Australian National University

National Security College

China Inc. and Indonesia's Technology Future

Response Options

Dirk van der Kley, Benjamin Herscovitch, Gatra Priyandita

Key Points

- Indonesia's technology choices will impact the regional contest for influence and technological leadership. Australia and other Quad countries need to do more to positively shape these choices.

- A lack of trained talent and infrastructure shortfalls are the biggest obstacles to further develop Indonesia's digital industries.

- Huawei and other firms backed by the Chinese government are providing free large-scale technology training to Indonesian officials, professionals, and students. Huawei alone is training tens of thousands of Indonesians every year. This is steering Indonesia's current and future tech leaders towards Chinese technology.

- Australia and other Quad countries do not have a coherent or well-resourced response to China's approach. Australia's focus on cyber norms and security misses Indonesia's needs for concrete technical training.

Key Recommendations

- Australia, in concert with other Quad countries, should deliver a vocational technology training program that is large enough to genuinely improve Indonesia's technology capacity and offer alternatives to Chinese state-backed technology and training.

- Large tech firms from Quad countries should contribute their technology and expertise to an internationally accredited vocational program. Australia's vocational education and training sector should also help develop people-to-people and educational links with Indonesia.

Huawei and other firms backed by the Chinese government are training Indonesian tech workers, government officials and students on an industrial scale for free.[1] This is good for Indonesia. The biggest blockage to Indonesia's digital development is a lack of trained talent and China is filling that gap. However, this is not completely altruistic, as training has become a key plank for pushing China's geopolitical tech ambitions. By comparison, Australia and other Quad countries have not done as much as China to build technology skills in Indonesia.[2]

China will remain a strong technological player in Indonesia. But it is in Australia's interest that Indonesia gets its training and technology from various sources.

So far Australia has stressed the cybersecurity risks of Huawei and other Chinese firms but has not offered viable alternatives to Indonesia. In Indonesia, Huawei is seen as a key cybersecurity partner because it helps build the country's capacity to combat cybercrimes. Australia alone cannot compete with China, but with the Quad it can develop a serious technology training program that is good for Indonesia's digital development and ensures a range of technology options.

Indonesia's digital imperative

Indonesia has not meaningfully closed the economic divide with advanced industrial economies. The gap in GDP per capita (current USD) between the US and Indonesia has risen from $23,710 in 1991 to $59,723 in 2020. Economic opportunity remains the dominant policy priority for Jakarta.

Indonesia — like many emerging economies — has seen that new jobs and wage growth are in the tech-led disruption of traditional industries. With 202 million internet users contributing US$70 billion to Indonesia's digital economy in 2021, the Indonesian government is banking on the transformational powers of digital technology to bolster economic growth.[3]

In some ways, Indonesia's digital ecosystem is more vibrant than Australia's. There are numerous e-commerce unicorns, which have transformed lives across the country. Competition is fierce and Indonesian firms are cutting-edge. But Indonesia is also a country where large swathes of the population have limited or no access to the internet and massive skills shortfalls remain.

Skills and infrastructure are the biggest hurdles to further digital development. A 2018 World Bank report found that Indonesia was facing serious ICT skill shortages and projected that Indonesia needed nine million skilled and semi-skilled ICT workers by 2030.

Meanwhile, although Indonesia has seen its digital connectivity improve steadily over the past decade, its ICT infrastructure remains insufficient to provide good quality internet to the nation's 270 million people. Internet access is also unequal, with much of the infrastructure concentrated in urban Java.

The primary risk is that digital development fails, and vital jobs never emerge. For Indonesia to address this risk, external assistance to overcome the infrastructure and talent challenge is welcome. Western concerns about Chinese investment in Indonesia often fail to appreciate this point. As one senior Indonesian official told the authors: "If we're constantly afraid, our development will stagnate."[5]

The most urgent cybersecurity threat for the Indonesian government is cybercrime. Indonesia is one of the most vulnerable countries to cybercrime on earth.[6] Data security is poor and Chinese firms are seen as partners for swift solutions. The Indonesian government understands the threat of Chinese espionage and that heavy reliance on Chinese technology could lead to political pressure.[7] But government officials have also expressed concern about the risk of espionage from Australia and the United States.[8] So, from Indonesia's perspective there will be cybersecurity vulnerabilities regardless of who supplies the underlying infrastructure.

China's technology training in Indonesia

Chinese firms — and increasingly the Chinese government — are helping Indonesia fill its infrastructure and talent gaps. One of the keys to their success is offering good quality products at lower prices than competitors.[9] Sometimes this is backed with export credits for Indonesian firms and Chinese-state support for research and development. This is reinforced by less costly maintenance and upgrade options. More importantly, there are also huge promises to develop the next generation of Indonesian tech talent.

Since the mid-2000s, Chinese firms have created training centres in partnership with local Indonesian telcos and universities to build the tech workforce. In April 2011, Huawei established an ICT training centre at the prestigious Bandung Institute of Technology to teach Indonesian students and researchers about internet protocols. Huawei has also signed agreements with other major universities to help develop digital talent.

And big universities are not the only ones being approached — smaller regional universities are given much needed resources and training programs too. In 2020, Huawei alone had pledged to give ICT training to up to 100,000 Indonesians. Outside of these training programs, Indonesians benefit from many scholarship programs, workshops, and bootcamps hosted by Chinese ICT firms to hone their tech skills.

Government agencies, too, are targets of training and capacity building programs. Huawei has claimed that 7,000 government officials have participated in various training activities and programs through the collaboration between Huawei and the National Cyber and Crypto Agency (BSSN), Indonesia's cybersecurity agency.

While other foreign ICT companies are also investing in technical vocational education in Indonesia, none have come close to matching the scale that Huawei and other Chinese firms — particularly Alibaba and ZTE — are providing.

An opportunity for the Quad

Indonesia's development priorities and technology skills shortfalls represent an opportunity for practical Quad collaboration. A large-scale program to provide specific technical training for Indonesia's digital workforce would contribute to the Quad's objectives of promoting an economically prosperous and secure Indo-Pacific. Such a program would also dovetail with each Quad country's efforts to deepen their political and people-to-people ties with Indonesia.

Australia should leverage Quad leaders' meetings and other gatherings of senior officials to advocate for boosting technology training in Indonesia. Such a program would add an extra concrete initiative to the Quad agenda and further enhance the grouping's image among South-East Asian countries as a provider of regional public goods.

Given the Quad's tendency to focus its efforts regionally, an initiative in Indonesia could be used as the beginning of an ASEAN-wide program to raise digital skills. By focussing on the provision of such manifestly beneficial public goods, such a program would also help blunt China's criticism that the Quad is sowing regional divisions. Given Indonesia's influence in ASEAN and its economic and demographic weight in the region, such a program would also amplify longstanding Quad support for ASEAN.

Australia's funding for this program could come from its aid and international education budget. Indonesia receives the second largest portion of Australia's aid spending. Redirecting just a few million from the roughly A$300 million of Australian aid to Indonesia would allow Australia to stand up a well-resourced digital training and capacity building initiative. With Japan and the United States also operating substantial aid programs in Indonesia, Washington and Tokyo could also help fund such a program.

This training and capacity building program would also offer opportunities for Australia to deepen its engagement and cooperation with a range of partners beyond the Quad. South Korea and the European Union (EU) are each home to world-leading technology companies, especially in the provision of ICT infrastructure. Despite this, these companies play a minor role in the Indonesian market, which their Chinese competitors dominate.

South Korea and the EU stand to benefit both commercially and strategically by partnering with Australia and the Quad on a training and capacity building program in Indonesia. Such an initiative would complement the EU's 'Strategy for cooperation in the Indo-Pacific' and would augment South Korea's efforts to deepen its ties in South-East Asia.

Private sector and educational partnerships

As well as high-level political support and government funding, such a program should also involve both vocational educational institutions and the private sector. Educational institutions that provide technical training should be encouraged to contribute expertise and services to this program. Noting India's huge capacity to produce highly skilled technology workers, there is likely to be an especially important role for Indian technical colleges in the roll out of this program.

By leveraging Australia's existing cyber capacity-building activities in Indonesia, Australian diplomats should begin scoping opportunities for Australia's, and other Quad countries', vocational education institutions to partner with local educational and private sector organisations in Indonesia to provide additional training and capacity building. The focus should be on higher volume, short-term courses to get people job-ready quickly. Australia could also offer additional short-term scholarship programs for Indonesians to acquire additional technical skills with Australian universities and vocational education institutions.

To enhance the quality and international recognition of this training and capacity-building program, it should use the expertise and technical capacity of a range of Quad countries' technology companies. Although the Australian private sector may lack the scale to provide necessary training in Indonesia, the Quad countries combined can overcome these human capital and technical constraints.

There should be as much flexibility in the program as possible to meet the needs of a mobile and geographically dispersed workforce. Courses could be delivered online and in hybrid formats. They could combine with the wide range of free digital skills training already offered online. The key priority is that more Indonesians get ICT skills quickly.

As well as enhancing the Quad countries' efforts to build influence in Indonesia, this program would allow the technology companies involved to make additional inroads in the large and increasingly lucrative Indonesian market. This is likely to be an appealing long-term proposition given bullish projections that Indonesia will emerge as the fourth-largest economy and a leader in e-commerce by mid-century.

The virtues of strategic competition

As well as further burnishing the tangible regional benefits of Quad cooperation and advancing each Quad country's individual ties with Indonesia, it would be manifestly advantageous for Indonesians. The digital skills gap is one of the biggest hurdles that Indonesia must overcome if it is to translate its lofty digital ambitions into reality.

There is also a strategic advantage. Such a program would provide Indonesians with different avenues to upskill beyond Chinese ICT companies' large-scale and longstanding training offerings. Moreover, rather than unsuccessfully seeking to freeze Chinese ICT companies out of the Indonesian market, such a program would subject these companies to the rigours of serious competition.

But regardless of China's active ICT agenda in the region, serious short-term vocational training in Indonesia is the right thing to do. So, Australia (and the Quad countries) should do it regardless of their goal of counteracting China's influence. Partnering on digital skills and capacity building in Indonesia would be a win-win for all.

It is in Australia's interest that Indonesia further meets its development potential. Providing vocational training is one of the most consequential actions Australia could take to achieve this. Indonesia has been asking for vocational technology training for decades. It is time for Australia and the Quad to deliver.

Endnotes

1. This is outlined in the authors' paper Localization and China's Tech Success in Indonesia published by the Carnegie Endowment for International Peace, https://carnegieendowment.org/2022/07/11/localization-and-china-s-techsuccess-in-indonesia-pub-87477.

2. Huon Curtis, Bart Hogeveen, Jocelinn Kang, Huong Le Thu, Rajeswari Pillai Rajagopalan, and Trisha Ray, Digital Southeast Asia Opportunities for Australia–India cooperation to support the region in the post-Covid-19 context (The Australian Strategic Policy Institute, Canberra: 2022).

3. Herman, "Digital Economy Expected to Become New Growth Engine," *Jakarta Globe*, 7 April 2022, last accessed 5 July 2022, https://jakartaglobe.id/tech/digital-economy-expected-to-become-new-growth-engine.

4. World Bank, "Preparing ICT Skills for Digital Economy: Indonesia within the ASEAN context," World Bank, 8 March 2018, last accessed 9 April 2022, https://blogs.worldbank.org/sites/default/files/preparing_ict_skills_for_digital_economy-revised_7mar2018.pdf.

5. Interview with senior Indonesian government official conducted in February 2022.

6. Greta Nabbs-Keller, Ryan Ko, Tracey Mackay, Nur Achmadi Salmawan, Wibawanto Nugroho Widodo, and Agus Hasan Sulistiono Reksoprodjo, *Cyber security governance in the Indo-Pacific: Policy futures in Australia, Indonesia and the Pacific* (The University of Queensland, Brisbane: 2021), https://policy-futures.centre.uq.edu.au/files/9577/Policy%20Futures_Cyber%20Security%20Indo%20Pacific_May21.pdf.

7. Interviews with senior Indonesian government officials conducted December 2021 to February 2022; *Rencana Kerja Pertahanan Negara Tahun 2013* [National Defence Strategic Plan, 2013] (Ministry of Defence, Jakarta: 2013), p. 12-13

8. Interview with senior Indonesian government officials conducted between December 2021 to February 2022.

9. Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *The Wall Street Journal*, 27 December 2019, last accessed 9 April 2022, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

About the Authors

Dirk van der Kley is a Research Fellow at the ANU National Security College and ANU School of Regulation and Global Governance. He focuses on China's overseas economic policies.

Benjamin Herscovitch is a Research Fellow at the ANU National Security College and ANU School of Regulation and Global Governance. His research focusses on economic statecraft and Australia-China relations.

Gatra Priyandita is an Analyst at the Australian Strategic Policy Institute. He researches extensively on Southeast Asian security, cybersecurity, and Indonesian foreign policy.

About the Editor

Dr William A. Stoltz is the Policy Director at the ANU National Security College. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates.

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

W nsc.anu.edu.au

@NSC_ANU

National Security College