of the rules-based order is more acute as Beijing and Moscow continue to chip away at the integrity of multilateral institutions.

World leaders recognize that a strategic competition is underway and that the geopolitical context in which it will play out is morphing. Many of these leaders also understand that technology is at the core of this competition. Technology-leading countries will drive the digital economy, gaining political power and military strength, and shaping the rules for technology use. Illiberal states see both a pathway to cementing their rule and opportunities to discredit democracies. Liberal democracies see a means to shore up the rules-based order and to hold creeping authoritarianism at bay.

Australia's leaders are updating the country's strategic posture in response. The new Australian defense strategy is a major reorientation within the Indo-Pacific; the updated national cyber strategy recognizes the rapidly evolving threats and the fundamental importance of ensuring the security and resilience of the country's networks. Meanwhile, the Australian Department of Foreign Affairs and Trade is pursuing novel international avenues to secure its technological future by establishing the Quad Tech Network, a Track 2 initiative between think tanks and academic institutions to foster technology policy collaboration among the member countries of the Quad: Australia, India, Japan, and the United States. This initiative is part of a broader effort to support and complement the forthcoming Cyber and Critical Technology International Engagement Strategy. This multilateral approach is key: the alliances and partnerships among the world's democracies are a strategic advantage that illiberal states come nowhere close to matching.

This report lays out a blueprint for Quad technology policy. After setting the scene of the current technological and geopolitical landscape and the context in which the group would operate, the report presents a policymaking framework called techno-democratic statecraft. This framework entails seven qualities that should guide Australia's 21st-century technology policy. The document further details values and principles Australia should promote and how Australia should pursue its interests internationally, via the Quad and beyond.

Much of this document is devoted to detailed policy recommendations that apply techno-democratic statecraft principles. These recommendations come in two categories: (1) opportunities for Australian leadership in the Quad Tech Network, and (2) opportunities to build Australia's tech capacity. Together, the framework and recommendations constitute an actionable plan for an affirmative and proactive multilateral technology pact rooted in shared democratic values.

Summary of Recommendations

Australia, with its strong bilateral ties to other Quad member states and as the smallest Quad economy, is well positioned to lead the Quad to achieve important technology policy objectives and simultaneously promote collaborative efforts that would boost its technological capabilities. These recommendations are crafted in the context of techno-democratic statecraft, a comprehensive approach to technology policy with proactive and practical multilateralism as a central feature. The specific technology policy areas capitalize on collective Quad strengths and consider capabilities most relevant for the technology competition that will play out over the next decades.

To create and lead a burgeoning Quad Tech Network, Australia's leaders should advocate for collaborative approaches that:

- ***Bolster cybersecurity.*** Focus in the near term on pursuing multilateral engagement for setting norms that promote a free and open cyberspace; crafting multilateral responses to nefarious cyber activity in accordance with international law; and spearheading a shared monitoring and cyber- intrusion remediation capability.
- ***Secure supply chains.*** Take a broader approach by including the United States in the Supply Chain Resilience Initiative and expanding diversification efforts by drawing in other countries and groups such as ASEAN.
- ***Pursue 5G and Beyond 5G technologies.*** Lay the foundation for a secure communications infrastructure future by partnering with Japan to promote open interfaces and modular architecture as the best way forward on 5G architecture for the Quad and its allies and partners, and by leading the Quad to execute a strategic plan for collaborative research and development (R&D) and deployment of beyond-5G technologies.
- ***Close the digital divide.*** Provide a positive alternative to Chinese digital entanglements in the Indo-Pacific by creating a standing multilateral mechanism to fund secure and fair digital infrastructure development in middle powers and emerging countries.

To boost Australia's technological capabilities, Australia's leaders should advocate that the Quad Tech Network:

- ***Pursue joint research, development, testing, and evaluation programs.*** Gain know-how and first-hand experience to broaden Australian expertise by pursuing collaboration in areas such as clean-energy technologies, rare-earth elements processing and recycling, information and communications technology, and space technologies, and creating a Quad-wide real-world technology testing and evaluation coalition to take advantage of the wide range of climates and topographies within the group.
- ***Create a Quad human capital network.*** Draw on the diverse scientific and technical capabilities of the Quad by pursuing new initiatives to foster cross-border collaboration within the Quad, such as an arrangement where qualified scientists, technologists, and engineers can readily work and live in the four countries.
- ***Set up shared compute and data resources.*** Facilitate broad-based and collaborative artificial intelligence (AI) research and address AI readiness shortfalls by directing the effort to create a Quad research cloud to offer widespread access to computational resources and datasets.
- ***Organize Quad innovation competitions.*** Tackle difficult science and engineering problems by initiating multinational tech challenges.

A Tech Future in Flux

Rarely is the future so uncertain – and so malleable. The current moment is one of geopolitical fluidity; decisions in the next few years will shape the decades ahead. There are widely divergent but plausible future scenarios for a post-pandemic world. There's little question the post-COVID-19 world will be different. How it will look depends on actions the world's leaders take – whether there is a renewed commitment to a rules-based international order, or a fragmented world increasingly dominated by authoritarianism. Whoever steps up to lead the world will drive the outcome.

The countries that figure out how to effectively restart and rebuild their economies as they emerge from the pandemic will set the course for the 21st century. It is not only economic heft that is of concern; political power and military might go hand in hand with economic dominance. Technology-leading nations will have outsized influence over the arc of international peace and security: by strengthening or challenging the rules-based order, by using technology responsibly or in illiberal ways, and by establishing rules and norms that reinforce or erode liberal democratic values.

At the center of this geostrategic and economic competition are technologies – such as AI, quantum computing, biotechnology, and fifth-generation wireless networking (5G) – that will be the backbone of the 21st-century economy. Leadership and ongoing innovation in these areas will confer critical economic, political, and military power, and the opportunity to shape global norms and values.

What is unfolding now is a competition to set the rules of the road for technology use for many years to come. At its core this contest is largely a binary one, with like-minded liberal democracies and authoritarian regimes jockeying for technological primacy.

Information technologies will be the key economic drivers for the coming decades, providing the essential digital infrastructure to communicate; to create and extract insight, and thus value, from data; to enable discovery and innovation; and to set the stage for further breakthroughs. These same technologies can also be used to control and distort information flows with censorship and disinformation; to monitor, isolate, and suppress individuals and groups; and to disrupt and disable critical infrastructure.

Differences within both camps exist, of course, with varying perspectives on notions such as data rights. There are also commonalities between the camps, such as a general desire for AI systems that are safe to use. Fundamentally, though, the two sides have conflicting views on appropriate uses of technology. These views are rooted in opposing norms and values pertaining to the rule of law, privacy, human rights, civil rights, civil liberties, and political freedoms. For Australia, its allies, and its democratic partners, assuring and maintaining leadership, sovereignty, and governance of technology policy are inseparable from protecting and preserving liberal democratic ideals and values.

The Self-Fulfilling Quest for Rapid Technological Change

This is an era of unprecedented and rapid technological change. This is not a science fiction world of technology run amok; humans invent and improve technologies and use them as tools. What often appears to be a bewildering, uncontrolled force is instead a man-made artifact of these times. Technology is developing in so many fields at such a fast clip because humans want things faster, better, easier, and at lower cost sooner. And not only do they believe this can happen, they expect it to.

Such expectations form a technology roadmap that companies race to complete. Gordon Moore, the engineer and businessman who identified the trend known as Moore's Law, remarked later in life that his edict on the doubling of transistors on a single chip every 12 to 24 months was really an observation about human activity in the realm of the scientifically and economically possible. It became a selffulfilling prophecy.[1] As a result, technology roadmaps with ambitious timelines abound – and are largely met. Information technologies are ground zero for this trend, with explosive growth in connected devices, data, transmitting speeds, and computing power.

The number of connected devices is expected to grow 10 percent every year, from about 22 billion today to 30 billion devices by 2023.[2] Over half of these will be internet of things (IoT) devices – such as appliances, factory and farming equipment, and logistics tracking – as early as 2021.[3] This trend will lead to a projected jump in global consumer IP traffic data volume from 212 exabytes per month in 2020 to 333 exabytes per month in 2022.[4] To put the scale of these figures in perspective: one exabyte of data would be a video call lasting 237,823 years; an office of 100 people would have to search the web for 57,077 years to accumulate that amount of data.[5]

This flood of additional data will be transmitted over more capable networks. Fixed broadband speeds in 2023 will be double those of 2018. Mobile speeds will see a more dramatic leap, tripling over the same time period for the average mobile network connection; 5G speeds will be 13 times higher than that average in 2023.[6]

Vast quantities of data are useless until they make sense. Computer processing power (compute) is required to turn these avalanches

of data into information and knowledge. Compute increased one-trillionfold from 1956 to 2015, while processing efficiency (performance per watt) improved 500,000-fold.[7]

Such leaps in capability drive further innovation: the amount of compute used for cutting-edge AI research increased 300,000-fold from 2012 to 2018.[8]

Driving this growth are key enabling technologies: semiconductors, 5G, and AI. This set of technologies will support advances in areas from autonomy to genomics, from robotics to synthetic biology, and from cyberspace to sensors. Rapid technological developments conjure up expectations of capabilities and breakthroughs to help make humankind healthier, wealthier, and freer. They also invoke fear of oppression, discrimination, and marginalization. Where the balance between these extremes will lie depends on what vision for the technology future prevails. The outcome rests with the countries that set the tone for the ways these technologies are used.

The first digital computer at NASA's Joint Propulsion Laboratory in 1953. Today, computer processing power is one trillion times greater and 500,000 times more efficient. Picture: NASA / Wikimedia, https://bit.ly/36fkMVi

Competing Tech Visions Causing Geopolitical Strain

Competing visions for technological sovereignty and tech governance are already disrupting geopolitics. The world's liberal democracies, the United States in particular, look to maintain a system that is largely distributed, bottom-up, and private-sector-led.

Existing international organizations are primarily intended to promote level playing fields for trade, standard setting, and economic competition. China and Russia in particular are damaging the efficacy and tarnishing the spirit of these organizations.

For example, both countries continuously fail to comply with commitments made for accession to the World Trade Organization, and Chinese firms are executing a deliberate strategy to subvert the integrity of international standard-setting bodies.[9]

Authoritarian regimes want to upend the bottom-up model by introducing top-down and state-centric technology governance. Part of the strategy to do so involves influencing and altering the functioning of multilateral forums to support this shift and pursuing dominance in key technology areas. Beijing, for example, is leveraging its power at the United Nations (U.N.) to pursue technology policy and governance goals. The U.N. is partnering with China's largest surveillance software company, Tencent, to host thousands of online conversations as part of the organization's 75th-anniversary celebration. In 2018, Tencent secured a contract with the U.N. Development Programme to create digital platforms in developing countries, providing it access to troves of foreign data that can be exploited for commercial gain and to inform foreign policy and intelligence objectives.[10]

Tencent, China's largest surveillance software company, has partnered with the U.N. to host the U.N.'s 75th-anniversary celebration. Tencent's collaboration with U.N. organizations has supported China's pursuit of state-centric technology governance. Picture: Mark Schiefelbein / NTB Scanpix, https://bit.ly/3pretpl

China further partnered with Russia to establish a U.N. group on cyber norms, generally viewed as intended to thwart U.S. efforts on consensus-building, and to pass a cybercrime-focused resolution that critics fear opens the door to targeting journalists and human rights groups by criminalizing online activity such as using encrypted apps.[11] These actions go beyond seeking to gain advantage in matters of trade and technology governance; they are part of a concerted effort to weaken key international organizations, particularly the U.N., and thus to entrench and promote illiberalism. American scholar Kristine Lee puts it bluntly: "Beijing is using the United Nations as a platform for legitimizing authoritarian rule."[12]

The Long Arm of the Global Digital Infrastructure Competition

Steps to gain the upper hand in global digital infrastructure are heavily intertwined with matters of everyday statecraft. That policymakers take action on matters such as trade and foreign relations in response to technology matters, and vice versa, underscores the stakes at play in the global technology competition. The nexus of technology, economics, diplomacy, and political ideology is increasingly tight. China uses its Digital Silk Road to fund and build infrastructure for surveillance and censorship, exporting its technology and know-how around the world.

In August 2020, the Donald Trump administration issued an executive order to ban TikTok, a Chinese video-sharing app, on the grounds of data security risks and of Chinese Communist Party (CCP)-influenced information control and censorship.[13] A follow-on order that directed Bytedance, TikTok's parent company, to destroy its data holdings collected from U.S. persons and divest its U.S. operations kicked off a flurry of acquisition interest from companies including Microsoft, Oracle, and Walmart.[14]

Beijing responded by placing export controls on a range of technology items, including certain algorithms used by TikTok, that sowed confusion over whether a takeover of TikTok by a U.S. firm would be feasible.[15] Chinese officials demonstrated that they are willing to deny a Chinese firm compensation for a valuable part of its business in an apparent show of force against U.S. actions. This action also underscores that Chinese firms have no recourse against the will of the CCP.

The Trump administration's actions on Chinese apps pale in comparison to those of India. The Indian government has banned dozens of apps developed by Chinese firms. The first order, banning 59 apps, came in June 2020 after the two countries engaged in a deadly border clash. Although this dispute is generally viewed as the impetus for the ban, India's technology ministry stated that the apps are "prejudicial to sovereignty and integrity of India, defence of India, security of state and public order."[16]

Use of Indian-made apps have soared since then, with download rates more than doubling.[17] In early September 2020, Indian authorities announced bans on an additional 118 Chinese apps, part of an expanding economic standoff with China.[18]

The case of 5G exemplifies the far-reaching implications and high stakes of the digital infrastructure competition. 5G networks will enable telemedicine, self-driving cars, and a proliferation of IoT devices to fuel the digital economy. Secure, reliable 5G networks will be essential elements of national infrastructure. Policymakers in Australia and Japan understood their importance early on and took decisive action to secure their 5G networks.[19]

U.S. officials took longer to act but are now at the forefront of warning of the risks of having equipment from untrusted vendors in 5G networks. Central to the debate are the threats that Huawei poses to national security, including the risk of espionage or disruption of critical infrastructure. Given the CCP's ability to exercise control over Huawei, there is justifiable concern over data integrity on networks that deploy Huawei equipment. Most concerning is the potential to use 5G equipment as a vector to cripple critical infrastructure. Such risk is not only about communications – 5G within a few years will be the backbone of controls needed for power grids, water supplies, and transportation infrastructure.[20] India looks to follow in the steps of its Quad partners. Although a formal ban appears unlikely, officials in New Delhi are signaling to Indian operators that Chinese equipment should be phased out.[21]

Beijing's reaction to growing international pushback on Huawei is telling, pointing to how crucial CCP officials view China's technological prowess to be to its broader foreign policy aims and economic goals, and how Chinese technology firms serve as an extension of and enabler for the CCP's ideological apparatus. A sampling of Chinese responses include extensive cyberattacks against Australia; Chinese state media's calling for "public and painful" retaliation against Britain; Beijing's threatening to withdraw from a trade agreement with Denmark; and China's ambassador to Germany's warning that German car sales in China could be torpedoed as retaliation for a potential ban on Huawei.[22] Chinese officials have also tried positive approaches. At the peak of the coronavirus pandemic in Europe in early 2020, Huawei and other Chinese tech firms shipped personal protective equipment and provided telemedicine services to Canada, France, the Netherlands, and the United States, among others, although the impact was mixed because of the uneven quality of the products.[23]

Illiberal Uses of Technology on the Rise

Although policymakers in liberal democracies recognize the long-term and wide-reaching implications of the global digital infrastructure competition, the uneven and largely uncoordinated responses to China's growing technological prowess and assertiveness are cause for concern. The lack of international consensus on rules and norms for the use of technology has resulted in unchecked deployments of technologies at odds with liberal democratic values, putting pressure on established and emerging democracies worldwide.

Illiberal deployments of technology, such as for censorship and surveillance, in nondemocratic countries are on a glide path from both policy and implementation standpoints. Such uses take place without public debate, and citizens rarely have recourse to protest. Liberal democracies, in contrast, have robust debates on the appropriate uses of technology. This is healthy. The nature of free and open discussion, however, is such that it also takes time to come to agreement, especially when national-level governments are hesitant to shape regulatory oversight of developments largely occurring in the private sector.

Meanwhile, Beijing is charging ahead, having exported AI surveillance technology to more than 60 countries.[24] Even leading democracies such as the United States and Germany have imported Chinese surveillance technology.[25] The proliferation concerns go beyond the equipment itself. In many cases, according to CNAS scholar Kara Frederick, Beijing is "exporting its norms, values, and governance practices to the rest of the world."[26]

Beijing looks to expand these efforts. The forthcoming China Standards 2035 strategic plan, Beijing's blueprint to lead global standard setting in areas such as AI and the IoT, emphasizes increasing China's influence over emerging technology standards.[27] Doing so would provide Chinese firms with a competitive edge and offer a means to increase illiberal use of such technologies as AI. In standardsetting organizations such as the U.N.'s International Telecommunication Union, the Chinese government has been promoting its vision for global internet and cyber governance, which favors a state-led approach to managing information flows.[28]

Geopolitics Affected by Tech Use Rules and Norms

Shaping how technology is used increasingly means shaping geopolitics.

China's proliferation of its technology, norms, values, and governance frameworks is bolstering dictatorships and eroding fragile democratic institutions around the world.

The gulf between liberal democracies and illiberal states is exemplified by divergent views on governance principles for AI.[29] While there are many similarities between Chinese frameworks such as the Beijing AI Principles and those of other global actors, such as using AI to better healthcare and education, there are also important differences.[30] Most notable is the framing of such principles as intended to advance the "community of common destiny," a core concept in CCP ideology that implies ambitions to reshape the current global order to a more China-centered world order.[31]

Some of the most prominent attempts to set global rules and norms concern cyberspace. Unfortunately, much of this work is disjointed. There are dozens of bilateral and multilateral statements, declarations, pledges, and agreements on standards for behavior in cyberspace.[32] One of the most important of these is the Convention on Cybercrime, the first binding multilateral agreement to regulate cybercrime – and one that is based on harmonization of national laws.[33] Given the interconnectedness of the world's digital infrastructure, unified and multilateral approaches to the problem are a must.

The authoritarian creep and the reactive approach to technology development and use by liberal democracies set the stage for a problematic future. Tech-leading democracies must take a fresh approach to technology policy, to include leading the way on rules and norms for technology use – an approach steeped in multilateral cooperation, based on shared values, and focused on effectively outcompeting illiberal countries. Australia, with its Quad Tech Network initiative, is poised to be a leading voice for such change.

Mind the Gap: Divergent Approaches to Tech Policy Present Hurdles and Opportunities

Broad-based technology policy cooperation and coordination will not be easy to achieve. They are, however, very much worthwhile and necessary. Australian policymakers should be clear-eyed about the road ahead: achieving these goals will require patience, compromise, and creativity.

While the Quad countries share a range of interests and goals, differences between them will cause inevitable friction. The Quad countries have different views on, experience with, and legal frameworks for tech policy matters. India in particular tends to be an outlier, as demonstrated by the government's penchant for shutting down internet access as a tactic to suppress protests and domestic civil unrest.[34]

Rules for use of facial recognition technology and personal data offer vignettes that provide insight into the challenges these differences pose to tech policy coordination and collaboration. At the same time, such varying perspectives also present important opportunities to begin a shift toward harmonizing policies on data collection, data management, and data privacy, setting minimum standards for concepts such as security, accuracy, and transparency, and establishing norms for how and when to use emerging technologies.

Australia

Considerations of facial recognition technology use in Australia have been wide-ranging. The Department of Home Affairs went as far as to propose that facial recognition be used to verify the age of people wishing to watch online pornography.[35] In October 2019, a parliamentary committee rejected proposed legislation for a national facial recognition database for its lack of protections for citizens' rights, in particular citing concerns over the potential for mass surveillance. Committee members recommended an overhaul of the laws to ensure they are centered on "privacy, transparency and subject to robust safeguards."[36] Despite concerns over insufficient safeguards for federal facial biometrics matching, individual Australian states continue to upload data such as photos, signatures, and other driver's license details to a national database to combat identity theft and other crimes. That database is expected to be operational by September 2021.[37]

Data governance is regulated by the Office of the Australian Information Commissioner (OAIC), which focuses on privacy, freedom of information, and overseeing governmental use of information.[38] While Australia's privacy laws – codified in the Privacy Act 1988 – are robust, critics note that OAIC is overburdened and underfunded.[39] Despite these challenges, OAIC continues to conduct investigations, including one into the way the company Clearview AI handed personal information obtained through its facial recognition tool.[40] The Clearview AI investigation, a joint effort with OAIC's British counterpart, could serve as a model for expanded collaborative investigations with Quad partner agencies.

India

Although the use of facial recognition technology in India is relatively new, the government led by Prime Minister Narendra Modi has grand ambitions for a nationwide database, the Automated Facia Recognition System. This database would match images obtained from closed-circuit television and other cameras with images from existing databases such as those used by the passport service and the country's police forces.[41]

Protests in late 2019 and early 2020 against the Citizenship Amendment Bill, which provides citizenship to illegal immigrants of certain religious minorities, are a helpful case study of Indian authorities' use of facial recognition technology.[42] Critics point to a lack of regulation on the technology's uses, which can include targeting individuals for arrest. Critics also point to a lack of transparency on the use of facial recognition by government entities. For example, the use of facial recognition first became public knowledge with a press report, not after open deliberation or an official announcement.[43] Broader concerns are that the technology in use in India is generally highly inaccurate and that the 2018 Personal Data Protection Bill contains wide-ranging and loosely defined exceptions for law enforcement's use of personal data.[44]

Residents of New Delhi protesting against the Citizenship Amendment Bill. Indian authorities were criticized for their use of facial recognition technology and specifically for the lack of regulations and transparency for targeting individuals for arrest. Picture: Sanjeev Yadav / Wikimedia, https://bit.ly/3ppcdi9

Japan

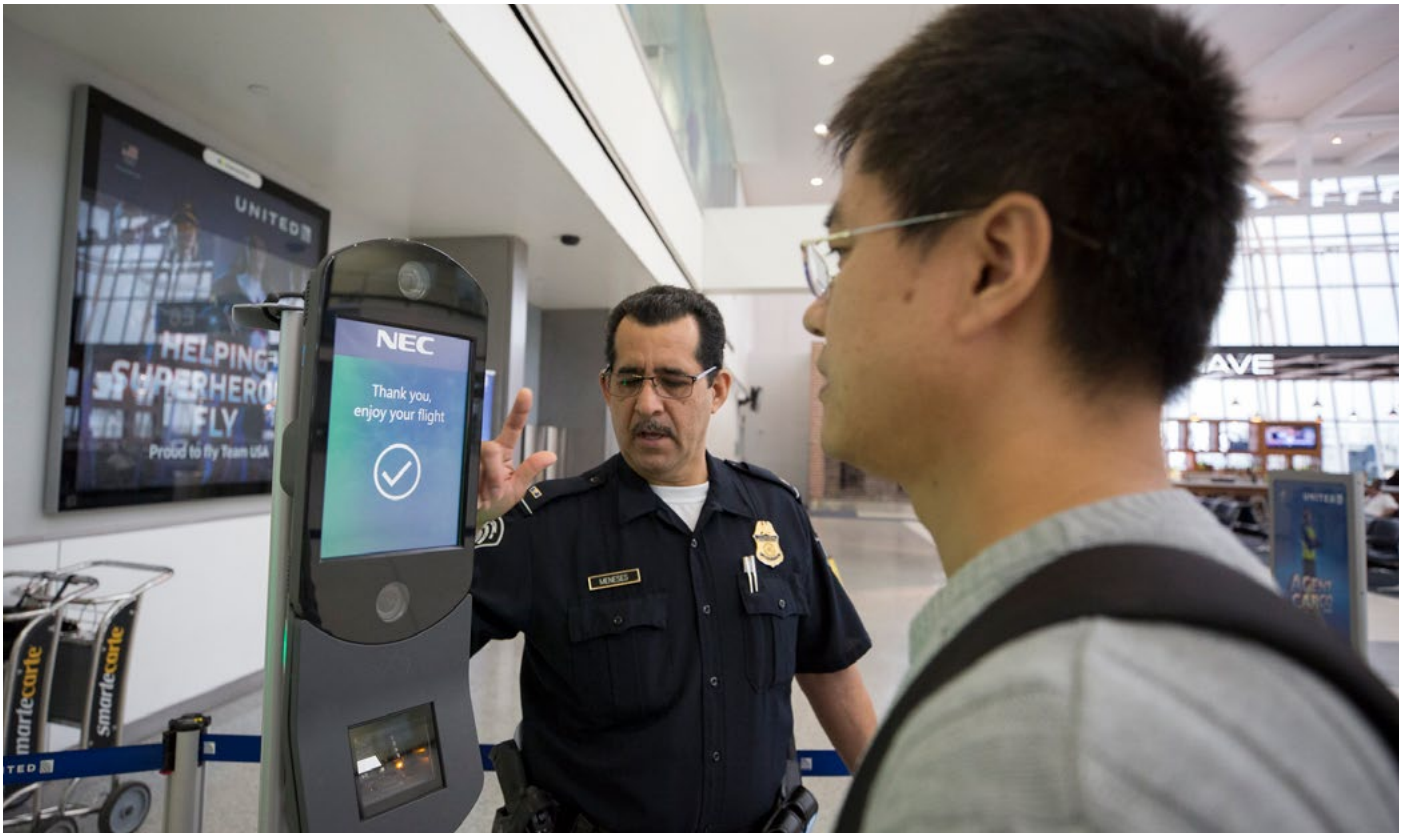
Facial recognition technology is widely deployed in Japan, with electronics giant NEC at the forefront of research, development, and deployment, using it for a range of consumer-oriented purposes such as cashless payments, ticketless entry, and banking services.[45] Japan Customs uses the capability at numerous airports for passenger screening.[46] Japanese firms are also at the forefront of using facial recognition and surveillance as ways to monitor employee productivity.[47] The Japanese government has proposed using facial recognition technology to identify and restrict admission of gambling addicts at casinos and racetracks.[48] Because of their advanced capabilities, Japanese firms see an opportunity to compete with China for dominance in facial recognition and other surveillance technologies.

The Personal Information Protection Commission (PIPC), a government entity established in 2016, is charged with overseeing the protection of personal information collected by public and private entities. The PIPC also has a mandate to foster international cooperation, which could position it as a useful model for cooperation on data collection and privacy matters among the Quad members.[49]

United States

Facial recognition has generated a grassroots-level pushback in the United States, particularly for its use by law enforcement. Several cities and states across America have banned facial recognition for law enforcement.[50] At the same time, certain U.S. airports are deploying facial recognition cameras as part of coronavirus-detection techniques.[51] Unlike its Quad colleagues, the United States lacks national-level laws and rules on facial recognition deployment. Instead, state and local authorities craft their own regulations, resulting in a patchwork that makes it increasingly difficult to develop a unified national approach and poses obstacles for technology companies that intend to conduct research and develop compliant products. In June 2020, Amazon and Microsoft put a moratorium on selling facial recognition to law enforcement and IBM cancelled its work on facial recognition.[52]

Data governance, for facial recognition and a slew of other personal data collected by devices and apps, is another area where the United States has no coherent regulatory framework. The policies that exist are generally formulated by the companies providing the service and are typically hard to understand. Anonymizing data or opting out altogether is often so cumbersome that it's effectively impossible for the average smart phone user, let alone engineers of major tech companies.[53]



The electronics giant NEC has been at the forefront of research, development, and deployment of facial recognition technology. Picture: Tomohiro Ohsumi / Getty Images, https://bit.ly/2NJk2Bx

Bridging the Gap: Collaborative Technology Policy

The varying approaches to and goals for the use of surveillance technology point to the challenges of collective action on technology policy. Healthy democratic societies have an array of viewpoints that wax and wane in influence. They exhibit the great strength of open societies: a common respect for democratic norms and values, as shown the ability to debate the tradeoffs between security, privacy, individual rights, and convenience within each country and with each other.[54] It is these qualities that can place Australia at the forefront of setting the norms and standards for using those technologies responsibly, especially if it does so in conjunction with the Quad and other partners, to successfully blunt opposing efforts by undemocratic states.

The liberal democratic/authoritarian divide further underscores the criticality of trusted supply chains. One of the most important activities for the Quad is to build a trusted network for the digital economy's key technologies. This task includes creating confidence that the supply of communications equipment won't be halted on a whim, that data stored by a foreign social media site won't be seized by that country's government without due process, and that shipments of critical minerals won't be cut off as punishment.[55]

There is a growing realization among the world's democracies that the current approach to tech policy – individual, disparate, and reactive – brings increasingly diminished returns and provides pathways for Beijing in particular to take advantage of the resulting fissures. In the face of growing authoritarianism, there is also renewed appreciation of how much more unites democracies than divides them. There is tangible evidence of this shift, such as the United States' joining the Global Partnership on Artificial Intelligence after much hemming and hawing and India's effectively banning Huawei from the country's 5G networks. Both seemed improbable mere months ago.

Given the flux of the technology future, concerted action to shape it is needed. Doing so successfully will require a new way of thinking about technology policy generally and collaborative approaches specifically: a techno-democratic statecraft for the 21st century.

Techno-Democratic Statecraft: A Framework for Crafting a Beneficial Tech Future

The trajectory of waning clout in technology development, standard setting, and proliferation poses an unacceptable and avoidable challenge to the interests of the world's leading liberal democratic states. Australia and its Quad partners are well positioned to formulate a fresh approach to technology policy for a new era. A new, comprehensive method is needed to navigate the 21st-century technology competition and maximize the odds that the technology future is a positive one. This framework, techno-democratic statecraft, comprises seven distinct but connected qualities. The approach is:

- **Proactive:** The leaders of each Quad member country should determine what technology areas are of priority based on their respective national needs and goals rather than trying to stay ahead of or chase the efforts of competitors. Although considerable overlap in priorities is likely, particularly with like-minded countries, framing the effort in this manner ensures that technology development takes place in the proper context and isn't unduly influenced by the main concerns of others.
- **All inclusive:** Policymakers should maximize the range of key inputs such as R&D investments, human capital, and education, and treat technology areas as parts of a large interrelated web rather than stovepiped and independent disciplines.
- **Whole of society:** Lawmakers should recognize that innovation and technological breakthroughs are not the sole domain of private industry. Governments play an important role in supporting and guiding technological developments, especially basic research, and must be proactive in addressing occasional misalignments between what companies want to produce and what governments need.
- **Flexible:** The Quad partners should adopt a mix of affirmative measures to boost competitiveness (such as investments in R&D, training, and supply chain resilience) and protective action (such as export controls and sanctions) to safeguard their existing advantages. The balance between affirmative and protective actions is likely to shift over time and vary between different technological disciplines.
- **Values driven:** Policymakers should make technology policy decisions in line with liberal democratic values, including human rights, civil rights, civil liberties, and political freedoms.
- **Multilateral:** Quad leaders should appreciate that no one country can tackle most tech policy challenges on its own; the requisite knowledge and capabilities are too diffuse. Broad-based, proactive, and long-term multilateral cooperation among like-minded countries is needed tomaximize effectiveness. The Quad's network of alliances and partnerships is one of its greatest competitive strengths and should be capitalized upon.

- **Pragmatic:** Lawmakers should be open to and welcome cooperation with nondemocracies where values and interests sufficiently align. Engagement on issues that transcend borders should trump ideological rigidity, whether it is cooperating with Vietnam on COVID-19 responses or working with China and Russia to address climate change.

The Quad is primed to execute techno-democratic statecraft. As a group with strengthening bonds and greatly overlapping interests, it presents two general pillars for coordination and collaboration on technology policy that support crafting and achieving a shared vision for a desired technology future:

1. **Alignment:** The Quad members share strategic interest in the outcomes that policies guided by techno-democratic statecraft principles are designed to produce. Each country seeks to protect and sustain an open and free Indo-Pacific, and to have robust economic growth aligned with a beneficial technology future.

2. **Compatibility:** All four Quad countries have key attributes in common. All are sizeable and robust economies, with broad and diverse capabilities in key technology areas. Together, they have considerable scale in R&D spending, science and technology output, industrial and manufacturing capacity, relevant infrastructure, and human capital. Their combined geographic breadth also affords important advantages for practical matters such as logistics and supply chains and geostrategic ones such as regional influence. Finally, Australia, India, Japan, and the United States share democratic values.

In the face of a rising China that is increasingly capable of and intent on being the global leader across a broad spectrum of emerging technologies, concerted action by the Quad is necessary to create a bulwark against the illiberal use of technology.

This effort requires taking the lead to establish the norms for ways technologies should be used, working to ensure that technologies and components are not used in violation of democratic values, cutting off technology exports that directly or indirectly enable the illiberal use of technology, and placing multilateral sanctions on the organizations and individuals that deploy technologies in violation of these norms.

Such an approach does not mean Australia and the other Quad member states must be in full alignment on all technology policy matters; that would be unreasonable and unrealistic. It would also be undesirable: the great strength of democracies is that they can take varied approaches according to their national interests while still adhering to core liberal democratic values. A coordinated tech policy approach by the Quad also doesn't prevent any member from pursuing similar arrangements with other democratic states or groups such as Canada or the EU, or with nondemocratic technology-leading states in the Indo-Pacific such as Singapore.[56] What is key, however, is that these tech partnerships be formed in a manner that enables like-minded countries to shape their technological future as they see fit, in accordance with their strategic goals and without compromising their values or sovereignty.

There is urgency to act. The geostrategic competition in cyberspace and emerging technologies is multifaceted, with developments moving at high speed. Especially in the wake of the COVID-19 pandemic, Beijing in particular is trying to improve its position on the global stage relative to the world's liberal democracies, taking advantage of their disjointed response and dearth of leadership.

Before the pandemic, the world's democracies already faced their gravest challenge in decades: the shift of economic power to illiberal states. By late 2019, autocratic regimes accounted for a larger share of global GDP than democracies for the first time since 1900. As former U.K. foreign secretary David Miliband recently observed, "liberal democracy ... is in retreat."[57] How Australia and like-minded partners respond post-pandemic will determine if that trend holds. Australia can rally the Quad, crafting a unified response by shaping a new strategic technology policy framework as part of the new Quad Tech Network.

The four tech partners should also use their partnership as a springboard for cooperation with other like- minded countries on matters of international peace and security, and to address the erosion of the rules- based order. The Quad has already engaged with South Korea, Vietnam, and New Zealand (the "Quad- plus") on collective responses to the COVID-19 pandemic.[58] Other opportunities for multilateralization abound: the United States and Australia could extend relationships with the Five Eyes partners, something Japan has already expressed strong interest in; U.K. government officials have proposed a "Democracy 10," which would include the Quad countries, to tackle 5G and other technology issues; and former U.S. government officials have proposed alliance frameworks to tackle a range of technology policy issues.[59] That Australia is a part of all these initiatives, active and proposed, should not come as a surprise – it enjoys important qualities that set it up for a leading role in an array of multilateral efforts.

Opportunities for Australian Leadership in the Quad Tech Network

Australia's size, geographic location, and strong bilateral relations with Quad members afford it advantages that allow it to take on a vital leadership role in creating and shaping a multilateral tech policy collaboration effort rooted in the Quad Tech Network. With the smallest economy and population of the Quad, Australia is often best placed to propose new initiatives, because there are no motivations that could be construed as designs on economic and geostrategic dominance. The country also serves as a geopolitical bridge between North America, South Asia, and the Asia-Pacific and as an objective arbiter on complex and sometimes contentious issues. Finally, Australia has strong bilateral ties with India, Japan, and the United States that put it in a position to be the chief interlocutor for negotiations within the group.

By applying techno-democratic statecraft principles, Australia can lead the Quad on a range of important technology policy issues, strengthening the Quad's economic competitiveness and promoting the development and deployment of technologies in a manner consistent with liberal democratic values.

Four areas recommended for priority attention are cyberspace, supply chains, 5G and beyond-5G technologies, and digital development in emerging countries. The goals for each of these recommendations are to boost the economic competitiveness of Australia and its Quad partners and to enhance each country's national security through collective action.

Bolster Cyber Security

One of Australia's foremost priorities should be to use the Quad as a means to strengthen its own national cybersecurity posture and to strive for better cooperation among like-minded partners. As is rightly noted in Australia's Cyber Security Strategy 2020, cyber threats are evolving rapidly, and secure, robust, and reliable digital infrastructure is essential to day-to-day functioning of society.[60] Three promising areas for near-term cooperation:

- **Multilateral engagement for setting norms that promote a free and open cyberspace.** The U.S. Cyberspace Solarium Commission – a congressionally mandated group charged with crafting a comprehensive cyberspace strategy – issued a report in March 2020 that contains numerous recommendations that could be adopted by the Quad to promote responsible behavior in cyberspace. These include building an enforceable rules-based international order in cyberspace and restoring the integrity of international standard setting, as part of an overarching framework for layered cyber deterrence.[61]

A common position on norms for cyberspace among the Quad should serve as the foundation for engagement with like-minded countries to standardize the myriad declarations on related norms, as well as engagement with other international actors such as Russia and China.

- **Multilateral responses to nefarious cyber activity in accordance with international law.** A coordinated effort is realistic and feasible because it would be rooted in shared values. The Quad could formulate consensus on how to respond to cyber operations that target democratic institutions and systems (e.g., election infrastructure), attacks on personal information of Quad country citizens and residents (e.g., targeting of people for supposed violations of Hong Kong's Security Law), and state-backed theft of intellectual property.[62] On that front, the three Quad partners signatory to the Convention on Cybercrime should prod India to join them as a first step toward harmonization of national laws and collective agreements on cyber issues.
- **Shared monitoring and cyber-intrusion remediation capability.** While the cyber networks and the respective cyber capabilities of Australia, India, Japan, and the United States differ considerably, there are important overlaps in interests and goals that make a quadrilateral cyberattack-mitigation network feasible. The India-Japan and Japan-Australia cybersecurity and cyber policy dialogues are but a few examples of how such cooperation could work.[63]

At a bare minimum, enhanced information sharing between the Quad's respective computer emergency readiness teams and signals intelligence agencies would help to identify and track cyberattacks and to learn from an attacker's modus operandi. As Five Eyes partners with robust signals intelligence capabilities, Australia and the United States have particular expertise here. The U.S. Cyber Command's "hunt forward" missions, which include disclosing findings to other parts of the U.S. government to defend critical networks and provide cybersecurity firms with important information to update their products and services, can serve as a model that could be internationalized on a formal basis within group.[64] The Quad countries can also collaborate on efforts to better engage with the private sector to help prevent and mitigate cyberattacks. More challenging would be initiatives such as developing a multilateral cyber early-warning system and surging personnel and other capabilities to assist a Quad partner under cyberattack.[65]

These actions in concert could help to foster a safer and more stable cyberspace. As the authors of the Cyberspace Solarium

Commission report note, there are three reasons why such an approach reduces the likelihood and effectiveness of cyberattacks: "norms change an adversary's decision calculus"; "a system of norms enforced by multiple actors is a relatively cost-effective means of bringing greater stability to cyberspace because it reduces the burden on any one nation to reinforce the system of norms"; and "frameworks of norms are sticky – once a pattern of behavior is set, the framework becomes hard to dislodge."[66] Australia and the Quad can be the vanguard of a sea change in global cybersecurity posture.

Secure Supply Chains

The fallout of the COVID-19 pandemic has exposed the widespread fragility of the world's supply chains. Quarantines, travel bans, and factory shutdowns showed the risks in achieving economies of scale through geographic concentration.[67] Export controls on medical equipment and Beijing's attempts at economic coercion, such as canceling trade agreements and imposing excessive tariffs on agricultural products, further highlighted the need to rethink the structure of global supply chains, particularly the heavy reliance on China for key inputs and components.

Numerous efforts to secure and diversify supply chains are beginning to take shape. The Japanese government announced a $2 billion program to help domestic firms repatriate manufacturing.[68] The United States is drafting the outline of an "Economic Prosperity Network" – a group that comprises the Quad, New Zealand, South Korea, and Vietnam – to move sourcing and manufacturing out of China.[69]

The Supply Chain Resilience Initiative, a trilateral effort with Australia and India spearheaded by Japan, is most pertinent in the near term to the Quad.[70] The goal of this budding effort is to reduce dependency on China for numerous supply chains. Priority One for Australian leaders should be to ensure U.S. involvement in this effort. The effort to achieve strategic autonomy in supply chains is a challenging one, especially without the involvement of the world's largest economy. A quadrilateral approach would also serve as a more effective springboard to broaden such cooperation with other countries or groups, such as ASEAN.

Pursue 5G and Beyond-5G Technologies

Australia is poised to be at the forefront of a new technological approach to wireless communications.

As the early voice in recognizing the risks involved in having untrusted vendors as part of 5G telecommunications networks, Australia has outsized influence in the debate over securing the 5G future.

One promising avenue is to promote a shift to modular architecture and open interfaces for wireless telecommunications infrastructure (open radio access network, or open RAN). A modular architecture allows an operator to choose multiple vendors, rather than being locked in with a single large, integrated vendor. Open interfaces, which allow the equipment from any vendor to work with that of another, make such architecture possible. The approach is marked by extensive use of software to take on the functionality currently carried out by proprietary hardware, in a process called network virtualization.[71]

There is broad support among government officials and lawmakers in Japan for open RAN as a technological alternative; the company Rakuten has deployed a nationwide 4G open RAN network and is in the process of establishing one for 5G. Interest in the United States is growing, with legislation that would provide R&D funding pending in the U.S. Congress and the Federal Communications Commission having held a large conference for government and industry leaders to discuss the subject in September 2020. India, which effectively banned the use of 5G network equipment from Huawei on India's telecommunications networks, has a large software industry that could become a major force in a revamped telecommunications sector. Similarly, Australia's software development companies could be formidable competitors in the space.

At the same time, Australia should corral the Quad and other partners to pursue collaborative efforts on beyond-5G technologies. Industry experts project that initial deployments of next-generation telecommunications will begin around 2030, and research into the foundational capabilities is underway in Japan and the United States, among others. The Japanese government has formulated a beyond-5G strategy and is keen on multilateral partnership. Australia's research community and high-tech industry are well placed to contribute to key capabilities including network virtualization, quantum cryptography, and photonics.[72]

By instituting long-term strategic planning for the development and deployment of next-generation telecommunications, the Quad countries can position themselves for technological leadership and as key enablers of innovation and economic growth. Prudent planning now will help to avoid much of the headache of the current state of affairs in the future.

Close the Digital Divide with Targeted Investments

The Quad should create a standing multilateral mechanism to fund secure and fair digital infrastructure development in middle powers and emerging countries. Such efforts would build on existing fair investment criteria and be anchored to the tenets of techno-democratic statecraft. Australia's Department of Foreign Affairs and Trade's export credit agency, Export Finance Australia, could spearhead this effort together with the Japan Bank for International Cooperation, the U.S. International Development Finance Corporation, and the Export-Import Bank of India.

The first course of action should be to craft a shared strategic vision for the investments and digital infrastructure – 5G, financial technology, and maritime domain awareness tools, among others – that are of highest priority to the Quad. Next the group should determine which resources to allocate and where. Focusing on telecommunications infrastructure and maritime domain

awareness tools in Southeast Asia is recommended to create a positive counterbalance to Chinese digital entanglement in the region and to help safeguard free and open access to the South China Sea and other sea lines of communication.

The Quad should adopt the investment criteria and certification model of the Blue Dot Network (BDN), an initiative to "promote infrastructure development that is open and inclusive, transparent, economically viable, financially, environmentally and socially sustainable, and compliant with international standards, laws, and regulations."[73] BDN's current participants are Australia, Japan, and the United States. India should be encouraged to formally join BDN, because there is notable common ground in values underpinning the certification model: its underlying principles are rooted in the G20 Principles for Quality Infrastructure Investment, to which India is signatory, and the Equator Principles – a risk management framework for financial institutions focused on environmental and social risk in development projects – which India's IDFC FIRST Bank adopted.[74]

Opportunities to Build Australia's Tech Capacity

Australia should leverage the Quad Tech Network to bolster its technology capacity. Each Quad member brings to bear an array of capabilities, human capital, and infrastructure, but Australia lacks the scale of resources that Japan and the United States in particular can typically apply to a problem. Through strategic partnerships in which Australia provides niche expertise and unmatched competencies, it can lay the foundation for broader capabilities in an array of scientific and technical domains.

Pursue Joint Research, Development, Testing, and Evaluation Programs

Opportunity abounds for joint R&D efforts to serve as a foundation for innovation and entrepreneurship. Promising areas for collaboration include clean-energy technologies, rare-earth elements processing and recycling, information and communications technology, and space technologies. These efforts could build on existing bilateral efforts such as the United States-India Science and Technology Endowment Fund, the India Japan Science Council, and longstanding Australia-Japan cooperation in science and technology.[75]

Testing and evaluation of component technologies and complete systems constitute another promising area.

Together, the four countries offer access to the most extreme real-world testing environments, from the world's highest mountains to the deepest ocean trenches, from the driest of deserts to steamy tropical rainforests, and from some of the coldest and to some of the hottest places on earth.[76]

Vast open spaces are also an appeal: Australia's Woomera Range Complex is the largest land-based test range in the world.[77]

A more ambitious, more difficult, and longer-term effort would be to create a Quad extension to the existing National Technology and Industrial Base (NTIB) – currently comprising Australia, Canada, the United Kingdom, and the United States – to create a larger defense technology cooperative framework. While there is much common ground between the Quad and NTIB on the types of weapons systems and platforms required for their respective defense postures and force projection requirements, there are also substantial obstacles that would need to be addressed before such cooperation could be feasible. A general issue is India's defense relationship with Russia, which involves substantial purchases and maintenance agreements for military systems, and a potential defense logistics agreement.[78] Any successful Quad relationship in this sphere would require India to cut such ties. There are two specific hurdles: implementing needed reforms to streamline NTIB implementation, particularly addressing intellectual property (IP) management and technology transfer stipulations, and addressing India's industrial policies that are designed to promote self-reliance.

First, implementation of NTIB is being hindered by constraints and a lack of urgency on the part of U.S. defense policy officials. While there are numerous bilateral U.S.-led NTIB efforts underway, multilateral projects pursued by all four NTIB members have been limited to exploring new avenues of controlled technology transfer and foreign direct investment review. Critics point to increasing opportunity costs for NTIB members while NTIB fails to live up to expectations. IP and export controls are notable barriers to achieving proper collaboration within the NTIB framework.[79]

Regarding IP, the main consideration would be whether to make Quad government-funded research publicly available whenever appropriate; to offer short-term patent protection to developing entities, after which the IP enters the public domain; or to implement a policy that mirrors the more common IP rights frameworks, with the caveat that the IP owners would be required to license out Quad-funded IP to third parties in the Quad member countries, with limited exceptions.

To ease joint research and technology transfer, changes would be necessary to existing export control and regulatory regimes. The U.S. International Traffic in Arms Regulations (ITAR) in particular poses a roadblock, because it restricts the export and import of defense articles even among allies. The Quad should explore a

limited "ITAR-free zone" to get rid of regulatory hurdles.[80]

Second, India's industrial policies designed to promote self-reliance constitute another constraint. New legislation – specific to defense policy – introduced in August 2020 requires domestic sourcing for a broad swath of weapons and platforms, including artillery, diesel-electric submarines, communication satellites, and shipborne cruise missiles.[81] Another key barrier is New Delhi's requirements for large offsets – contracted provisions to an import agreement – for joint R&D for, joint production of, or purchases of defense goods.[82] Revised guidelines published in June 2020 shift more emphasis on production and manufacturing solely in the defense industry and away from civilian sectors to boost self- sufficiency.[83] A more positive development is India's raising the foreign direct investment cap in the defense sector to 74 percent from 49 percent, but these caps should be eliminated for any Quad-related collaboration.[84] Such policies have no place in comprehensive defense technology cooperation; they are by definition antithetical to the kind of proactive defense tech cooperation proposed here.

Create a Quad Human Capital Network

One of the Quad's greatest collective strengths is its large and diverse reservoir of scientific and technical talent – an underutilized resource. Barriers such as student and work visas, and bureaucratic hurdles to scientific exchanges, pose unnecessary obstacles to maximizing valuable human capital. Because technical innovations are more likely to occur with the free flow of ideas, new initiatives to foster cross- border collaboration within the Quad should be considered.

A Quad human capital network could include a Schengen-like arrangement where qualified scientists, technologists, and engineers could readily travel and live in the Quad countries for research in the public and private sectors, and there could be regular talent exchanges to build networks and promote the exchange of ideas among scientists. Such arrangements could serve to bolster skills in critical areas such as AI, likely to be one of the most consequential technology areas in coming decades. Although the Australian government has articulated the importance of AI technologies for the country's economy and society, its AI ecosystem is relatively underdeveloped.[85] Particularly, Australia's private sector lags behind its peers in AI adoption readiness.[86]

Set up Shared Compute and Data Resources

Another limiting factor for AI-related development is that innovations in machine learning, especially deep learning, depend on large datasets and compute resources that are not widely available. The Quad should explore mechanisms to pool data and computing resources to facilitate broad-based and collaborative AI research. For example, the Quad could create a multilateral version of the U.S. national research cloud, an initiative to offer widespread access to computational resources and datasets to academic researchers across the United States. This effort has strong bipartisan support in the U.S. Congress.[87]

Pooling of standardized datasets from the four countries could facilitate training of machine learning models. Although privacy and other concerns place limits on which data are suitable for sharing, any major increase in data availability would be of value. In May 2020, Japan submitted to the World Economic Forum a framework for ensuring trusted open data flows to help boost international trade and industrial production.[88] This framework could serve as a starting point for deliberations within the Quad on cooperative data governance to better capitalize on growing digitalization in the Quad economies.

Recent breakthroughs in fully homomorphic encryption also open up the possibility of using encrypted data for machine learning without revealing the actual contents of the data, thus making available more sensitive datasets.[89]

Organize Quad Innovation Competitions

Innovation prize competitions such as the U.S. Defense Advanced Research Projects Agency's series of challenges and the XPRIZE Foundation's contests have successfully tackled some of the toughest science and engineering problems.[90] Organizing Quad-wide challenges would be an effective way to harness the diverse human capital pool of the group, particularly if multinational team participation were emphasized. Such competitions could be geared toward addressing general problem statements, such as developing novel energetic materials and cost-effective carbon-sequestration technologies, or focused on narrowly defined issues, such as using nascent quantum computers to create high-quality synthetic data or using generative adversarial networks to design alternatives to rare-earth elements by creating new compounds of naturally-occurring materials.[91]

A team of engineers participates in an innovation competition held by the Defense Advanced Research Projects Agency. Quad-wide challenges with multinational teams could effectively harness human capital to solve the world's toughest science and engineering problems. Picture: DARPA, https://bit.ly/39oE1On

Conclusion

Australia has the potential to bring about a consequential shift in international technology policy in creating the Quad Tech Network. There is considerable opportunity for Australian leadership to craft affirmative initiatives that will strengthen both the country's own economic competitiveness and that of its Quad partners. Particularly by anchoring this group's activities in techno-democratic statecraft,

Australia's leaders can set a course to craft and execute an affirmative technology agenda by bolstering cyber security, securing supply chains, pursuing 5G and beyond-5G technologies, and closing the digital divide in the Indo-Pacific with targeted investments.

Australia further has the opportunity to craft collaborative efforts that can boost its tech capacity in a range of disciplines. Among the Quad's great strengths are its large and diverse pool of human capital, its wealth of knowledge and capabilities across the board in scientific and technical disciplines, and its extensive supporting infrastructure. Australia should tap into these strengths by pursuing joint research, development, testing, and evaluation programs; creating a Quad human capital network; setting up shared compute and data resources; and organizing Quad innovation competitions.

All the while, pursuing these efforts in the broader context of techno-democratic statecraft will promote more effective multilateral collaboration between like-minded countries and serve as a bulwark against encroaching authoritarianism by promoting norms and values for technology uses that comport with liberal democratic values. In doing so, Australia can help to ensure that its technological future is a beneficial one.

Endnotes

1. Ethan R. Mollick, "Establishing Moore's Law," *IEEE Annals of the History of Computing*, 28 no. 3 (July–September 2006), 62–75.
2. "Cisco Annual Internet Report (2018–2023)," Cisco, 2020, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf.
3. "The Zettabyte Era: Trends and Analysis," Cisco, July 2016, https://webobjects.cdw.com/webobjects/media/pdf/Solutions/Networking/White-Paper- Cisco-The-Zettabyte-Era-Trends-and-Analysis.pdf.
4. J. Clement, "Data volume of global consumer IP traffic, 2017–2022," Statista, February 28, 2020, https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip- traffic/.
5. Patrick Thomas, "Defining an Exabyte," BackBlaze, March 23, 2020, https://www.backblaze.com/blog/what-is-an- exabyte/#:~:text=The%20International%20System%20of%20Units,million%20terabytes%20%3D%201%20billion%20gigabytes.
6. "The Zettabyte Era: Trends and Analysis."
7. Nick Routley, "Visualizing the Trillion-Fold Increase in Computing Power," Visual Capitalist, November 4, 2017, https://www.visualcapitalist.com/visualizing-trillion-fold- increase-computing-power/; Max Rose and Hannah Ritchie, "Technological Progress," Our World in Data, 2013, https://ourworldindata.org/technological-progress.
8. Dario Amodei and Danny Hernandez, "AI and Compute," Open AI, May 16, 2018, https://openai.com/blog/ai-and-compute/.
9. U.S. Trade Representative, "2019 USTR Report to Congress on China's WTO Compliance," March 2020, https://ustr.gov/sites/default/files/2019_Report_on_China%E2%80%99s_WTO_Complian ce.pdf; U.S. Trade Representative, "2019 Report on the Implementation and Enforcement of Russia's WTO Commitments," February 2020, https://ustr.gov/sites/default/files/2019_Report_on_Russia's_WTO_Compliance.pdf; and William Morrissey and John Givens, "The Measure of a Country: America's Wonkiest Competition with China," *War on the Rocks*, August 21, 2020, https://warontherocks.com/2020/08/the-measure-of-a-country-americas-wonkiest- competition-with-china/; Martijn Rasser, Rebecca Arcesati, Shin Oya, et al., "Common Code; An Alliance Framework for Democratic Technology Policy" (Center for a New American Security, October 2020), https://www.cnas.org/publications/reports/common-code; and Justin Sherman and Mark Raymond, "The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom," *The Washington Post*, December 4, 2019, https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed- cybercrime-resolution-thats-not-good-news-internet-freedom/.
10. Kristine Lee, Associate Fellow, Center for a New American Security, "The United Nations: An Emerging Battleground for Influence," Testimony before the U.S.-China Economic and Security Review Commission, June 24, 2020, https://s3.amazonaws.com/files.cnas.org/documents/Lee_Testimony.pdf?mtime=202007 22083241.
11. Shannon Vavra, "The U.N. passed a resolution that gives Russia greater influence over internet norms," CyberScoop, November 18, 2019, https://www.cyberscoop.com/un- resolution-internet-cybercrime-global-norms/.
12. Kristine Lee, "Coming Soon to the United Nations: Chinese Leadership and Authoritarian Values," *Foreign Affairs*, September 16, 2019, https://www.foreignaffairs.com/articles/china/2019-09-16/coming-soon-united-nations- chinese-leadership-and-authoritarian-values.
13. Executive Order 13942 of August 6, 2020, "Executive Order on Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain," *Code of Federal Regulations*, title 3 (2020), https://www.govinfo.gov/content/pkg/DCPD- 202000579/pdf/DCPD-202000579.pdf.
14. Paul LeBlanc and Maegan Vazquez, "Trump orders TikTok's Chinese-owned parent company to divest interest in US operations," CNN, August 14, 2020, https://www.cnn.com/2020/08/14/politics/tiktok-trump-executive-order/index.html.
15. Liza Lin, Aaron Tilley, and Georgia Wells, "TikTok Deal Talks Are Snarled Over Fate of App's Algorithms," *The Wall Street Journal*, September 2, 2020, https://www.wsj.com/articles/tiktok-deal-talks-are-snarled-over-fate-of-apps-algorithms- 11598995674?mod=hp_lead_pos4.
16. "India bans 59 mostly Chinese apps amid border crisis," Reuters, June 29, 2020, https://www.reuters.com/article/us-india-china-apps/india-bans-59-mostly-chinese- apps-amid-border-crisis-idUSKBN24025V.
17. Kiran Sharma, "Indian apps soar after ban on China's TikTok, WeChat and Baidu," *Nikkei Asia*, August 4, 2020, https://asia.nikkei.com/Spotlight/Asia-Insight/Indian-apps- soar-after-ban-on-China-s-TikTok-WeChat-and-Baidu.
18. Manish Singh, "India bans PUBG Mobile, and over 100 other Chinese apps," Tech Crunch, September 2, 2020, https://techcrunch.com/2020/09/02/india-bans-pubg-and- over-100-additional-chinese-apps/.
19. 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.
20. Rasser and Riikonen, "Open Future."
21. Amy Kazmin and Stephanie Findlay, "India moves to cut Huawei gear from telecoms network," *Financial Times*, August 24, 2020, https://www.ft.com/content/55642551-f6e8- 4f9d-b5ba-a12d2fc26ef9.
22. Dylan Welch, Echo Hui, and Stephen Dziedzic, "'Cyber attacks' point to China's spy agency, Ministry of State Security, as Huawei payback, say former Australian officials," ABC News, June 19, 2020, https://www.abc.net.au/news/2020-06-19/cyber-attacks-likely- huawei-5g-ban-payback-from-china-spy-agency/12374374; Arjun Kharpal, "UK should face 'public and painful' retaliation over Huawei decision, Chinese state media urges," CNBC, July 15, 2020, https://www.cnbc.com/2020/07/15/huawei-uk-ban-china-state-media-urges-retaliation- against-britain.html; "China threatens Germany with retaliation if Huawei 5G is banned," *The Straits Times*, December 15, 2019, https://www.straitstimes.com/world/europe/china-threatens-germany-with-retaliation- if-huawei-5g-is-banned.

23. David Hutt, "China's 'mask diplomacy' in pandemic-hit Europe stirs unease," *Nikkei Asia*, March 25, 2020, https://asia.nikkei.com/Spotlight/Coronavirus/China-s-mask-diplomacy- in-pandemic-hit-Europe-stirs-unease; Arjun Kharpal, "Canada and France say donations of coronavirus masks won't influence decisions on Huawei and 5G," CNBC, April 10, 2020, https://www.cnbc.com/2020/04/10/coronavirus-canada-france-deny-masks-will-affect- huawei-5g-decisions.html; and "Governor Cuomo Announces Significant Donations to Help Increase The State's Supply Capacity Amid Ongoing COVID-19 Pandemic," New York State, March 26, 2020, https://www.governor.ny.gov/news/governor-cuomo-announces- significant-donations-help-increase-states-supply-capacity-amid.
24. Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 17, 2019), https://carnegieendowment.org/files/WP- Feldstein-AISurveillance_final1.pdf.
25. Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras- police-government.html; Krystal Hu and Jeffrey Dastin, "Exclusive: Amazon turns to Chinese firm on U.S. blacklist to meet thermal camera needs," Reuters, April 29, 2020, https://www.reuters.com/article/us-health-coronavirus-amazon-com-cameras/exclusive- amazon-turns-to-chinese-firm-on-u-s-blacklist-to-meet-thermal-camera-needs- idUSKBN22B1AL.
26. Kara Frederick (fellow, Center for a New American Security), in discussion with the author, September 2020.
27. Alexander Chipman Koty, "What is the China Standards 2035 Plan and How Will it Impact Emerging Industries?" China Briefling, July 2, 2020, https://www.china- briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging- technologies-what-is-link-made-in-china-2025-goals/.
28. Rasser, Arcesati, Oya, et. al., "Common Code."
29. Paul Scharre and Elsa Kania made important substantive contributions to this section of the paper.
30. "Beijing AI Principles," Beijing Academy of Artificial Intelligence, May 28, 2019, https://www.baai.ac.cn/blog/beijing-ai-principles.
31. Liza Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenges for Washington and Its Allies," *Texas National Security Review*, 2 no. 1 (November 2018).
32. Carnegie Endowment for International Peace, Cyber Policy Initiative, "Interactive Cyber Norms Index,"
33. Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime And The Challenges of Harmonisation," *Monash University Law Review* 40, no. 3 (2016), https://web.archive.org/web/20160430024621/https://www.monash.edu/ data/assets/pdf_file/0019/232525/clough.pdf.
34. Sonia Faleiro, "How India became the world's leader in internet shutdowns," *MIT Technology Review*, August 19, 2020, https://www.technologyreview.com/2020/08/19/1006359/india-internet-shutdowns- blackouts-pandemic-kashmir/.
35. Jamie Tarabay, "Australia Proposes Face Scans for Watching Online Pornography," *The New York Times*, October 29, 2019, https://www.nytimes.com/2019/10/29/world/australia/pornography-facial- recognition.html.
36. Sarah Martin, "Committee led by Coalition rejects facial recognition database in surprise move," *The Guardian*, October 23, 2019, https://www.theguardian.com/australia- news/2019/oct/24/committee-led-by-coalition-rejects-facial-recognition-database-in- surprise-move.
37. Luana Pascue, "Western Australia Joins National facial biometrics matching database," BiometricUpdate.com, April 2, 2020, https://www.biometricupdate.com/202004/western- australia-joins-national-facial-biometrics-matching-database.
38. Office of the Australian Information Commissioner, https://www.oaic.gov.au/.
39. Fergus Hunter, "Already over-extended, Australia's privacy commissioner takes on behemoth Facebook," *The Sydney Morning Herald*, March 14, 2020, https://www.smh.com.au/politics/federal/already-over-extended-australia-s-privacy- commissioner-takes-on-behemoth-facebook-20200312-p549ce.html.
40. Justin Hendry, "Australian privacy watchdog launches investigation into Clearview AI," iTnews, July 9, 2020, https://www.itnews.com.au/news/australian-privacy-watchdog- launches-investigation-into-clearview-ai-550281.
41. Anthony Kimery, "India set to stand up world's largest government facial recognition database for police use," BiometricUpdate.com, March 11, 2020, https://www.biometricupdate.com/202003/india-set-to-stand-up-worlds-largest- government-facial-recognition-database-for-police-use.
42. "Citizenship Amendment Bill: India's new 'anti-Muslim' law explained," BBC News, December 11, 2019, https://www.bbc.com/news/world-asia-india-50670393.
43. Alexandra Ulmer and Zeba Siddiqui, "India's use of facial recognition tech during protests causes stir," Reuters, February 17, 2020, https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of- facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ.
44. Press Trust of India, "Delhi police facial recognition software has only 2 per cent accuracy: HC told," *Business Standard*, August 23, 2018, https://www.business- standard.com/article/pti-stories/delhi-police-facial-recognition-software-has-only-2-per- cent-accuracy-hc-told-118082301289_1.html; Government of India, *The Personal Data Protection Bill*, 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
45. Kosuke Shimizu, Ryosuke Hanada, and Takashi Kawakami, "Japan in race with China for facial-recognition supremacy," *Nikkei Asia*, December 20, 2019, https://asia.nikkei.com/Business/Business-trends/Japan-in-race-with-China-for-facial- recognition-supremacy; SmartCitiesWorld News Team, "Japan to introduce ATMs with facial recognition," SmartCitiesWorld, September 12, 2019, https://www.smartcitiesworld.net/news/news/japan-to-introduce-atms-with-facial- recognition-4575.
46. "Six major airports in Japan set to adopt facial recognition technology by 2020," Future Travel Experience, July 2019, https://www.futuretravelexperience.com/2019/07/six- major-airports-in-japan-set-to-adopt-facial-recognition/.

47. "That's cold: Japan tech blasts snoozing workers with air-con," *The Straits Times*, July 26, 2018, https://www.straitstimes.com/asia/east-asia/thats-cold-japan-tech-blasts- snoozing-workers-with-air-con.

48. "Government to request Japan's gambling venues use facial recognition to restrict admission of addicts," *The Japan Times*, March 8, 2019, https://www.japantimes.co.jp/news/2019/03/08/national/japan-use-facial-recognition- restrict-admission-gambling-addicts/.

49. Personal Information Protection Commission Japan, 2020, https://www.ppc.go.jp/en/.

50. Brian Fung, "Tech companies push for nationwide facial recognition law. Now comes the hard part," *The Philadelphia Tribune*, June 15, 2020, https://www.phillytrib.com/news/business/tech-companies-push-for-nationwide-facial- recognition-law-now-comes-the-hard-part/article_fe78e04e-e8be-5aab-9402- 00203a44510f.html.

51. Rich Thomaselli, "Hawaii Moves Forward With Facial Recognition Technology," Travel Pulse, August 29, 2020, https://www.travelpulse.com/news/destinations/hawaii-moves- forward-with-facial-recognition-technology.html.

52. "We are implementing a one-year moratorium on police use of Rekognition," in *Day One* blog on Amazon.com, June 10, 2020, https://blog.aboutamazon.com/policy/we-are- implementing-a-one-year-moratorium-on-police-use-of-rekognition; Jay Greene, "Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM," *The Washington Post*, June 11, 2020, https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial- recognition/; and Hannah Denham, "IBM's decision to abandon facial recognition technology fueled by years of debate," *The Washington Post*, June 11, 2020, https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/.

53. Kate Cox, "Unredacted suit shows Google's own engineers confused by privacy settings," Ars Technica, August 25, 2020, https://arstechnica.com/tech- policy/2020/08/unredacted-suit-shows-googles-own-engineers-confused-by-privacy- settings/.

54. Kara Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem" (Center for a New American Security, September 3, 2020), https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital- surveillance-ecosystem; Paul Scharre (senior Fellow, center for a New American Security), in discussion with the author, September 2020.

55. Scharre, discussion.

56. Scharre, discussion.

57. Dave Lawler, "The view from the mountaintop," in *Axios World*, January 24, 2020, Axios, https://www.axios.com/newsletters/axios-world-d9a67b4e-7380-4d4e-8caa- f8d181a61ea8.html.

58. Jeff M. Smith, "How America is Leading the 'Quad Plus' Group of 7 Countries in Fighting the Coronavirus," The Heritage Foundation, April 1, 2020, https://www.heritage.org/global-politics/commentary/how-america-leading-the-quad- plus-group-7-countries-fighting-the.

59. Wajahat Khan and Masaya Kato, "China's rise forges new bond between Japan and Five Eyes," *Nikkei Asia*, August 7, 2020, https://asia.nikkei.com/Politics/International- relations/China-s-rise-forges-new-bond-between-Japan-and-Five-Eyes; Daishi Abe and Rieko Miki, "Japan wants de facto 'Six Eyes' intelligence status: defense chief," *Nikkei Asia*, August 14, 2020, https://asia.nikkei.com/Editor-s-Picks/Interview/Japan-wants-de-facto- Six-Eyes-intelligence-status-defense-chief; Reuters, "UK seeks alliance to avoid reliance on Chinese tech: The Times," May 28, 2020, https://www.reuters.com/article/us-britain-tech- coalition/uk-seeks-alliance-to-avoid-reliance-on-chinese-tech-the-times-idUSKBN2343JW; Anja Manuel, "How to Win the Technology Race with China," Stanford.edu, June 18, 2019, https://fsi.stanford.edu/news/how-win-technology-race-china; https://www.cnas.org/technology-alliance-project.

60. Commonwealth of Australia, "Australia's Cyber Security Strategy," August 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy- 2020.pdf.

61. U.S. Cyberspace Solarium Commission, "U.S. Cyberspace Solarium Commission Report," March 2020, https://www.solarium.gov/report.

62. For detailed insight on crafting such an approach, see Christopher B. Porter, "Collective Defense of Human Dignity: The Vision for NATO's Future in Cyberspace" (The Atlantic Council, July 2019), https://www.atlanticcouncil.org/in-depth-research-reports/issue- brief/collective-defense-of-human-dignity-the-vision-for-nato-s-future-in-cyberspace/.

63. Dipanjan Roy Chaudhury, "India, Japan to collaborate on outer space and cyber security projects," *The Economic Times*, July 2, 2019, https://economictimes.indiatimes.com/news/politics-and-nation/india-japan-to- collaborate-on-outer-space-and-cyber-security- projects/articleshow/70033935.cms?from=mdr.

64. Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08- 25/cybersecurity.

65. Recommendations along these lines can be found in U.S. Cyberspace Solarium Commission, "U.S. Cyberspace Solarium Commission Report."

66. U.S. Cyberspace Solarium Commission, "U.S. Cyberspace Solarium Commission Report."

67. Martijn Rasser, "Pandemic Problem: America's Supply Chains are Dangerously Brittle," *The National Interest*, March 17, 2020, https://nationalinterest.org/feature/pandemic- problem-americas-supply-chains-are-dangerously-brittle-134022.

68. Naomi Tajitsu, Makiko Yamazaki, and Ritsuko Shimizu, "Japan wants manufacturing back from China, but breaking up supply chains is hard to do," Reuters, June 8, 2020, https://www.reuters.com/article/us-health-coronavirus-japan-production-a/japan-wants- manufacturing-back-from-china-but-breaking-up-supply-chains-is-hard-to-do- idUSKBN23F2ZO.

69. Humeyra Pamuk and Andrea Shalal, "Trump administration pushing to rip global supply chains from China: officials," Reuters, May 4, 2020, https://www.reuters.com/article/us-health-coronavirus-usa-china/trump-administration- pushing-to-rip-global-supply-chains-from-china-officials-idUSKBN22G0BZ.

70. Pranab Dhal Samanta, "India-Japan-Australia supply chain in the works to counter China," *The Economic Times*, August 19, 2020, https://economictimes.indiatimes.com/news/economy/foreign-trade/india-japan- australia-supply-chain-in-the-works-to-counter- china/articleshow/77624852.cms?from=mdr; Su-Lin Tan, "India, Japan, Australia keen to boost supply chain security by reducing reliance on China," *South China Morning Post*, August 21, 2020, https://www.scmp.com/economy/global- economy/article/3098310/india-japan-australia-keen-boost-supply-chain-security; and "Japan, Australia and India to Launch Supply Chain Initiative," Bloomberg, August 31, 2020, https://www.bloomberg.com/news/articles/2020-09-01/japan-australia-and-india-to- discuss-supply-chains-alliance.

71. Rasser and Riikonen, "Open Future."

72. "Growing Australia's Quantum Technology Industry" (CSIRO, May 2020), https://www.csiro.au/en/Showcase/quantum; "Institute of Photonics and Optical Science," The University of Sydney, 2020, https://www.sydney.edu.au/science/our- research/research-centres/institute-of-photonics-and-optical-science.html.

73. "Blue Dot Network," U.S. Department of State, 2020, https://www.state.gov/blue-dot- network/.

74. "Blue Dot Network"; "EP Association Members & Reporting," Equator Principles, 2020, https://equator-principles.com/members-reporting/.

75. "United States–India Science and Technology Endowment Fund,", https://www.iusstf.org/usistef/us-india-science-technology; "S&T Cooperation," Embassy of India, December 2019, https://www.indembassy-tokyo.gov.in/st_cooperation.html; and "Australia-Japan cooperation in science and technology," Australian Department of Industry, Science, Energy and Resources, November 27, 2019, https://www.industry.gov.au/news-media/science-news/australia-japan-cooperation-in- science-and-technology.

76. A similar idea, specifically for testing of military systems, was proposed by Daniel Kliman, Ben FitzGerald, Kristine Lee, and Joshua Fitt, in "Forging an Alliance Innovation Base" (Center for a New American Security, March 2020), https://www.cnas.org/publications/reports/forging-an-alliance-innovation-base.

77. "Woomera Range Complex," Defence South Australia, 2020, https://www.defencesa.com/precincts/test-and-training-areas/woomera-range-complex#:~:text=The%20Woomera%20Range%20Complex%20is,ground%20and%20spa ce%20test%20activities.

78. Kiran Sharma, "India and Russia in talks over co-manufacturing Sputnik V," *Nikkei Asia*, August 28, 2020, https://asia.nikkei.com/Politics/International-relations/India-and- Russia-in-talks-over-co-manufacturing-Sputnik-V.

79. Brendan Thomas-Noone, "Ebbing Opportunity: Australia and the U.S. National Technology and Industrial Base, United States Study Centre, https://www.ussc.edu.au/analysis/australia-and-the-us-national-technology-and- industrial-base#continuing-challenges-for-ntib-implementation.

80. As proposed by Kliman et al. and Rasser et al.

81. Vivek Raghuvanshi, "India announces ban on 101 imported arms. Who benefits, and who loses out?" *Defense News*, August 13, 2020, https://www.defensenews.com/global/asia-pacific/2020/08/13/india-announces-ban- on-101-imported-arms-who-benefits-and-who-loses-out/.

82. Gueorgui Ianakiev, "Defence Offsets: Regulation and Impact on the Integration of the European Defence Equipment Market," in *The Evolving Boundaries of Defence: An Assessment of Recent Shifts in Defence Activities*, ed. Renaud Ballais (Melbourne: Emerald Group Publishing Limited, 2014), 251–270; "Defence Offset Management Wing," Indian Ministry of Defence, 2020, https://domw.gov.in/.

83. Jon Grevatt, "India releases updated defence offset policy," Janes, July 8, 2020, https://www.janes.com/defence-news/news-detail/india-releases-updated-defence- offset-policy.

84. "Raising FDI cap to 74% in defence manufacturing will be 'game changer': Rajnath Singh," *The Economic Times*, May 16, 2020, https://economictimes.indiatimes.com/news/defence/raising-fdi-cap-to-74-in-defence- manufacturing-will-be-game-changer-rajnath- singh/articleshow/75781028.cms?from=mdr.

85. "Artificial intelligence," Australian Department of Industry, Science, Energy and Resources, https://www.industry.gov.au/strategies-for-the-future/artificial-intelligence; Gleb Chuvpilo, "Who's Ahead in AI Research in 2020? Insights from the International Conference on Machine Learning (ICML 2020)," Medium, July 14, 2020, https://medium.com/@chuvpilo/whos-ahead-in-ai-research-in-2020-2009da5cd799.

86. Asha Barbaschow, "Australian businesses rank last in global artificial intelligence maturity: Infosys," ZDNet, January 17, 2017, https://www.zdnet.com/article/australian- businesses-rank-last-in-global-artificial-intelligence-maturity-infosys/.

87. Steve Lohr, "Universities and Tech Giants Back National Cloud Computing Project," *The New York Times*, June 30, 2020, https://www.nytimes.com/2020/06/30/technology/national-cloud-computing- project.html.

88. "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows" (World Economic Forum, May 2020), http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.

89. Jim Salter, "IBM completes successful field trials on Fully Homomorphic Encryption," Ars Technica, July 31, 2020, https://arstechnica.com gadgets/2020/07/ibm-completes- successful-field-trials-on-fully-homomorphic-encryption/.

90. "Prize Challenges," Defense Advanced Research Projects Agency, https://www.darpa.mil/work-with-us/public/prizes; XPRIZE Foundation, https://www.xprize.org.

91. Siddharth Venkataramakrishnan, "Rigetti to build UK's first commercial quantum computer," *Financial Times*, September 2, 2020, https://www.ft.com/content/cc9b866c- 02fd-4a5c-b283-a17dd3dad6c3; Patrick Tucker, "Can AI Solve the Rare Earths Problem? Chinese and US Researchers Think So," Defense One, August 27, 2020, https://www.defenseone.com/technology/2020/08/can-ai-solve-rare-earths-problem-chinese-and-us-researchers-think-so/168057/.

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