Working Paper

A Comprehensive Approach to Indo-Pacific Allied Technology Cooperation:

Defend, Advance, Assist

Jennifer Jackett & Dr. Charles Edel

1. Introduction

The Biden administration has identified technology as the key field of competition for the twenty-first century as it will prove the most important factor for economic power, national security, and the rules that govern global institutions. Technology is also, increasingly, a dominant feature in strategic rivalry between Washington and Beijing and where “we are going to see increasing maneuvering between the great powers…for pre-eminence,” according to Australia’s Director General of National Intelligence Andrew Shearer. And it is a field where U.S. advantages are most likely to be found in concert with others.

Understanding the importance of technology for economic prosperity, national security, and for the values that govern global norms, countries across the Indo-Pacific have taken measures to shore up their technological future. Multiple nations have invested in critical and emerging technology, prioritized the training of a technologically adept workforce, tightened the rules governing screening of foreign investment and export controls, and endeavored to secure supply chains, pool resources, and collaborate in their efforts to set global rules around the use of technology.

These efforts are critical. But they are not as comprehensive or as coordinated as they could be. The goal should not be complete alignment, as national efforts will be uniquely tailored to a country’s experiences and resources. Yet, a more ambitious and better synched regional effort could yield enormous strategic dividends, including enhancing the technological competitiveness of likeminded partners, better preventing unwanted technology transfer to potential adversaries, and strengthening the resilience of third countries. What follows is an effort to survey key national efforts among like-minded nations in the Indo-Pacific, explore opportunities for closer collaboration, identify issues likely to make closer alignment challenging, and develop a

---

1 Jennifer Jackett is a Sir Roland Wilson Scholar at the National Security College at the Australian National University and a Non-Resident Fellow in the Foreign Policy and Defence Program at the United States Studies Centre at Sydney University. Her doctoral research examines the role of U.S. allies in U.S.-China competition for leadership over advanced technologies. Ms. Jackett is an experienced national security policy adviser and was most recently a Senior Adviser in the Department of the Prime Minister and Cabinet, and is currently on leave from the Australian Government. She has also held roles in the Cabinet Secretary’s Office, Department of Defence, and Office of National Intelligence. Dr. Charles Edel is the inaugural Australia Chair and a senior adviser at the Center for Strategic and International Studies. He previously taught at the University of Sydney, where he was also a senior fellow at the United States Studies Centre. Prior to that, Dr. Edel was a professor of strategy and policy at the U.S. Naval War College and served on the U.S. secretary of state’s Policy Planning Staff from 2015 to 2017. He is the coauthor of The Lessons of Tragedy: Statecraft and World Order (Yale University Press, 2019) and author of Nation Builder: John Quincy Adams and the Grand Strategy of the Republic (Harvard University Press, 2014).

framework for building out technological collaboration through an Indo-Pacific Technology Partnership.

2. Technology Leadership Will Shape the Future Power Balance

Technology has always played a role in relations among states. It is central to comprehensive national economic, political, and military power and the capacity of states to advance their strategic interests in a competitive international system. However, in the early twenty-first century, the geopolitical disruption created by the advent of new technologies has accelerated in both pace and scale. Simultaneous advances in artificial intelligence (AI), quantum physics, and biotechnology have supported opportunities for digital transformation, productivity growth, and improvements in quality of life through medical breakthroughs. Such technologies have also enabled new avenues for malicious cyber activity, espionage, political interference, and disinformation. Whichever states can stay at the forefront of the development, manufacture, use, and governance of the most critical technology will not only be the global technology leaders but will amplify their national power.

In a post-Covid world, the role of technology leadership in the economic resilience of states cannot be underestimated. Supply chain disruptions during the pandemic, along with the weaponization of trade including economic coercion by hostile states, highlighted strategic vulnerabilities associated with the concentration of technology-related raw materials, inputs, and manufacturing in certain countries. In response, many countries have taken steps to decouple or diversify supply chains away from potential sources of dependence through onshoring or near-shoring of critical supply chains, including through industry assistance. Strategic policy in capitals across the world has shifted from a preference for globalization and just-in-time economics to managed openness, and a need for economic security and self-reliance in critical goods.

Amid a shifting geopolitical landscape, technology leadership has also become a battleground between democracies and authoritarian regimes. On March 7, 2022, Australian Prime Minister Scott Morrison highlighted this challenge when he said, “a new arc of autocracy is instinctively aligning to challenge and reset the world order in their own image.”

Democracies are striving to keep the internet and internet-enabled applications free and open and underpinned by core liberal values like freedom of speech and right to privacy. Moreover, democracies are seeking to build secure technology that is resilient to espionage, theft, or interference. Standing in stark contrast, authoritarian regimes are seeking to use technology to enhance the power and legitimacy of the state and oppress everyday citizens including through increased surveillance. Such regimes also seek to exploit the inherent openness of free market economies and societies to undermine democratic institutions and sow division and divide, particularly through ‘grey zone’ tactics like disinformation. Ultimately, whichever system emerges ascendent in this technological competition will be better placed to secure its interests in line with its values.

---


China continues to advance technologically

Today, China’s technological advance has underpinned its emergence as an economic and military power resulting in one of the biggest shifts in the regional and global security environment since the end of the Cold War. China now possesses a growing capacity for world-class research, higher-value exports, and globally competitive companies. It boasts at least three hundred ‘unicorns,’ companies with valuations over USD 1 billion. In cutting edge research with potentially significant military applications, like quantum communications, Chinese scientists have also demonstrated some noteworthy achievements.

Domestically, technology has supported state security and authoritarian rule. Such technologies have been employed to closely surveil minority groups, notably Muslim Uighurs in Xinjiang. Internationally, the growth and successes of Chinese technology companies like Huawei, as well as China Mobile, Alibaba, Baidu, and Tencent, has underpinned China’s role in technology markets and the commercial and strategic imperatives for China seeking a bigger role in technology standard-setting and data governance. The Chinese state has also leveraged its technology companies as an increasingly active infrastructure provider to third countries through its ‘Digital Silk Road’ initiative.

China’s continued advances are no accident. Science and technology are central to the Chinese Communist Party’s (CCP) agenda for self-reliance and national rejuvenation. China has seen decades of state-led development and industrial policy initiatives, including the ‘Made in China 2025’ high-tech manufacturing plan released in 2015. Within the decade, Xi Jinping has declared he wants China to become a world leader in AI. China’s approach of ‘civil-military fusion’ has also aimed to support civilian technological advances being quickly translated into military capabilities, and China is now thought to be at the forefront of military technology in some specific areas, like shipbuilding, land-based conventional ballistic and cruise missiles, and integrated air defense systems.

But many challenges remain to China realizing its technology ambitions. Industry subsidies bring inefficiencies and duplication of effort. For critical inputs, like semiconductors, China still relies largely on foreign technology, despite investments to develop domestic capacity. The

---

regulatory environment has also become more challenging as the Chinese state has sought to regulate data and impose additional cybersecurity obligations on Chinese companies, also impeding their overseas operations. China also stands accused of adopting underhanded market practices, such as industrial espionage and intellectual property (IP) theft, to gain access to sensitive technology to accelerate its efforts.\(^\text{10}\) As a result, Chinese researchers, technology companies, and investors have had to navigate growing scrutiny abroad.

**U.S. technological competitiveness is under challenge**

The United States remains the world’s dominant technology power. On measures from basic research output to leading companies, the United States has been at the forefront of global technological advancement since the end of World War II. It is the home of innovation and entrepreneurial spirit, the world’s best research institutions, and a highly competitive and thriving environment for global technology companies and talent. But even with the difficulties China faces in its pursuit of becoming a high-tech power, the technology dominance of the United States is under challenge. This is not only due to the relative increase in China’s capabilities, but underinvestment in areas that support competitiveness like research and development (R&D).\(^\text{11}\) A shift in the global center of innovation, talent, and market share away from the United States has serious ramifications for foundations of U.S. power.

To be sure, both U.S. and Chinese governments, businesses, and consumers have benefitted immensely from deep technology cooperation over decades. This cooperation has provided access to capital, knowledge, talent, inputs, and goods that have driven the development of the digital economy in both countries, and globally. U.S. companies want to continue to profit from trade with China, and vice versa. Yet, the balance of opportunity and risk for U.S. technology cooperation with China has now shifted. U.S. concerns about supply chain dependencies, espionage and interference, and unwanted Chinese access to dual-use technologies have prompted a re-think of how, and in which areas, cooperation occurs. The emphasis of U.S. leaders in the current and former administration is now on how to protect U.S. national and economic security vis-à-vis China.

Under the Trump administration, wide-ranging measures were implemented to manage perceived risks. The U.S. government restricted the access of Chinese technology companies to U.S. markets, most notably by banning Huawei 5G telecommunications technology. In 2018, the passage of the Foreign Investment Risk Review Modernization Act (FIRRMA) expanded the authority of the Committee on Foreign Investment in the United States (CFIUS) and introduced new mandatory filing requirements.\(^\text{12}\) Numerous technology items were also added to the U.S. ‘entity list’ to prevent U.S. export licenses of sensitive technologies to Chinese firms. Internationally, the Trump administration advocated for similar approaches among allies and

---


partners, such as through the ‘Clean Network,’ which in part aimed to exclude Chinese telecommunications companies from partner economies.

The Biden administration reset U.S. technology strategy by embarking on a more positively-focused approach to defend and enhance U.S. technological competitiveness through wide-ranging policy reform, legislation, and funding. In his first address to Congress, President Biden made clear that his goal is to “develop and dominate the products and technologies of the future.” Although many of the protective measures introduced in the Trump era have continued in support of this objective, Biden’s strategy can be distinguished by its focus on long-term initiatives to secure critical technology supply chains, invest in R&D, and develop digital infrastructure. This will be further bolstered once a Conference Committee reconciles the House-passed America Competes Act and Senate-passed United States Innovation and Competition Act for presidential sign-off. The final bill is expected to include around USD 52 billion in funding to support semiconductor manufacturing and increased funding for the National Science Foundation (NSF), among many other initiatives. The ambition and breadth of current U.S. technology strategy is commendable, although the real test of its impact will be timely implementation and sustained advances over generations, not years.

*Indo-Pacific allies key to collective technological edge*

While President Biden has laid a new blueprint for U.S. domestic technological rejuvenation, U.S. allies are an important layer and force multiplier of U.S. technology strategy, as well as broader strategic competition with China. The United States knows that acting alone will be insufficient to sustain its technological advancement. The United States relies on the global scientific community for access to leading talent and to support cutting-edge research. Technology supply chains are global and dispersed, such that U.S. self-reliance is an unrealistic, or at least very expensive, proposition. Efforts to guard against technology leakage to China will also be futile if like-minded partners do not adopt similar approaches. The major markets and the advanced technology players of the Indo-Pacific, including Japan, South Korea, India, and Taiwan, are also critical to the trajectory of global technology leadership.

---


In recognition of the role of U.S. allies and partners, new technology-focused partnerships have been a signature of the Biden administration’s Indo-Pacific engagement. The United States has sought to coordinate efforts on issues including harmonizing regulatory approaches to defend the leakage of critical technology to potential adversaries, addressing shortages of strategic technologies like semiconductors by leveraging the unique place of partners in the supply chain, and integrating defense and industrial bases. Cooperation on advanced military capabilities in areas such as AI, quantum computing, cyber, undersea, and hypersonic flight, was a central pillar of the AUKUS trilateral security partnership announced between the United States, Australia, and the United Kingdom in September 2021. Critical and emerging technology has also been a core stream of work for the reinvigorated, and increasingly high-profile, Quadrilateral Security Dialogue (‘the Quad’) between the United States, Australia, India, and Japan.

3. Regional Responses Growing but Prioritization Required

The increasingly prominent focus on critical technology across the Indo-Pacific does not just reflect U.S. concerns. Rather, from India and Australia to Japan and South Korea, there are converging strategic imperatives pulling Indo-Pacific democracies together. Specifically, they all have an ambition to advance their technological competitiveness to support the transformation of their economies and societies, as well as the development of cutting-edge military capabilities. Each country possesses a shared interest in a reliable, secure, and diverse supply of critical technology. And they have all stated that they want such technology to be developed and used in a way that aligns with liberal democratic values. Finally, each occupies different but broadly complementary roles in global technology supply chains, bringing to the table strengths across research, workforce, materials, capital, manufacturing capacity, and regulatory frameworks. These converging strategic imperatives have manifested in growing layers of bilateral, minilateral, and multilateral diplomatic initiatives and agreements among Indo-Pacific democracies (see Annex A – Examples of Allied Indo-Pacific Technology Cooperation).

Techno-diplomacy taking hold across the Indo-Pacific

Bilateral forums have been the clearest route for agreeing and advancing ambitious critical technology initiatives, particularly where joint investment is concerned. Following U.S. and allied decisions to exclude high-risk Chinese vendors over the preceding years, like-minded countries have focused on practical initiatives to improve the security and diversity of 5G telecommunications providers. For example, U.S. and South Korean leaders agreed in 2021 to

“work together to develop open, transparent, and efficient 5G and 6G network architectures using Open-RAN technology.” Shortly after, the United States and Japan announced the Competitiveness and Resilience (CoRe) Partnership, which also committed USD 4.5 billion for research, development, testing, and deployment of 5G and next generation networks. Critical technology supply chain vulnerabilities highlighted by the Covid-19 pandemic have also led to growing bilateral and public-private cooperation. U.S. and Japanese leaders, and U.S. and South Korean leaders, have each committed to deepening cooperation on sensitive supply chains, particularly semi-conductors. On upstream supply issues, Australia and the United States have pursued critical minerals cooperation, a key input to advanced civilian and military technology. In 2021, the U.S. Department of Defense awarded a USD 30 million technology investment agreement to Australian company Lynas Rare Earths to establish U.S. processing capabilities for rare earth elements. Such projects have been complemented by broader statements of intent among a growing array of partners. The 2021 Australia-South Korea Memorandum of Understanding on Cyber and Critical Technology Cooperation, for instance, supports closer information sharing, and cooperation on the design, development, and use of secure critical technology, as well as norms and standards development. South Korea and India have also committed to enhancing cyber and critical technologies cooperation and collaboration on R&D in the defense sector. Each arrangement creates the framework, and bureaucratic connections, for deeper practical cooperation in the long-term.

Minilateral groupings of like-minded countries have taken center stage as a preferred pathway for Indo-Pacific democracies to advance their critical technology interests due to their small and flexible nature. Most notably, in March 2021, Quad leaders announced the establishment of a Critical and Emerging Technology Working Group, which has since produced key guiding principles on ‘Technology Design, Development, Governance, and Use.’ The challenge for the working group moving forward is translating a broad agenda on issues like telecommunications, transfers, and technology cooperation into concrete projects.

---

standards, horizon scanning, and Science, Technology, Engineering, and Math (STEM) talent into practical actions that make a difference.\textsuperscript{25} AUKUS represents an even more ambitious minilateral grouping. The enhanced trilateral security partnership announced by Australia, the United States, and United Kingdom in September 2021 commits to a step-change in defense technology cooperation in response to a deteriorating regional security environment.\textsuperscript{26} This is expected to occur through deeper integration of the three science and technology, defense, and industrial bases. The success of AUKUS will be contingent on long-term political will, successful negotiations on complex legal and administrative arrangements to enable technology transfer, and substantial investments—especially by Australia—to build the necessary workforce, basing, and sustainment capabilities. Ultimately, AUKUS will also provide a litmus test for the significant potential of minilateral arrangements to advance a critical technology capability edge among like-minded states, and even to shape and deter adversary behavior in the region.

Multilateral groupings involving countries across the region have tended to focus on dialogue and norm building and have been weaker when it comes to practical actions. That is not to undervalue their value. They are an important layer for sharing perspectives, identifying common challenges, and providing the chance for frank engagement with non-like-minded countries. For example, the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace involved twenty-five countries, including Australia, China, Indonesia, Japan, Singapore, the United States, and the Russian Federation. In their final report to the General Assembly in 2021, the group concluded that international law applies to cyberspace, and that “States must not intervene directly or indirectly in the internal affairs of another State, including by means of Information and Communications Technologies.”\textsuperscript{27} Such agreements provide a mechanism for countries to hold each other to account if, and when, they are breached.

In its various forms, the techno-diplomacy occurring across the region is a positive development. But for like-minded democracies to both maintain, and capitalize on, current political momentum in support of their shared interests, timely implementation of commitments already made is critical. As the bandwidth of every country’s leader and bureaucracy is finite, regional leaders also need to decide on where best to focus attention to achieve the greatest strategic effect, in the short and long-term. Groupings that support practical action should therefore take precedence.

4. **National Responses Strengthening but Closer Harmonization Necessary**

In addition to optimizing their diplomatic agenda, regional leaders need to understand where current national approaches align or diverge, and on what issues such differences matter. There is scope to better harmonize varied regulatory approaches to protect critical technology, coordinate steps to improve technological competitiveness, and dovetail investment in regional infrastructure. Left unaddressed, differences could lead to weak links in the defense of critical technology from unwanted technology transfer, overlapping initiatives and investments, or problematic gaps in assistance to third countries.

*Areas of policy alignment and opportunities for closer coordination*

Foreign investment screening provides a good example of where many countries, including Australia, Japan, South Korea, and New Zealand, appear to be moving in a similar direction toward tightening regulatory frameworks to better manage concerns arising from foreign investment. Australia introduced major national security reforms to its foreign investment framework in January 2021, including mandatory notification requirements for proposed investments in businesses that develop, manufacture, or supply critical technology for military or intelligence purposes. Of 730 non-residential foreign investment applications in the first six months of the updated screening regime, 60 were notifiable or reviewable national security actions which would previously not have been reviewed, resulting in 13 having conditions applied to protect national security as part of their approval. Prior to the Covid-19 pandemic, India was on a different path, seeking to liberalize the foreign investment screening regime. However, in April 2020, India tightened its screening requirements, in part to mitigate the risk of opportunistic acquisitions by foreign buyers during the pandemic economic downturn, but also to increase scrutiny of Chinese acquisitions amid growing geopolitical tensions.

Likewise, since the early days of the pandemic, like-minded democracies have sought to strengthen their national supply chain resilience. In 2020, Japan committed USD 535 million (JPY 57.4 billion) in subsidies for Japanese companies to relocate factories out of China back to Japan or other countries in Southeast Asia to reduce its trade dependence. In Australia, where supply chains proved generally resilient despite the cumulative shocks of the pandemic, Chinese

---


economically coercive, and natural disasters, the government has sought to support business through measures like the Export Market Development Grants. In the United States, a range of initiatives and investments have followed the 100-day supply chain review released in June, including around USD 50 billion for semiconductor manufacturing, USD 7 billion for battery production, and USD 10 billion in support to small businesses.  

However, on evolving threats like countering foreign interference, including in research, there is more variation—and shortcomings—in regional responses. Australia has been active in its approach, including passing legislation that criminalizes covert and deceptive activities of foreign actors and establishing a transparency register of foreign influence in government and political processes. Australian government agencies have also worked in partnership with the university sector to protect research, for example, the Australian Security Intelligence Organization briefed universities or university affiliated forums more than 60 times in 2020-21. This has resulted in better sectoral awareness and management of risks through governance, due diligence, and transparency measures, as well as cybersecurity improvements. Japan has no directly relevant legislation, but in 2021, Japan tightened researcher reporting requirements for financial contributions from foreign or external sources. India has taken several actions to strengthen its research security, including restricting academic collaborations with Chinese institutions in 2019, a departure from the country-agnostic approach of Australia and Japan, and now also requires government approval for academic events sponsored by overseas or involving foreign participation. India also strengthened the Foreign Contribution (Regulation) Act in 2020 to

---

improve transparency over foreign sources of funding to Indian organizations. South Korea has no specific law in relation to foreign interference, although its Political Funds Act prevents foreign political donations.\(^{38}\) Countering foreign interference in research presents a strong case for greater information sharing and better aligning national responses.

Although countries have also varied in their steps to advance technological competitiveness, almost all countries have acted, whether through funding for basic research, co-investment with private industry, or direct assistance to support sovereign capabilities. Australia’s USD 1.1 billion (AUD 1.5 billion) 2020 \textit{Modern Manufacturing Strategy} aims to support industry to become more competitive and resilient, including in the defense, space, and critical minerals sectors.\(^{39}\) Underpinning actions range from improving tax settings and aligning research to priority areas to addressing gaps in critical supply chains.\(^{40}\) In South Korea, the government and semiconductor companies together will invest USD 450 billion this decade to become a global chip base, with South Korean companies also committing USD 40 billion in investments to support U.S. semiconductor manufacturing.\(^{41}\) The biggest divergence among partners appears to be the level of government appetite to directly fund industry assistance, with many countries in the region not going as far as the United States in their industrial policies.

Like-minded partners have also played different roles in efforts to assist third countries to manage the risks and capitalize on the opportunities associated with critical technology. Australia’s ‘Cyber and Critical Tech Cooperation Program’ guided by its International Cyber and Critical Technology Engagement Strategy includes USD 15 million (AUD 20.5 million) dedicated to strengthening resilience in Southeast Asia and USD 12.5 million (AUD 17 million) to support Pacific countries to counter cybercrime and disinformation.\(^{42}\) Together, the United States and Japan are also promoting secure connectivity in the Indo-Pacific, including through cybersecurity capacity building as part of the Global Digital Connectivity Partnership.\(^{43}\)

---


Other initiatives have focused more directly on the provision of digital infrastructure in third countries, with activities ranging from technical advice and training to project certification and co-investment. For instance, the ‘Blue Dot Network,’ launched by the United States, Japan, and Australia in 2019, provides assessment and certification of regional infrastructure projects in line with infrastructure standards and guidelines set by the G20, G7, and OECD to help mobilize private sector investment. In 2019, South Korea established a USD 423 million Global Plant, Construction, and Smart City Fund, along with a ‘Smart City Global Cooperation Program’ to provide technical expertise and training, as well as planning and investment support to third countries, including the Philippines, Indonesia, and Vietnam. The focus of these initiatives has been high-quality and sustainable projects, in part seeking to provide an attractive counteroffer to China’s Belt and Road Initiative (BRI).

Despite some variation and differences in national approaches, the goal is not to achieve complete alignment across responses of like-minded democracies. Instead, if cooperation was better synched, this could pay large dividends, and help distribute costs more evenly. The key issue is how to ensure their efforts to defend and advance their critical technology interests are complementary, coordinated, and comprehensive.

5. Towards an Indo-Pacific Technology Partnership to Defend, Advance, and Assist

Though there are many layers of regional techno-diplomacy, there remains a clear opening and need for a broader grouping among Indo-Pacific nations—inclusive of major players like South Korea, but also smaller players like New Zealand. This could be considered an informal alliance of like-minded countries, although it might be better thought of as an ‘Indo-Pacific Technology Partnership’ (IPTP). The main purpose of the IPTP would be to have a ministerial and bureaucratic central touch point for critical technology policy coordination. Such an arrangement should not displace existing cooperation growing through groupings like the Quad. Instead, it would provide an opportunity to convene ministers and senior officials at least annually to share information and coordinate joint action as opportunities arise. The IPTP could also be expanded to encompass like-minded countries outside the immediate region, but which still have common interests and an important stake in how technology dynamics in the region unfold, such as the United Kingdom, European Union, and Canada.

An agenda for an Indo-Pacific Technology Partnership

A common challenge of existing techno-diplomacy is the breadth of potential areas of cooperation among like-minded partners. Instead of seeking to add to this agenda, a regional technology partnership could be most helpful by reinforcing and building on areas of cooperation that are the most pressing and likely to have the greatest impact. The three initial areas of focus recommended are: regulatory harmonization to counter foreign interference in research; security and diversification of 5G telecommunications supply chains; and coordinating approaches to regional digital infrastructure investment.

Priority 1: Regulatory harmonization to counter foreign interference in research

Countering foreign interference and unwanted knowledge transfer in sensitive areas of research requires closer coordination among like-minded states to address national and collective vulnerabilities in relation to critical technology protection. As part of the IPTP, members should convene to share threat intelligence where possible, including information on the specific technologies of most interest to hostile actors, as well as those areas of comparative advantage requiring closer protection. Discussions should also focus on lessons learned from different policy approaches and their impacts to support best practice, including how to balance important considerations around maintaining an open and collaborative scientific community while adequately protecting research in a targeted and proportionate way. This issue could be the first topic of many as part of a broader agenda on regulatory harmonization, with future areas of focus to include issues like foreign investment screening, export controls, and critical infrastructure regulation.

Priority 2: Security and diversification of 5G telecommunications supply chains

With the rollout of 5G communications technologies underway across the region, the security and diversity of 5G supply chains needs sustained focus by like-minded partners. The IPTP could helpfully build on bilateral and minilateral 5G initiatives, such as the Quad’s work with the Open Radio Access Network Policy Coalition, to support security, openness, and interoperability of 5G telecommunications networks. Discussions should focus on research and testing of 5G and next generational communications technology, joint standards development including cooperation in multilateral standard-setting fora, and co-investment with private sector partners to help diversify hardware and software suppliers. This issue could be the first supply chain topic for the IPTP, which could be followed by other supply chain discussions focused on priority areas such as semiconductors and critical minerals.

Priority 3: Coordinating approaches to regional digital infrastructure investment

Assistance to third countries through digital infrastructure investment could have a substantial impact on their capacity to capitalize on the vast economic and social opportunities associated with critical technology, while managing national security risks. The IPTP could help focus the efforts of like-minded countries by mapping what digital infrastructure investment is already occurring and where, to understand areas of potential overlaps and gaps. This could then
inform a comprehensive strategy to guide national, bilateral, and minilateral regional infrastructure investment, and in line with the Blue Dot Network’s proposed certification framework for quality infrastructure. An annual meeting should occur to check progress and identify priority follow-on areas of investment. The private sector will be an essential partner in this initiative to support the financing and commercial viability of projects, with co-investment and support from government partners where needed to get projects off the ground.

**Barriers to cooperation remain, but are not without a way forward**

Despite many common geostrategic interests, realizing the potential of the Indo-Pacific Technology Partnership is not without barriers. Three stand out: managing different approaches to China, leveraging the key role of private industry, and navigating competing commercial equities. These are not reasons not to pursue closer cooperation, though they will require careful management.

Unique strategic, political, and economic contexts mean that each country will view its role in strategic competition over critical technology differently, and how it manages related issues in its bilateral relationship with China. The United States has been forward leaning in identifying the risks posed by China to critical technology security and in its aim of competing with the China for technological dominance. Japan recognizes China as a growing security threat but frames its steps to defend and advance its technological competitiveness in terms of economic security.46 This is similar to South Korea, which also remains sensitive to any steps that might provoke Chinese economic retaliation.47 India has sought to restrict technology collaboration with China in specific areas like 5G and sensitive research, amid broader concerns about Chinese influence in South Asia.48 Australia has adopted a country-agnostic approach to its critical technology policy, but has called out Chinese behavior in specific instances, like attributing malicious cyber activity.49 Australia has also been clear in pushing back against China in response to political pressure and economic coercion.50 New Zealand released a frank assessment of China’s ambitions to reshape the international system, though on sensitive policy issues has generally preferred to adopt less forthright approaches.51 To help manage some of these sensitivities, it will be important that the IPTP maintains a positive agenda focused on advancing the group’s technological edge and the


provision of helpful public goods to the region, as much as mitigating risks from potential adversaries.

All the suggested areas of cooperation either directly involve, or impact, private industry. The success of closer collaboration across the region therefore depends upon constructive and close relationships with industry partners. That means understanding the effect of regulatory approaches on businesses and consumers and seeking to limit actions that carry additional costs unless necessary. For supply chain security initiatives and infrastructure investment, governments need to focus on the incentives and co-investment options they can provide to private industry to support such initiatives, especially where such investments are strategically significant but the commercial viability may be more challenging.

Like-minded countries across the region may share common geostrategic interests, but commercially, their companies are also competing intensely for trade and investment opportunities. Tensions between the security and economic interests of governments may lead to different calculations in relation to the desired level of regulation in the economy, or a government’s willingness to provide direct industry investment and support. Where there are differences in those policy choices between like-minded countries, overly protectionist approaches by one country may cause concern for countries preferring to limit free market interventions. Improving information sharing on the basis for decisions and regularly identifying areas for closer alignment is key to reducing costly differences between partners.

Annex A. Examples of Allied Indo-Pacific Technology Cooperation

<table>
<thead>
<tr>
<th>Construct</th>
<th>Initiative*</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bilateral</td>
<td>India-Japan Special Strategic and Global Partnership (2014) (includes civilian and defense tech cooperation)</td>
<td>India, Japan</td>
</tr>
<tr>
<td></td>
<td>India-Korea Special Strategic Partnership (includes critical technologies) (2015)</td>
<td>India, Republic of Korea (ROK)</td>
</tr>
<tr>
<td></td>
<td>Australia-Indonesia Memorandum of Understanding on Cyber Cooperation (2018)</td>
<td>Australia, Indonesia</td>
</tr>
<tr>
<td></td>
<td>Australia-Thailand Memorandum of Understanding on Cyber and Digital Cooperation (2019)</td>
<td>Australia, Thailand</td>
</tr>
<tr>
<td></td>
<td>Australia-Singapore MoU on Cyber Security Cooperation (2020)</td>
<td>Australia, Singapore</td>
</tr>
<tr>
<td>Working Paper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Minilateral</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australia-ROK ‘Memorandum of Understanding on Cyber and Critical Technology’ (2021)</td>
<td>Australia-ROK</td>
<td></td>
</tr>
<tr>
<td>U.S.-Japan Competitiveness and Resilience Partnership (2021)</td>
<td>U.S., Japan</td>
<td></td>
</tr>
<tr>
<td>United Kingdom-Australia Cyber and Critical Technology Partnership (2022)</td>
<td>United Kingdom, Australia</td>
<td></td>
</tr>
<tr>
<td>Five Eyes Technical Cooperation Program</td>
<td>U.S., UK, Canada, Australia, New Zealand</td>
<td></td>
</tr>
<tr>
<td>Digital Economy Partnership Agreement (2020)</td>
<td>New Zealand, Chile, Singapore</td>
<td></td>
</tr>
<tr>
<td>‘AUKUS’ enhanced trilateral security partnership (2021)</td>
<td>Australia, U.S., UK</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Resilience Initiative (2021)</td>
<td>Australia, India, Japan</td>
<td></td>
</tr>
<tr>
<td><strong>Multilateral</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996) (42 countries)</td>
<td>Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, ROK, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and U.S.</td>
<td></td>
</tr>
<tr>
<td>ASEAN Regional Forum Information and Communications Technologies Work Stream (2015)</td>
<td>10 ASEAN member states; 10 ASEAN dialogue partners; Bangladesh, the Democratic People’s Republic of Korea (DPRK), Mongolia, Pakistan, Sri Lanka, Timor-Leste; and one ASEAN observer (Papua New Guinea)</td>
<td></td>
</tr>
<tr>
<td>Australia, ASEAN member states</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiative/Conference</td>
<td>Members/Signatories</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>United Nations General Assembly Group of Governmental Experts on Advancing responsible State behaviour in cyberspace (2019-2021)</td>
<td>Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, Uruguay</td>
<td></td>
</tr>
<tr>
<td>G7 Build Back Better World Initiative (2021)</td>
<td>U.S., Japan, Canada, France, Germany, Italy, UK</td>
<td></td>
</tr>
<tr>
<td>Global Partnership on Artificial Intelligence (2020)</td>
<td>Australia, Canada, EU, Germany, India, France, Italy, Japan, New Zealand, ROK, Singapore, Slovenia, UK, U.S.</td>
<td></td>
</tr>
</tbody>
</table>

*Highest level of agreement or arrangement captured (i.e., not all relevant underpinning dialogues or meetings are included)*

## Acknowledgements

The authors would like to thank George Cross from the Australian National University for his valuable research support. The authors are grateful for helpful feedback and comments provided by CSIS representatives and stakeholders in a CSIS-hosted roundtable in March 2022. Nonetheless, the authors are responsible for all content and arguments contained in the paper.