

## ARGUMENT



*An expert's point of view on a current event.*

# Why Indonesia Has Embraced Huawei

If the U.S. wants to compete with China in developing countries, our research shows it needs to offer tangible assistance in response to real needs.

By [Benjamin Herscovitch](#), [Dirk van der Kley](#), and [Gatra Priyandita](#)

JULY 28, 2022, 12:10 PM

China is neither liked nor trusted in Indonesia. Yet Chinese tech firms—particularly Huawei and ZTE—have become trusted cybersecurity partners for the country. They provide the tech and the training for much of the workforce and the government officials charged with Indonesia's cybersecurity. These Chinese tech successes in Indonesia offer sobering lessons for the United States, its allies, and its partners—not just in Indonesia, with a population of more than 270 million, but in the broader Indo-Pacific as well.

Unless policymakers in Washington take some pages from the Huawei and ZTE playbook, these Chinese tech titans will not face any serious competition as they maneuver to train vast swaths of the 21st century's digital workforce. After all, the United States and its allies and partners have for years been in the business of walling themselves off from the perceived security vulnerabilities of dependence on Chinese technology.

Starting in the early 2010s, staunch U.S. allies such as Australia began limiting Huawei's involvement in critical information communications technology infrastructure. This eventually culminated

in strong restrictions—and sometimes outright exclusions—for Huawei and its peers such as ZTE.

But for much of the developing world, the story could not be more different.

With a few notable exceptions including Vietnam and India, the developing world still welcomes Chinese tech companies as providers of sorely needed communications infrastructure and training. Huawei and ZTE have experienced among their warmest embraces in Indonesia. First entering the Indonesian market in the late 1990s and early 2000s, these companies have emerged as integral suppliers both of Indonesia’s essential communications infrastructure and the training that will empower the workforce of the country’s booming digital economy. Huawei, for example, already has by a wide margin the largest share of Indonesia’s telecom carrier equipment market.

As with many other developing countries, the relatively low price point of Huawei and ZTE kits is a big part of the appeal. By some estimates, Chinese communications infrastructure is as much as 30 percent cheaper than its competitors’.

Yet in setting out to document how senior Indonesian government officials approach the risks of technological reliance on Chinese companies for our new report, *Localization and China’s Tech Success in Indonesia*, we found that the reasons for the expansive role of China’s tech companies are more complex and numerous than price point. As our interviews with a wide range of Indonesian officials and experts made plain, Chinese tech companies are seen as partners to both realize Indonesia’s big digital economy goals and navigate its daunting cybersecurity challenges.

Although the digital economy is central to the Indonesian government’s plans for catapulting the country into the top 10 global economies by 2030, the country also faces a massive skills shortage in the field of information communications technology, with the World Bank projecting that it will need 9 million additional such workers by 2030.

Meanwhile, Indonesia is among the countries most vulnerable to cyberattacks globally. According to Indonesia’s National Cyber and Crypto Agency, the country experienced 1.4 billion cyberattacks or web traffic anomalies in 2021. In 2017, when the number of cyberattacks was closer to 200 million, they were estimated to have cost the country \$34.2 billion.

Despite deep suspicion of Chinese tech companies among rich liberal democracies, Huawei and ZTE have presented themselves as the solution to Indonesia’s twin challenges of an impending tech skills shortfall and pervasive cyberattacks.

In 2020, Huawei pledged to train 100,000 Indonesians in essential digital skills, including cloud computing and 5G. Despite the ambitiousness of the move, Huawei is backing its pledges with resources.

We found that Huawei is partnering with local Indonesian universities to offer free short courses and certifications in app development and other key skills. One Indonesian academic we spoke to shared emails showing that Huawei is expanding its outreach by seeking to partner with more local universities and education providers.

Huawei is offering training to the Indonesian government as well, with the company reportedly having trained 7,000 officials since 2019. Indonesia has long been a victim of China's sophisticated cyber-espionage. Despite this, Indonesia sees the training offered by Chinese tech companies as a solution to many of the country's most severe cybersecurity challenges.

For Indonesia, the threat of state-based cyber-espionage is far down the list of security concerns when compared to cybercrime committed by nonstate actors, misinformation, and disinformation. In addition to financial losses for Indonesian companies and identity theft and fraud for ordinary Indonesians, these threats endanger the country's social and political stability.

With Chinese tech companies offering the training, technology, and security practices to reduce vulnerabilities to cybercrime committed by nonstate actors and the skills and technology needed to manage the information domain, the Indonesian government sees firms like Huawei as partners. As a testament to this, the country's National Cyber and Crypto Agency signed a memorandum of understanding with Huawei on cybersecurity capacity building in 2019. This agreement was then upgraded to a three-party agreement with a leading Indonesian technology institute in 2021.

For the United States or Australia, the notion that a cybersecurity agency would sign such an agreement with Huawei might seem absurd—especially considering that the Chinese government can compel Chinese companies to assist with its intelligence efforts.

But for Indonesia, these concerns about state security are trumped by the training and technology benefits that companies like Huawei provide. As one senior Indonesian government official said to us: “If we're constantly afraid, our development will stagnate.”

If the United States and its allies and partners want to compete with China in developing countries such as Indonesia, then, much like Huawei, they

need to get themselves in the business of offering tangible benefits that respond to real needs.

The U.S. government should partner with its leading tech companies to offer free or at least highly subsidized technical training programs in Indonesia and elsewhere in the Indo-Pacific. As well as subjecting the offerings from Chinese companies to some healthy competition, such initiatives would be welcomed by key U.S. allies and partners.

Countries such as Japan, Australia, and India are similarly concerned about the rise of Chinese tech companies across the Indo-Pacific and would strongly support such a U.S. initiative. Moreover, these countries could bolster such a U.S.-led effort by providing additional know-how, funding, and technology. Such a so-called minilateral initiative could also potentially be rolled into existing Quad efforts to provide more public goods in the Indo-Pacific.

Rhetoric from the United States and like-minded countries about the rules-based international order and a free and open Indo-Pacific isn't bad. But it won't persuade developing countries to turn down tangible benefits like technology and training. To shift decision-making in Jakarta and elsewhere, Washington will need to step up with technology and training offers that provide a more appealing value proposition.

None of this is to say that strategic competition with China is the only reason for offering tech training programs in Indonesia and other developing countries in the Indo-Pacific.

Helping to upskill future generations of tech workers in the region is an unambiguously good thing. Many Indo-Pacific countries and their young populations will need these skills to realize their development goals in the global economy's digital future.

But as well as the clear development rationale for providing these kinds of opportunities, there is a compelling realpolitik reason. Without training funded and supported by the United States and its allies and partners, Huawei and other Chinese tech companies will only increase their already strong influence over Indonesia's—and the broader region's—technology landscape.

The United States and its allies and partners have been missing in action on tech training in Indonesia and other key developing economies in the Indo-Pacific. It is time for them to get back in the game.

**Benjamin Herscovitch** is a research fellow at the Australian National University.

**Dirk van der Kley** is a research fellow at the Australian National University.

**Gatra Priyandita** is an analyst at the Australian Strategic Policy Institute.

**TAGS:** CYBER SECURITY & HACKING, INDONESIA, SCIENCE AND TECHNOLOGY