CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

JULY 2022

CHINA local global

Localization and China's Tech Success in Indonesia

Gatra Priyandita, Dirk van der Kley, and Benjamin Herscovitch

Localization and China's Tech Success in Indonesia

Gatra Priyandita, Dirk van der Kley,
and Benjamin Herscovitch

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

China Local/Global

China has become a global power, but there is too little debate about *how* this has happened and what it means. Many argue that China exports its developmental model and imposes it on other countries. But Chinese players also extend their influence by working through local actors and institutions while adapting and assimilating local and traditional forms, norms, and practices.

With a generous multiyear grant from the Ford Foundation, Carnegie has launched an innovative body of research on Chinese engagement strategies in seven regions of the world—Africa, Central Asia, Latin America, the Middle East and North Africa, the Pacific, South Asia, and Southeast Asia. Through a mix of research and strategic convening, this project explores these complex dynamics, including the ways Chinese firms are adapting to local labor laws in Latin America, Chinese banks and funds are exploring traditional Islamic financial and credit products in Southeast Asia and the Middle East, and Chinese actors are helping local workers upgrade their skills in Central Asia. These adaptive Chinese strategies that accommodate and work within local realities are mostly ignored by Western policymakers in particular.

Ultimately, the project aims to significantly broaden understanding and debate about China's role in the world and to generate innovative policy ideas. These could enable local players to better channel Chinese energies to support their societies and economies; provide lessons for Western engagement around the world, especially in developing countries; help China's own policy community learn from the diversity of Chinese experience; and potentially reduce frictions.

Evan A. Feigenbaum
Vice President for Studies, Carnegie Endowment for International Peace

Summary

On average, Indonesians distrust China and many Chinese firms. Yet Huawei and to a lesser extent ZTE have successfully positioned themselves as trusted cybersecurity providers to the Indonesian government and the Indonesian nation. This has been no easy feat given long-held Indonesian animosity toward China. Many Chinese companies have faced protests over concerns they were taking local jobs. Huawei and ZTE have suffered no such fate. Nor has there been a broad coalition of Indonesian voices against using Chinese technology in critical telecommunications infrastructure. In short, Indonesians care a lot more about Chinese cement plants than they do about Huawei involvement in 5G networks.

This is a vastly different conversation to those happening in rich liberal democracies. Huawei and ZTE have been able to achieve success in Indonesia, despite a sense of ambivalence among the Indonesian political and defense establishment about Chinese intentions and growing Western scrutiny over the use of Chinese technology in broadband networks.

As other papers in this series have demonstrated, Huawei and ZTE needed to localize their strategies. Like elsewhere in the world, available evidence suggests that part of Huawei's and ZTE's value proposition is cheaper prices (compared to those of competitors) for high-quality technology.

But that is only part of the story. Huawei has positioned itself as Indonesia's cybersecurity provider of choice by offering enormous cybersecurity and other related training programs across the country for groups ranging from senior government officials to students in rural Indonesia. Much of this training is technically focused on practical vocational skills with a hope that students one day will become customers. In addition, the company offers an attractive maintenance and upkeep package.

Since the mid-2000s, Chinese information and communications technology (ICT) firms have created training centers in partnership with local Indonesian telecoms companies and universities to train the next generation of Indonesian engineers and tech specialists. Government agencies are also increasingly targets of training and capacity-building programs, with Huawei claiming that 7,000 government officials have participated in its training programs. The Indonesian government, corporations, and ordinary citizens alike have welcomed Huawei and ZTE as essential partners in their efforts to build both the infrastructure and human capital necessary to prosper in the twenty-first century's digital economy.

What Huawei and ZTE offer is knowledge transfer, not technology transfer. The technology is still being built in China by Chinese firms. Huawei's role in training relates instead to capacity building. Indonesians will install, maintain, and use the networks. China will build the hardware.

There is also evidence that China has had some rhetorical success in pushing its version of cyberspace governance. Beijing's preferred cyberspace governance language was inserted into a memorandum of understanding between Indonesia's National Cyber and Crypto Agency and the Cybersecurity Administration of China. However, it is difficult to see how the memorandum has influenced Indonesia's cybersecurity governance in practice.

One of the concerns often leveled by rich liberal democracies is that reliance on Chinese tech will end up aligning the political interests of countries like Indonesia with those of China. Other key worries are that China's pervasive espionage and the enduring (though as yet unrealized) risk that Chinese companies with a dominant role in an ICT ecosystem could be used by Beijing to apply coercive political pressure.

Despite Indonesia's embrace of Huawei and ZTE, political leaders in Jakarta have not simply disregarded the hard security questions posed by upgrading ICT equipment, especially when foreign suppliers are involved. Indonesian officials simply rate the need for development and cybersecurity-related capacity building higher than the risk of using Chinese ICT hardware in their critical infrastructure systems.

If rich liberal democracies are concerned about this trend, then they need to offer workable alternatives that place Indonesia's enormous digital development needs at the heart of any value proposition. It is unlikely that Indonesia will stop using Chinese hardware in its infrastructure, but alternatives could prevent overreliance.

Introduction

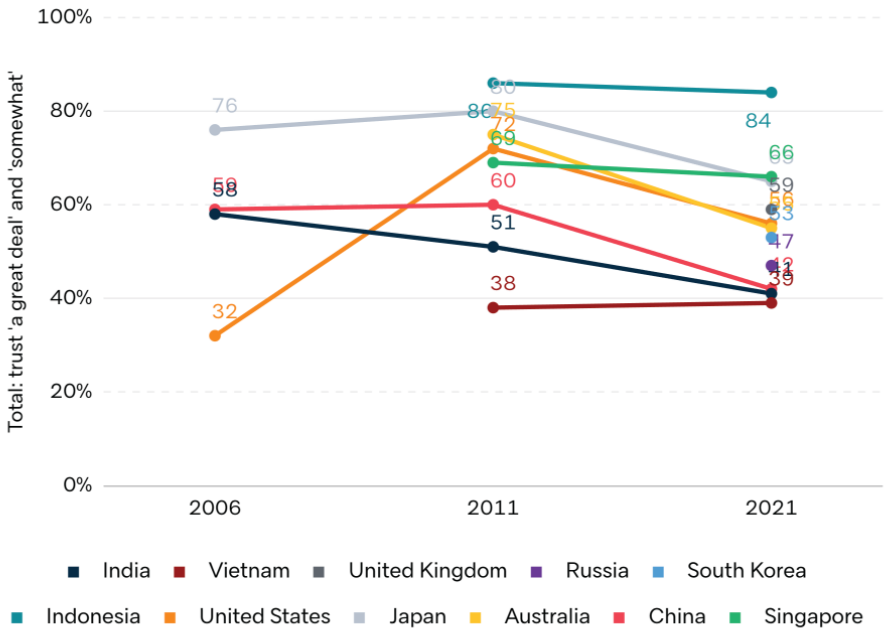
Two seemingly contradictory trends are occurring in Indonesia. On the one hand, trust in China has rapidly fallen (see figure 1).[1] Trust in other major powers has also declined, but China remains far less trusted than the United States or Japan. Sources of distrust range from China's repression of Muslim minorities to its increasingly assertive maritime claims over waters that Jakarta views as part of its exclusive economic zone. There is also public animus toward certain types of Chinese investments and projects in Indonesia. Chinese cement plants, for example, are accused of undercutting their Indonesian competitors and employing Chinese workers at the expense of Indonesians in need of jobs.[2]

Yet, despite this level of distrust, the key Chinese suppliers of telecommunications infrastructure in Indonesia—the Chinese national telecoms champions Huawei and ZTE—have faced no major pushback from the government or ordinary Indonesians. Unlike other types of labor-intensive Chinese projects that have sparked persistent protests in Indonesia for favoring Chinese workers over local Indonesian ones, Huawei and ZTE have generated minimal negative press.[3] The network security or other potential threats from Huawei or other Chinese digital infrastructure suppliers that have dominated debates elsewhere do not rate highly in the long line of policy concerns in Indonesia.

FIGURE 1

Indonesia's Declining Trust in Global Powers

How much do you trust the following countries to act responsibly in the world?



SOURCE: Ben Bland, Evan Laksmana, and Natasha Kassam, "Charting Their Own Course: How Indonesians See the World," Lowy Institute, April 2022, 13, https://interactives.lowyinstitute.org/features/indonesia-poll-2021.

Indeed, because the top policy priorities in Indonesia are job creation and economic development, warnings that Huawei and ZTE pose security threats have not generally resonated. As one senior Indonesian government official told the authors in an interview: "If we're constantly afraid, our development will stagnate."[4] Neither intensifying technology competition between China and the United States nor cases of China-sponsored cyber espionage are likely to change Indonesia's position.

Adaptation to local conditions in Indonesia has been a major reason why China's two largest telecom hardware exporters, Huawei and ZTE, have become integral to Indonesia's development strategy. An attractive price differential between the products they offer and international alternatives is, of course, one part of their appeal.[5] All the Indonesian interviewees the authors spoke with (from a wide range of government departments and agencies and across academia and think tanks) stated that the price advantage of Huawei and ZTE was a big factor in Indonesia's decision to deploy Chinese equipment. But beyond the advantages of a lower price point, Huawei and ZTE have embarked on a huge and rapidly growing capacity-building effort among Indonesians that has helped to address Indonesia's biggest hurdle to a flourishing digital economy: a lack of cybersecurity talent and technology.[6]

Both Chinese companies have offered cybersecurity training to Indonesian officials, tech workers, and students at a level that is unmatched by any other foreign company or government. In 2020, Huawei claimed that it would train 100,000 Indonesians within five years in cybersecurity skills.[7] The authors began this research skeptical of those numbers, but as they dug into the story, they saw a training regime that is unparalleled by any other foreign technology company operating in the country. So intense are Indonesia's demands for knowledge and skills transfers, capacity building, and workforce training that Huawei and ZTE themselves have fought an uphill battle to plug up the cybersecurity capability shortages Indonesia faces. But they have adapted to this local imperative by offering more than their competitors have.

Even if Indonesians fret more about the cybersecurity implications of deep partnerships with Chinese national champion telecom firms amid warnings from the governments of rich democracies, Huawei and ZTE have positioned themselves as the solution to Indonesia's cybersecurity challenges, not the source of the problem.[8] And those challenges *are* immense. There were 1.4 billion cyber attacks in Indonesia in 2021, up from 495 million the previous year, according to Indonesia's National Cyber and Crypto Agency (BSSN).[9] One interviewee showed the authors the ease with which the private personal data of the average Indonesian citizen can be accessed.[10]

Amid this proliferation of cyber threats, Indonesians and their government are most worried not about China but about cyber crime committed by nonstate actors and threats to domestic social and political stability, such as misinformation and disinformation.[11] The possibility of espionage and the

prospect of a foreign government using information and communications technology (ICT) infrastructure for leverage are well understood, but they rank far down the list of Indonesia's cybersecurity concerns. With Huawei's and ZTE's offers to help Indonesian officials better combat nonstate cyber crime and more effectively manage the digital information domain, many in Jakarta view these firms as security partners, not prospective antagonists.

This paper first examines Indonesia's ICT ecosystem and assesses how competing development and security imperatives have created the right conditions for Chinese ICT companies to prosper. Second, it analyzes the history of Huawei and ZTE in Indonesia's telecommunications sector. Third, it examines key dimensions of Chinese local strategies: upskilling and capacity building. Finally, the paper explores Indonesia's vision of its cybersecurity interests and how Huawei and ZTE have found ways to fit themselves and their offerings into that decidedly local vision.

Indonesia's Development Imperative

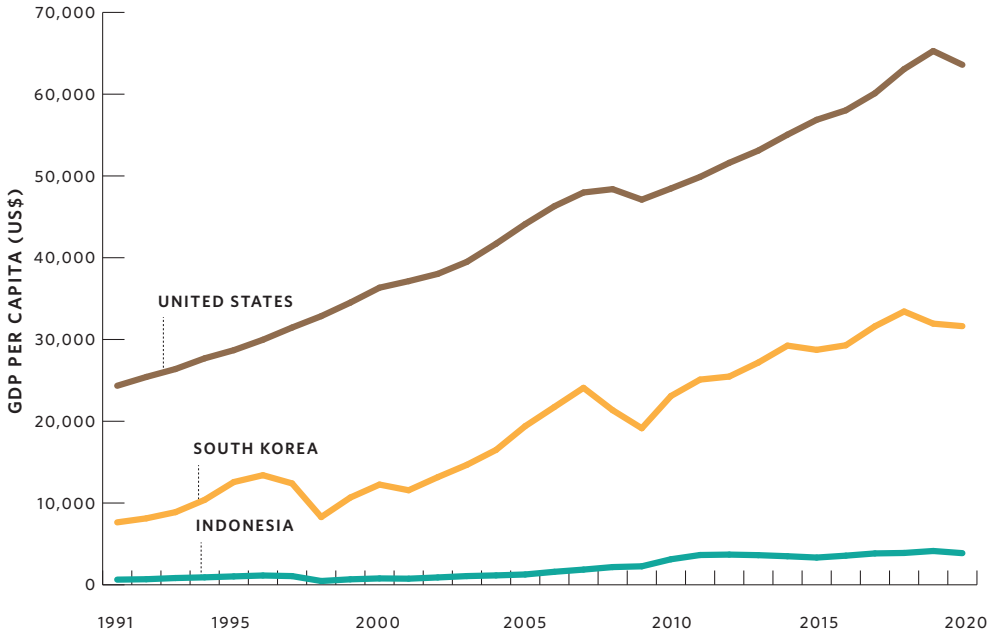
Although Indonesian policymakers have focused on development for decades, the country continues to face multiple socioeconomic challenges. Indonesia has not closed the economic gap between itself and advanced postindustrial economies, a gap that has widened over the last thirty years.

Illustratively, figure 2 demonstrates the growing chasm in gross domestic product (GDP) per capita (in current U.S. dollars) between Indonesia, South Korea, and the United States since 1991. A counterpoint to this argument is that the United States' GDP per capita was around thirty-nine times bigger than Indonesia's in 1990 but was only about sixteen times bigger in 2020.[12] However, from the point of view of many Indonesians, such a statistical metric is unlikely to be comforting. Another way to represent the same data is to look at the persistent gap in GDP per capita between the United States and Indonesia—and there, the size of the gap has risen from $23,710 in 1991 to $59,723 in 2020.

Economists sometimes prefer purchasing power parity (PPP) measurements of GDP to figures in current U.S. dollars. PPP figures account for the lower costs of living and greater corresponding purchasing power in less developed countries. For example, a haircut, a doctor's appointment, and even some food costs less in Indonesia than the same goods and services would cost in the United States. However, all key digital hardware in Indonesia is purchased from abroad, so even using PPP figures does not substantially improve Indonesia's developmental position in telecoms infrastructure (although Indonesia has cheaper labor to install the equipment compared with that in advanced economies). This is just another indicator of Indonesia's remaining development hurdles: labor is cheap because of a lack of high-paying jobs. Even when the GDP measurements of the United

FIGURE 2

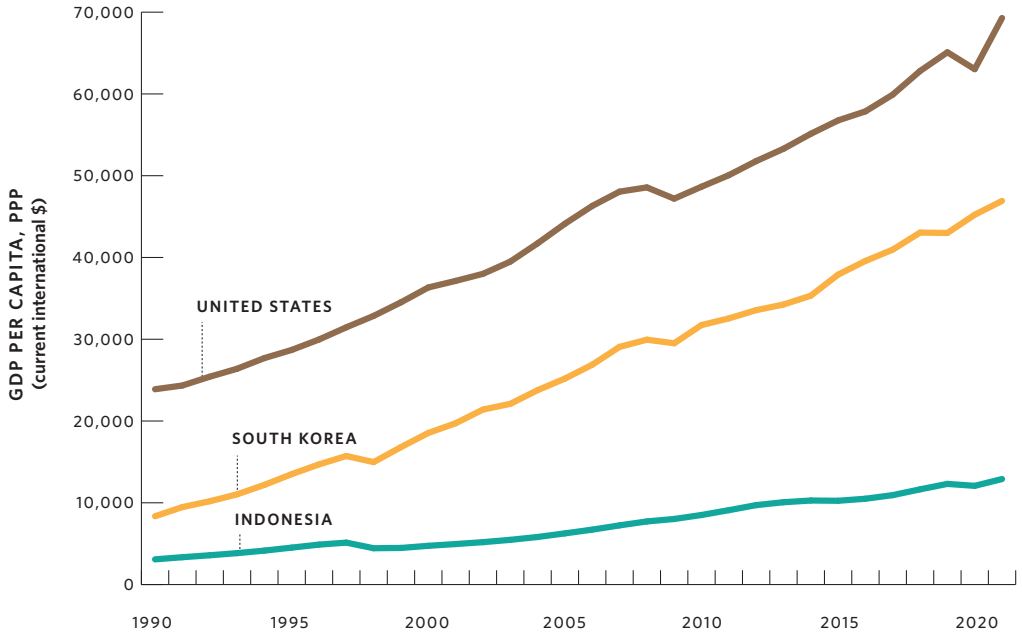
GDP Per Capita of Indonesia, South Korea, and the United States



SOURCE: World Bank, "World Development Indicators," World Bank, 2020, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=US-ID-KR.

FIGURE 3

PPP-Adjusted GDP Per Capita in Indonesia, South Korea, and the United States



SOURCE: World Bank, "World Development Indicators," World Bank, 2020, https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?locations=ID-US-KR

States, South Korea, and Indonesia are adjusted for PPP (see figure 3), it is clear that the gap in GDP per capita in actual terms (not multiples) between the United States and Indonesia is still growing rapidly.

The failure to close these development gaps forms the economic basis for Indonesia's policy decisions in the telecommunications space and other technology-related sectors. At the same time, Indonesia, like many developed and emerging economies, has seen the most wage growth and new jobs in technology-related industries and has had to wrestle with technological disruption in traditional industries. As a 2021 report from the consultancy Bain and Company argues, "It's increasingly clear that technology extends beyond being an industry unto itself; it's the primary force of disruption in every industry across the globe. This phenomenon turns up empirically in the fact that the largest equity gainers across most sectors of the global economy are either technology companies or enterprises with a tech-led strategy."[13] Almost all emerging countries, including Indonesia, are now incorporating technology industries as an essential component of their development path.

For these reasons, Indonesia's drive to spur development has taken an increasingly digital and technology-centric turn. The Indonesian government seeks to create millions of additional jobs in the knowledge economy and use growth in the digital economy to propel Indonesia into the ranks of the top ten biggest global economies by 2030.[14] In 2021, the administration of President Joko Widodo completed its first "Digital Indonesia Roadmap for 2021-2024." The road map is not publicly available, but it reportedly emphasizes investing in the nation's digital and ICT infrastructure, improving human capital, and developing the cybersecurity capabilities needed to support and protect a digitally integrated economy and society.[15] This road map builds on existing initiatives of the past decade, which highlights Indonesia's prioritization of the digital economy with a focus on artificial intelligence, cloud computing, and 5G, as well as the associated applications of these technologies, including for smart cities, e-government, and e-commerce (see table 1).

TABLE 1

Select Recent Indonesian Government Digital Economy Policies

Policy	Year	Areas of Focus
National E-Government Road Map[16]	2016	Infrastructure and e-government
National E-Commerce Road Map[17]	2016	E-commerce, manufacturing, the digital economy, and infrastructure
Making Indonesia 4.0[18]	2018	Automation, manufacturing, and R&D spending
National Strategy on Artificial Intelligence 2020–2045[19]	2020	Healthcare services, bureaucratic reforms, food security, mobility, and smart cities
Digital Indonesia 2021–2024 Road Map[20]	2021	Digital infrastructure, digital administration, the digital economy, and digital community

SOURCES: Various government and media sources.

Despite the rapid growth of Indonesia's digital economy in the past five years, there are still major shortcomings blocking the country's efforts to become a global competitor in this area. First, Indonesia still lacks the talent to support its digital ambitions. A 2018 World Bank report found that Indonesia faced a serious ICT skills shortage and projected that Indonesia's economy requires 9 million additional ICT workers by 2030 to support the county's rapidly growing digital economy.[21]

Second, although Indonesia's digital connectivity has improved steadily over the past decade, the country's ICT infrastructure remains insufficient to connect its 273.5 million geographically dispersed people.[22] There is also the problem of unequal internet access, with connectivity infrastructure being highly concentrated in Java, Indonesia's most populous island. In November 2020, a senior official from the Ministry of Communication and Information Technology said that one major challenge continues to be providing connectivity to approximately 12,500 villages without previous internet access.[23] Many villages across Indonesia must set up their own internet connections without help from the government or corporations.[24]

Indonesian officials and telecom operators recognize that the rapid geographic expansion and increased sophistication of its ICT infrastructure are essential inputs for realizing their aspirations for the digital economy.[25] Although homegrown ICT companies have taken up the challenge to connect Indonesia's hundreds of millions of people, they still require substantial financial resources and technical assistance from foreign firms. However, the Indonesian government faces mounting fiscal challenges because of demographic pressures and extensive infrastructure needs. This poses long-term challenges for Indonesia's hopes of prioritizing the digital economy given the capital-intensive nature of ICT infrastructure projects.

ICT infrastructure requires large investments in international and national fiber optic cables, middle-mile networks, satellite links, shortwave radios, and broadband cables to connect homes and offices with the internet. Indonesia's archipelagic geography—comprising approximately 6,000 inhabited islands—makes ICT infrastructure especially capital intensive.[26] These factors mean Jakarta is both price-sensitive and broadly welcoming of foreign investment in its ICT infrastructure. Moreover, Indonesia lacks the substantial sovereign capability to build and modernize its ICT infrastructure, making the country overwhelmingly reliant on foreign technology companies and expertise for the development of the necessary digital networks.

Indonesian political leaders and policymakers are acutely conscious of the massive developmental gains their country would forgo if they fail to embrace the challenge of rapidly expanding and further developing the country's ICT infrastructure. Indonesia saw an increase of 25 million internet

users between 2018 and the second quarter of 2020, bringing the country closer to a benchmark of 200 million internet users.[27] A 2020 report on Southeast Asia by Google, Temasek, and Bain and Company estimated that the gross merchandise value of Indonesia's e-commerce sector stood at $21 billion.[28] This number had shot up to $32 billion by the end of 2020, with more Indonesians shopping and doing business online because of the coronavirus pandemic.[29] Meanwhile, Indonesia's broader digital economy was worth $44 billion in 2020, and Bain and Company projects that it will grow to $124 billion by 2025.[30] The Indonesian government has estimated that Indonesia's digital economy will be worth around $146 billion by 2025.[31]

In a country where the median age is just twenty-nine years, the rapid spread of the internet and digital technology promise to have transformative effects on Indonesian political, economic, and social life.[32] Indonesians are the world's fourth-most active users of social media.[33] The nation also has a dynamic tech start-up ecosystem, having produced at least eight unicorns.[34] Driven by changing consumer behavior, rapidly growing mobile phone and internet penetration, a booming tech sector, and lucrative opportunities for tax revenue, the Indonesian government sees value in championing such a digital transformation. As president, Widodo has made the transformation of Indonesia's digital infrastructure a national mandate.[35] Sustained growth in the digital economy is central to the Indonesian government's broader development plan for the coming decades. It is therefore unsurprising that both Chinese technology companies and Chinese capital are being lured into the Indonesian market considering its status as potentially one of the largest digital economies globally.[36]

The Role of Huawei and ZTE in Indonesia's Digital Infrastructure

Huawei and ZTE are original equipment manufacturers (OEMs), firms that produce infrastructure and hardware for network operators (also called telcos or carriers). Operators sell services to consumers using infrastructure provided by the OEMs. In Indonesia, the network operators are Indonesian firms.

Providing infrastructure to telcos is not Huawei's and ZTE's only business line in Indonesia. Huawei, in particular, has a wide range of business activities in Indonesia and globally. These activities can be separated into three categories (see table 2). Huawei manufactures and sells personal devices such as phones to consumers. It also provides hardware and software solutions to enterprises and other large organizations, such as universities and local governments. Finally, Huawei's carrier business provides network equipment for Indonesian carriers.

TABLE 2

Business Areas of Huawei and ZTE

Business Areas	Definition	Huawei's and ZTE's Competitors
Consumer business	Production of consumer goods like phones, tablets, and laptops	Apple, Samsung, Tecno, and Oppo
Carrier business	Building and managing network equipment, such as "towers, base stations, cables, and licensing on Long-Term Evolution (LTE) devices"[37]	Ericsson, Nokia, Alcatel-Lucent, and Siemens
Enterprise business	Client-tailored private software involving proprietary information for corporate instant messaging and other functions[38]	Cisco and IBM

SOURCE: Henry Tugendhat, "How Huawei Succeeds in Africa: Training and Knowledge Transfers in Kenya and Nigeria," China-Africa Research Initiative, Working Paper 34, March 2020, 5, https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/5e73acb2efefbe3e97b7c258/1584639155488/WP+34+-+Tugendhat+-+Huawei+Kenya+Nigeria.pdf.

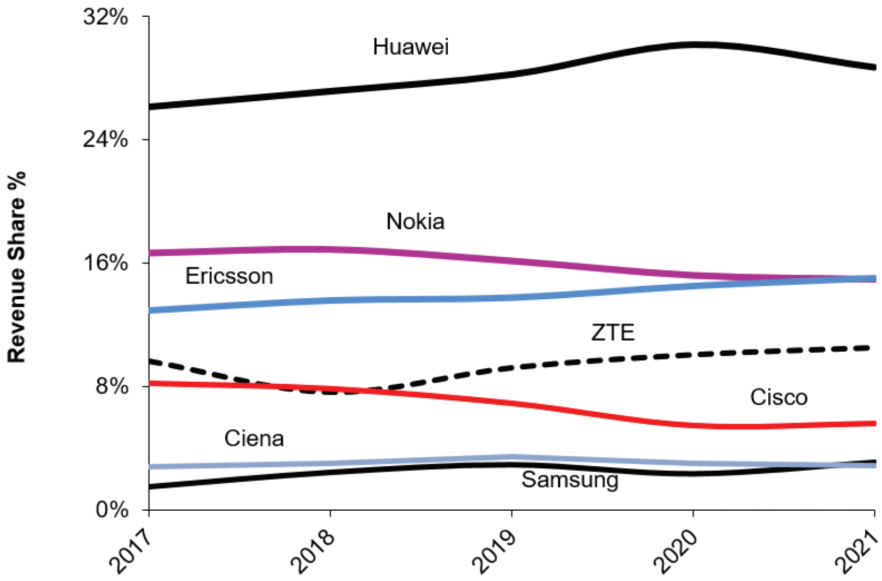
At a global level (including China), Huawei is the market leader by revenue in the carrier equipment business, while ZTE is a middling player (see figure 4). However, China, as the two firms' home market, accounts for about one-quarter of the global carrier equipment market.[39] Outside of China, Huawei's market share is closer to those of Nokia and Ericsson (see figure 5). ZTE is a relatively small player outside of China in this market segment. This paper focuses on Huawei's and ZTE's carrier business in Indonesia, with their enterprise business referenced as necessary given that this business line can involve key government hardware and software too. The firms' consumer businesses are not covered.

It is more difficult to ascertain the market share of Chinese firms in Indonesia's telecom carrier equipment market. But the best available evidence suggests that Huawei is the leader. All interviewees said that Huawei was the largest supplier.[40] A private research report purchased from a firm called 6WResearch stated that Huawei had a 31.7 percent market share, with Nokia placing second at 14.6 percent in 2021.[41] Huawei tends to do much better in emerging economies in general. The authors emailed Huawei in Indonesia a series of questions, including one about Huawei's market share. Huawei did not provide specific details but noted the scale of Indonesia's shortfalls in ICT infrastructure and digital skills and further emphasized Huawei's intent to help Indonesia meet its needs.[42]

Chinese firms were not always the dominant telecom equipment providers in Indonesia. ZTE set up shop in Indonesia in 1999, through the establishment of a Jakarta branch.[43] Meanwhile, Huawei entered the Indonesian market in 2000 through the establishment of a subsidiary.[44] Their entrance into the Indonesian market came at a time of increasingly stiff competition. After decades of strong state control, Indonesia's telecom sector underwent extensive reforms in the early 1990s to attract more foreign capital and expertise to rapidly grow Indonesia's communications infrastructure. By the

FIGURE 4

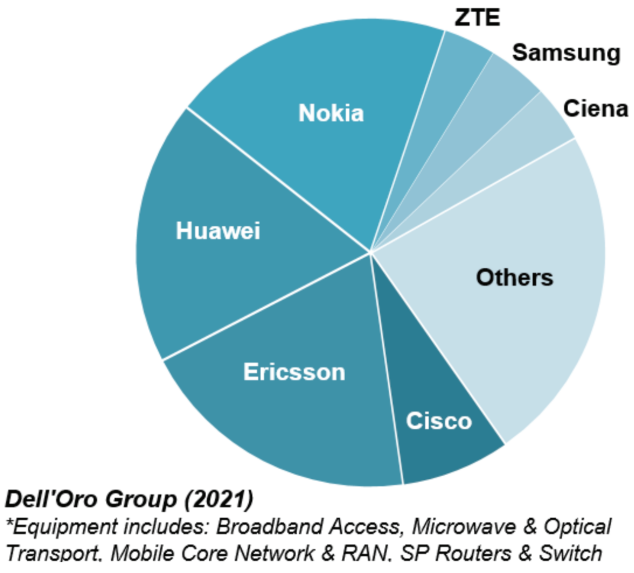
Worldwide Telecom Equipment Revenue by Original Equipment Manufacturers



SOURCE: Stefan Pongratz, "Key Takeaways – 2021 Total Telecom Equipment Market," Dell'Oro Group, March 14, 2022, https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market.

FIGURE 5

Worldwide Telecom Equipment Revenue Outside China by Original Equipment Manufacturers



SOURCE: Stefan Pongratz, "Key Takeaways – 2021 Total Telecom Equipment Market," Dell'Oro Group, March 14, 2022, https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market.

mid-1990s, Indonesia's telecom operators had secured joint ventures with, among others, France Telecom, Telstra Global, NTT Communications, and Singapore Telecom.[45] The sector became even more saturated with domestic and international telecom firms following the 1997–1998 Asian financial crisis, as the sector came under heavy pressure to deregulate as a condition of loans from the International Monetary Fund. Moreover, deregulation also left Indonesia's telecom operators with more autonomy to operate with foreign companies and experiment with more kinds of communication technologies.[46]

Despite a drop in consumer purchasing power, the Asian financial crisis was followed by a period of increasing internet usage and connectivity, as the emergence of a new democratic regime—and the end of the authoritarian New Order regime of former strongman president Suharto—led to a growing appetite among Indonesians for internet access. Although there was only an estimated 700,000 active internet users in 1997, over 4 million Indonesians were online by 2001 and 2002.[47] Seeking to meet increasing demand, Indonesia's major telecommunications operators launched large-scale plans to extend the reach of the country's networks. Huawei, and later ZTE, joined a cohort of foreign ICT companies competing to win a slice of Indonesia's dynamic and expanding telecom equipment business.

In June 2003, Huawei secured its first partnership in Indonesia through a $10 million contract with PT Excelcomindo Pratama (presently XL) to supply it with the GSM equipment needed to expand the operator's network in Sumatra, Kalimantan, and Sulawesi.[48] Meanwhile, ZTE secured its first project in July 2004, when the company was awarded a $47.6 million contract to help Telkom Indonesia build a CDMA network and digital loop carrier network connecting Jakarta and neighboring areas.[49]

These successes were followed by a continuous flow of major Indonesian contracts for Huawei and ZTE, sometimes in conjunction with other foreign ICT firms, to develop Indonesia's mobile network and telecoms infrastructure. From 2009 onward, another Huawei subsidiary, Huawei Marine, was able to win a series of lucrative contracts to help construct undersea cable systems that improved internet penetration and connectivity in northwestern Indonesia.[50] Meanwhile, ZTE became a major equipment supplier to Indonesian telecoms in their construction of 3G and 4G/LTE networks.[51]

By the early 2010s, Huawei and ZTE were offering more services that went beyond the construction of telecommunications networks to include services aimed at fulfilling the Indonesian government's goals of digitizing the economy and government. Through its Smart City Program, Huawei and Indonesian telcos provided digital services, public safety infrastructure, and cybersecurity and technical capacity building to Indonesian municipal governments. ZTE provided these services too. In August 2015, ZTE signed a memorandum of understanding (MoU) with the municipal government

of the city of Makassar to improve its public safety system, including through the deployment of technology for emergency workers to communicate and respond to crises.[52] Huawei also constructed a research center in Jakarta focused on software development.[53]

Huawei's and ZTE's successes, including in Indonesia, are often attributed to their ability to leverage the low costs of their products. Although exact prices are difficult to come by, industry observers and government officials have repeatedly noted that the relatively cheaper costs of Huawei's and ZTE's products at least partly explain their rapid rise as major ICT providers in Indonesia.[54] Initially, those costs savings could have been based on their large pool of Chinese engineers with low wages, which enabled them to outcompete their rivals.[55] However, even now, as Chinese wages have increased substantially and Huawei's research and development (R&D) spending has grown enormously, all the interviewees for this paper stated that Huawei and ZTE were able to offer lower prices than competitors. This is consistent with a 2019 *Wall Street Journal* investigation that corroborated the finding that Huawei has managed to give highly competitive financing options and outprice competitors by around 30 percent.[56] This investigation found that Huawei was able to outbid rivals such as Ericsson and Nokia thanks, in part, to tens of billions of dollars in financial backing from the Chinese government over more than two decades.[57]

Huawei's and ZTE's financial advantages are not just about lower prices. Chinese state-owned banks—both policy banks and commercial banks—pledged to provide at least $600 million worth of financial assistance in export buyer's credits to Indonesian companies in 2005 and 2007, which may have helped Indonesian telecoms purchase Huawei and ZTE products.[58] In August 2010, the Industrial and Commercial Bank of China, China's largest state-owned bank, signed an export buyer's credit agreement with Huawei's Indonesian clients to finance imports of Huawei products.[59] In November 2017, the China Development Fund (the investment fund of the China Development Bank, one of Beijing's two main policy lenders) also provided credit for PT Global Mediacom to purchase ZTE products.[60]

Huawei and ZTE also offer more product extras, despite their lower costs, offerings that can be sorted into two categories. The first is direct add-ons for products—better maintenance and technical support as well as better training for those using the acquired Chinese technology. Gerald F. Rossi, who served as president director of Excelcom when Huawei was awarded its first Indonesian contract, attributed Huawei's success to a "commitment to a high standard of service support *and local training*."[61] In particular, Huawei and ZTE were able to outmaneuver their competitors by providing additional technical assistance (including maintenance) services and investing in training.

The second type of extra feature is a broad-based commitment to developing the technology capacity and human capital of Indonesia. Over time, Huawei and ZTE have become increasingly savvy on

this front. In May 2006, ZTE opened a telecoms training center in partnership with the Telkom Institute of Technology (presently Telkom University).[62] Huawei has built research and training centers to help develop the necessary workforce skills for Huawei's own company needs and Indonesia's ICT human capital as a whole. In April 2011, Huawei established an ICT training center with the School of Technology at the prestigious Bandung Institute of Technology, which trains Indonesian students and researchers about internet protocols.

Indonesian government agencies have also been recipients of training programs designed by Huawei. In January 2016, the Agency for the Assessment of Application of Technology (BPPT), a now-defunct government agency tasked with researching the implementation of new technology, signed an agreement with Huawei for the company to help develop BPPT's capacity to plan the application of artificial intelligence and cloud computing for government purposes and the digital economy. In October 2019, Huawei signed an MoU with the BSSN to help develop the agency's human capital through advanced lessons on cybersecurity. This agreement was renewed in September 2021 (though it is unclear whether this meant anything different in practice).[63] The next section will detail the rapidly increasing size of Huawei's training program in Indonesia.

Huawei's and ZTE's strategies are working. As stated above, Huawei and ZTE are major players in Indonesia's carrier equipment and enterprise equipment business sectors. Moreover, Huawei and ZTE have inked deals with major Indonesian telecom operators to construct the country's 5G mobile network as these companies have met major headwinds in many developed countries.[64] Despite increasingly negative perceptions about China in Indonesia, Huawei and ZTE have not attracted major protests or widespread negative media attention. In fact, their role has been seen as largely positive in many parts of Indonesian society.

Training and Capacity Building

China's role in training and upskilling Indonesians in digital technology has largely been company-driven. The companies have responded to demands from parts of the Indonesian government or Indonesian society, as they recognize the need for a social license to operate. Indonesia has a shortage of information technology (IT) expertise and tech-savvy entrepreneurs. As an Australian government report has noted, "Indonesia has only 278 IT workers per 1 million people, compared to Malaysia (1,834) and India (1,159)."[65] In addition, IT companies have expressed a need for more highly qualified graduates than the Indonesian education system is producing.[66]

Huawei's pledges to provide Indonesians with training on ICT technologies are unrivaled and are a major selling point for the company. These commitments have increased with time, including a pledge in 2020 to train 100,000 Indonesians.[67] Table 3, below, shows examples of formalized

training pledges from Chinese ICT companies up to 2021. Because so many pledges have been made, it can be hard to decipher which pledge is being fulfilled when training occurs. But Huawei trains thousands, and likely tens of thousands, of Indonesians every year. Beyond the examples listed in table 3, Chinese firms also provide smaller, nonformalized training, including on-site job training or small-scale interactions such as the cybersecurity training that Huawei offered to BSSN officials in November 2021.

TABLE 3

Examples of Formalized ICT Training Pledges by Huawei and ZTE in Indonesia

Chinese Firm	Date	Details
Huawei	January 2011	Huawei launches annual "Seeds for the Future" program for Indonesian ICT students, where they receive ICT training, scholarships, and internships.[68] The project continued online in 2021 due to pandemic-related travel restrictions in China.[69]
Huawei	April 2011	Huawei established Training Centre with the School of Technology at Bandung Institute of Technology.[70]
Huawei	March 2017	Huawei launched SmartGen, an ICT training program for students of seven top Indonesian universities.[71]
Huawei	January 2019	Huawei signed an MoU to help develop the BSSN's human capital.[72] The MoU was renewed in 2021.[73]
Huawei	January 2020	Huawei pledged to train 100,000 people in digital technology, such as cloud computing and 5G.[74]
Huawei	January 2021	Huawei opened the Huawei–Association of Southeast Asian Nations (ASEAN) Academy Engineering Institute, collaborating with some of Indonesia's leading universities.[75] The dean of the academy estimates that "1,500 to 2,000 ICT . . . training and certification programs can be completed each year."
ZTE	June 2021	ZTE established an Engineering and Service Training Center.[76] Very few details on proposed student numbers are available.

SOURCES: Various corporate and media sources.

Chinese ICT firms have not always lived up to their training commitments. For example, ZTE established a training center at STT Telkom (a telecoms training institution) in 2006.[77] ZTE initially claimed that it would eventually train 10,000 students annually (a commitment not included in the list above because of its historical nature). Although the center continues to operate, there is no indication that it has ever operated at the scale envisioned. Similarly, in 2018, Jack Ma, the lead founder of the Chinese tech company Alibaba Group, stated that he planned to open a training institute for entrepreneurs in Indonesia (an initiative that is not included in the list above as this announcement did not include a formal signing or opening of a center).[78] The authors could not find much further information beyond the initial announcement, which could indicate the institute never became a reality.

Despite these shortcomings, Huawei and ZTE are expending significant and growing resources to upskill Indonesians. The training is not simply for the companies' own staff either. Huawei, for example, offers training to government employees, university students, and those looking to upskill or change careers, as well as its own employees. In almost any given month, it is possible to find reports of Indonesian civil servants attending a Huawei training course. Huawei claims to have held various "training activities, webinars," and other capacity-building activities to "nearly 7,000 [Indonesian] government officials" since 2019.[79] The quality of these offerings remains unclear. This is just one government program out of the many that Huawei has pledged.

Beyond government training programs, Huawei provides free or subsidized short-term courses for software development and hardware upskilling at local universities and training colleges. Onno W. Purbo, a leading Indonesian IT specialist and academic, showed the authors an email from Huawei offering a free five-week international certification in app development to students of the South Tangerang Institute of Technology (Institut Teknologi Tangerang Selatan). Apple offers its own development courses in Indonesia. Some of these courses, such as the one offered at Binus University, are free.[80] These appear to admit far fewer students than Huawei's offering. Beyond the free programs, Apple also hosts paid programs.[81] Purbo stated that would be a barrier for many of his students.[82] Purbo accepted the Huawei offer because it gave his students a free pathway to better job opportunities. The training course was ongoing as of March 2022. Purbo estimates that over 1,000 students are participating in the course. The email also asked whether he could introduce Huawei to other universities in the country.[83] This indicates that Huawei is actively seeking out training opportunities for Indonesians throughout Indonesia, including in rural parts of the country. None of these initiatives are recorded in high-level announcements, and they tend to fly under the radar.

A majority of the workers that ZTE and Huawei employ in Indonesia are local hires. A 2021 article in the *Jakarta Post* states that local hires make up around 90 percent of Huawei's more than 2,000 workers in Indonesia.[84] Numerous interviewees in government, academia, and the business world agreed that Huawei employs mostly locals.[85] None of them voiced concerns about a lack of local hires. The authors' search of Indonesian media coverage revealed that Chinese laborers working on Chinese projects are a common concern, but rarely has Chinese labor involving Huawei and ZTE been a controversial political issue in the country.

Beyond generic statements about a desire to boost Indonesia's cybersecurity capabilities, Huawei and ZTE do not explicitly state why they fund such wide-ranging training opportunities in the country, to a level well beyond what is necessary for their own projects. Nor do the generic statements explain why the companies' training efforts have increased so significantly in recent years.

The authors, based on interviews with Indonesian officials and cybersecurity specialists, posit three reasons.[86] First, it is necessary for both firms to earn a social contract to operate in Indonesia. They are aware of global wariness toward China and Chinese technology firms. Both firms judge that they need to show that they offer value to communities in host countries.

Second, training locals is a good way to get customers. When the authors asked Purbo why Huawei provided training to his students, his reply was: "Because they want us to buy their equipment."[87] Locals who receive training may go to work for telecom hardware or software purchasers such as banks, universities, and government departments, and if and when they do so, they will have preexisting knowledge and relationships with Huawei. Henry Tugendhat had similar findings for a research paper on Huawei in Kenya and Nigeria. A Huawei spokesperson was quoted in the paper: "We train university students in the hope that they might become future customers, much like Cisco. We currently offer these training programs for free to universities, although the students may still pay a fee to their university as part of their tuition. We intend for these qualifications to be equivalent to an employer backed certification that they might do as an elective or as part of their coursework, for example."[88]

Finally, Huawei and ZTE could potentially tell Chinese political leaders that the training they provide improves other countries' uptake of Chinese technology, which is a key political goal for Beijing. Huawei receives enormous sums of subsidized state funding, and it likely needs to demonstrate that it is delivering political outcomes for leaders in Beijing.

Huawei, and to a far lesser extent ZTE, have done much of the work on training and capacity building in this sector. More recently, the Chinese government has started to test its own upskilling and training programs for people living in emerging economies, including Indonesia. Senior leaders have long talked about global vocational education programs provided by China. For example, in 2011, then premier Wen Jiabao put forth a proposal that China "set up ten vocational education and training centers to help ASEAN countries develop human resources needed in economic and social development."[89] But, until recently, the Chinese government offered few programs for overseas vocational training.

Globally, China is in the early stages of establishing vocational colleges called Luban Workshops in dozens of countries to train students in subjects such as ICT.[90] These vocational training programs had their origins in a local government proposal. The first one was formed in Thailand in 2016 by the municipal government of Tianjin (Lu Ban's hometown). So far, it has reportedly trained over 1,000 Thai students and more than 8,000 pupils from elsewhere in Southeast Asia, likely including Indonesia.[91]

Luban Workshops are generally hosted by local institutions in the participating countries, often in vocational colleges. In May 2021, a newspaper in China reported that eighteen Luban Workshops had been established around the world.[92] Members of China's senior leadership promised in September at least ten would be built in member states of the Shanghai Cooperation Organization, with some potential overlap with prior plans. The Tianjin Dongli District Vocational Education School established Indonesia's first Luban workshop in December 2017.[93] At this workshop, students have learned ICT (and other) skills. It is possible that more Luban Workshops will be established in Indonesia.

The Chinese government also made other earlier attempts to upgrade workers' skills and transfer technology to Indonesia. Many of these initiatives were also pioneered at the provincial level. The results of this outreach have been modest at best. The Guangxi Zhuang Autonomous Region has tried to position itself as the main center for ASEAN-China technology and training exchanges. The functionality of this program remains unclear.

China and Indonesia also established a technology transfer center in Guangxi, the fifth such site between China and an ASEAN country.[94] These technology transfer centers were established under the auspices of the broader China-ASEAN Technology Transfer Center.[95] It appears that these centers have amounted to little in reality. The website has featured little new information since 2015. The China-ASEAN Cybersecurity Exchange and Training Centre was established in Nanning, Guangxi, in 2019.[96] This remains at a very early stage of development. And while other countries are investing in technical vocational education in Indonesia, no other country has come close to matching Huawei's pledge to train 100,000 students in the ICT sector.[97]

A Different Vision of Security

Indonesians have serious concerns about China, but these misgivings are not at the top of the long list of potential challenges for the country. The Lowy Institute's 2021 Indonesia Poll asked Indonesians to rank various threats (see figure 6).[98] The possible answers that directly mentioned China were seen as the least threatening. This is a relative list, and plenty of respondents were concerned about threats involving China such as a U.S.-China war, a dispute in the South China Sea, and the rise of China. But they were seen as less of a threat than terrorism, domestic instability, and food shortages, among many other issues. The issue of foreign workers (which also involves China) was seen as a bigger threat than U.S.-China conflict and the South China Sea.

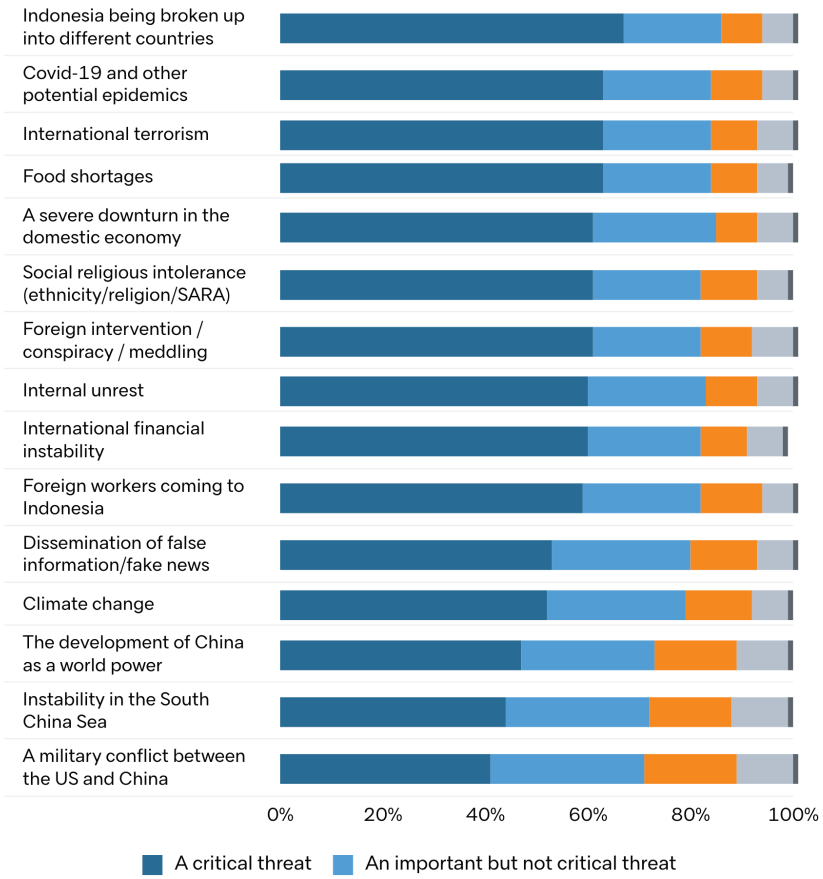
These views flow into how Indonesia treats its cybersecurity engagement with China. Indonesia's digital development is primarily about jobs and economic growth. The biggest cybersecurity risk

from Indonesia's perspective is that its online environment is not competitive enough to create sufficient jobs or that the cybersecurity environment is too insecure for average Indonesians to trust it. There remains a recognition of China's malign cyber activities, but the associated risks do not rate highly compared to a range of other much more pressing security challenges.[99]

The 2008 Indonesian Defense White Paper first recognized the country's cybersecurity vulnerabilities as its susceptibility to cyber crimes grew alongside the size of its internet and mobile phone user base.[100] Another threat identified was cybersecurity and (more generally) technological dependence on foreign states. The 2008 Defense White Paper argued that cyber and technological dependence may not only "cause Indonesia to become a market for foreign products" but also could "make it difficult for Indonesia to manage potential technological threats perpetrated by certain actors to weaken Indonesia."[101] Despite this recognition of the risks of cyber vulnerabilities and technological

FIGURE 6

Poll Results on Threats to Indonesia's Vital Interests



SOURCE: Ben Bland, Evan Laksmana, and Natasha Kassam, "Indonesia Poll 2021: Charting Their Own Course: How Indonesians See the World," Lowy Institute, April 2022, 13, https://interactives.lowyinstitute.org/features/indonesia-poll-2021.

dependence on foreign states, Jakarta has long judged that additional international partnerships and associated foreign investments will be essential for Indonesia's development in critical, high-priority fields such as artificial intelligence, cloud computing, and 5G.[102] Such overseas inputs will be significant assets for Indonesia as it seeks to reap the economic and developmental benefits associated with the application of these fast-evolving technologies in fields such as the Internet of Things and e-commerce.[103] As previously mentioned, Indonesia sees Huawei and ZTE as two of its most critical partners in its digital economy and development endeavors.

However, financial and developmental considerations only partially explain Indonesia's approach to the security risks associated with using Chinese ICT companies. The oft-cited security risks attributed to Chinese ICT infrastructure include perceptions that its use could heighten the dangers of: intellectual property theft, large-scale data mining and surveillance, the potential withholding of system maintenance and upkeep as a source of political leverage, and possible access to and control over critical infrastructure (including public health and energy infrastructure and other essential utilities).[104] But there are few publicly known, tangible instances of such security risks stemming from the use of Chinese ICT infrastructure specifically (though many examples have arisen of Chinese-led cyber attacks using other countries' ICT infrastructure). One of the few widely known public cases is the example of the exfiltration of data from the African Union headquarters, which was seemingly facilitated by the organization's use of Huawei software and hardware.[105] Another is a recently revealed episode from 2012 involving Australia in which Chinese intelligence apparently infiltrated the ranks of Huawei technicians to compromise a software update from Huawei.[106] Despite few confirmed instances of such potential risks, the aforementioned security concerns are nevertheless regularly raised in relation to Chinese ICT infrastructure.[107]

Of course, Chinese state-backed cybersecurity threats, including intellectual property theft and large-scale data mining and surveillance, are pervasive globally. A large coalition of wealthy liberal democracies increasingly have been attributing these widespread and persistent cyber threats to the Chinese state in a coordinated fashion. Notable recent attributions include the July 2021 attribution of "malicious cyber activity and irresponsible state behavior" to China and its Ministry of State Security by Australia, Canada, the European Union, Japan, New Zealand, the United Kingdom, and the United States.[108] Indonesia and other developing states have also probably been subjected to persistent and broad-based Chinese state-backed cyber activities.[109] But these episodes have not been attributed for a range of diplomatic and political reasons. Most recently, a Chinese state-sponsored cyber group allegedly hacked servers belonging to Indonesian intelligence.[110] Despite the real and present cybersecurity threats posed by Chinese state-backed or -affiliated actors, it remains unclear whether the use of Chinese ICT equipment makes this threat significantly more acute.[111]

Jakarta also judges that espionage risks would still exist if Indonesia were to rely on ICT infrastructure built by Japanese, South Korean, and European companies. From the perspective of the United States and its allies, concerns about state-based cyber-enabled espionage and security threats primarily center on concerns about China and Russia, and to a lesser extent Iran and North Korea.[112] However, Indonesia also has espionage concerns about the United States and its allies and partners.[113] Revelations in leaks by former U.S. national security contractor Edward Snowden of industrial-scale U.S. and Australian espionage against Indonesians and their political leaders have understandably led Jakarta to see Washington and Canberra as prime sources of espionage and associated security threats.[114] For example, evidence emerged in November 2013 that Australia had hacked the phones of key members of the Indonesian political elite, including then president Susilo Bambang Yudhoyono.

The apparent complicity of leading U.S. ICT companies, including Google and Microsoft, in mass U.S. and allied surveillance understandably has engendered cynicism in Indonesia regarding claims of an elevated espionage and security risk associated with Chinese ICT companies.[115] Meanwhile, in contrast to speculative claims that China might use intelligence collected via Chinese ICT equipment to undermine Indonesia's economic or infrastructure security, Australia and the United States have probably previously sought to use their intelligence collection to economically disadvantage both Indonesia and neighboring Timor-Leste.[116] Just as Chinese ICT infrastructure might leave Indonesia vulnerable to state-based cyber-based espionage and security threats, Japanese, South Korean, and European ICT infrastructure is not a barrier to sustained and severe espionage and associated security threats from the United States and its allies and partners. Combined with Indonesian leaders' high prioritization of economic development and the cheap acquisition of ICT infrastructure, Indonesia's risk assessment of the impact of ICT vendors on cybersecurity threats is shaped by the perception that all vendors, Chinese or not, entail risks for Indonesia that are hard to mitigate.

Indonesia's digital domain is giving rise to new and evolving concerns. Low cybersecurity awareness among citizens has contributed to a lack of use of virus protection software. According to some sources, Indonesia experienced some 423 million cyber attacks in 2020 alone.[117] Meanwhile, the BSSN's Honeynet cybersecurity system recorded 246 million cyber attacks and more than 190,000 malware attacks in 2020.[118] Indonesia is also regularly cited as being among the world's biggest victims of cyber attacks, accounting for nearly four-tenths of "global hacking-related traffic" in 2013.[119] These cyber attacks cause significant economic damage. According to the BSSN, there were 290 million cyber attacks in Indonesia in 2019, causing $34.2 billion in losses.[120] A 2013 report by Indonesia's Ministry of Communication and Information Technology indicated that the nation had been the top global target for cyber attacks.[121] The expansion of cyberspace has also led to a deluge of misinformation and disinformation, with conspiracy theories and deepfakes eroding religious tolerance and democracy.[122]

Many of the effects of these attacks in Indonesia so far have been economic. In one sense, then, state-sponsored misinformation or state-sponsored distributed denial of service attacks are less of a concern than traditional cyber crime is. But the links between government-sponsored cyber attacks and cyber crime have blurred. The governments of China, Russia, Iran, and North Korea are also involved in economic espionage (not just political-military espionage) and ransomware attacks for economic purposes.[123] For example, the WannaCry ransomware attack, which is believed to have been developed by the North Korean government, disrupted essential services in Indonesia and led to the creation of the BSSN in 2017.[124] The Ministry of State Security in China as well as equivalent organizations in Russia and Iran engage private groups to work for them.[125] Their staff also sometimes work for private cyber groups while still being employed in state security.[126] This leaves open the possibility of privileged state information being used for economic cyber crime. There is evidence that at least one group contracted by the Ministry of State Security has been hiring linguists fluent in Southeast Asian languages too.[127]

Given the pervasiveness of economic cyber crime, even if a fraction of that activity is due to state-linked actors in China, Indonesia is looking for any partner to help boost the country's cybersecurity capabilities. Notably, the Chinese government and Chinese firms have adjusted their ICT infrastructure and broader technological cooperation offerings to Indonesia to help address these nonstate threats.[128] Given the training and capacity-building opportunities from Huawei and ZTE detailed above, Jakarta judges that collaborating with Chinese ICT infrastructure companies will assist its efforts to tackle the severe primary challenges posed by cyber crime and threats to social cohesion.[129]

The Chinese government seeks to promote its version of cyber norms and standards beyond its borders, including in Southeast Asia. Indonesia, being the largest country in the region, is a major target. Beijing promotes cyber sovereignty, which is a version of cyberspace in which the government takes a more interventionist role in the control of information, data storage, and market access.[130] Wealthy liberal democracies have also become more interventionist in terms of internet policy, albeit at a much lower level than China.

To promote this vision, China has established a slew of cybersecurity dialogues with ASEAN.[131] A handful of Indonesian government bodies have also signed or announced cyber agreements or MoUs with the Chinese government or Chinese firms. At least one has a clear reference to cyberspace governance. For example, an MoU between the BSSN and the Cyberspace Administration of China, signed in January 2021, states that "both sides uphold the principle of state sovereignty for cyberspace."[132] The MoU also states that both sides will promote "the information sharing of regulatory system regarding cyberspace governance which may include exchanges in laws and legislation, regulations and management policies concerning cyberspace." This document contains Beijing's

preferred language of state sovereignty over the internet and plans to share information about laws. At this stage, there is no indication that the MoU has any effect on cyberspace governance in Indonesia. Because the authors do not have access to the text of other MoUs and agreements, additional details can be hard to glean. Huawei and the BSSN did sign an MoU on cybersecurity capacity building in 2019, which was upgraded to a three-party agreement with the Del Institute of Technology (Institut Teknologi Del) in October 2021.[133] The focus is on cybersecurity capacity building, but one could envisage that it also covers legal and legislative capabilities as with the aforementioned agreement with the Cyberspace Administration of China.

Indonesian governance of cyberspace falls somewhere in the middle of the spectrum between the practices of China and those of the United States. Indonesia has a series of loosely worded laws that allow people to be charged with a host of crimes including defamation, "religious blasphemy, committing treason, or inciting public disorder."[134] These laws impact online content. For example, individuals have been jailed for posting online in favor of the independence of West Papua, a part of eastern Indonesia that is home to a long-standing independence movement. In the past, the internet and social media platforms have at times been shut down or slowed down, in response to unrest in West Papua.[135]

There are also pieces of new cyber-related legislation under discussion or that have already become policy in Indonesia that further reduce freedoms for internet users. One such proposal called Ministerial Regulation 5, which was issued by the minister for communication and informatics and became policy in 2020, requires any platform that deals with data from users in Indonesia to, according to one interpretation, "ensure that their platforms do not help spread prohibited documents and information—characterized as content which 'violates Indonesian law,' 'promotes social anxiety and disrupts public order,' or 'informs methods or provides access towards prohibited electronic information and/or documents.'"[136] The Ministry of Communication and Informatics has the authority to require that specific online content be taken down and to impose penalties if such orders are not followed within twenty-four hours. (The minister and ministry have undergone several name changes in the last few years and so are not always referred to by the titles this paper has used.) Ordinary people can also submit content that they believe violates these laws for ministry officials to consider.

The logic behind the law is to force content companies to be responsible for the information disseminated on their platforms. Yet, given the Indonesian laws, platform owners may end up self-censoring on content discussing, for example, West Papuan independence, which could be interpreted as contravening Indonesian law. But despite similarities between elements of Indonesia's and China's approaches to the governance of cyberspace, the authors have not found evidence suggesting that

these parallels are a result of Beijing's influence. Rather, Jakarta's approach appears to be driven by the Indonesian government's domestic political and social priorities. Although Indonesia will happily align aspects of its cyberspace governance language with that of China in joint MoUs, this reflects an overlap of preexisting views rather than the product of Beijing's efforts to spread its preferred language.

Lessons Learned

Indonesia will not be persuaded to reduce its dependence on Chinese ICT companies in absolute terms, much less end it entirely. This is likely true for other countries in similar developmental situations (with the exception of a handful of cases like India and Vietnam).[137] Commonly recited concerns about the security risks associated with Huawei or ZTE technology will not change Jakarta's risk calculus. Indonesia will first and foremost make ICT equipment acquisition and investment decisions based on development considerations. Governments seeking to reduce or moderate the role of Chinese ICT companies in the colossal Indonesian market should therefore make tangible offers of training and capacity building rather than talking up security threats or proselytizing about cybersecurity norms.

A more pragmatic approach to engaging with Indonesia on cybersecurity and ICT infrastructure issues would benefit all. It would provide Indonesia with additional options for its gargantuan mission of building its ICT infrastructure and digital skills base, both of which are necessary for the country to realize its digital aspirations and broader developmental ambitions. Such efforts would also provide the United States and its allies and partners with additional avenues to build goodwill in Indonesia, while also ensuring that Chinese ICT companies face a healthy degree of competition in the Indonesian market.

A low price point for ICT network equipment will always be imperative, and Indonesia will seek other added benefits from would-be providers, such as training and capacity building. Governments seeking to slow the global spread of Chinese ICT companies in one of the world's largest and most dynamic digital economies should therefore study the examples of Huawei and ZTE. The U.S. government should consider how it could collaborate with U.S. educational institutions and ICT companies (or those of its allies and partners) to provide Indonesia with an appealing value proposition, including competitively priced ICT infrastructure and relevant training and capacity building.

Although Chinese ICT companies are helping Indonesia make progress toward its goals for a digital economy and greater economic development, the offerings from Huawei and ZTE do not exhaust Indonesia's massive ICT infrastructure needs and digital skills shortfalls. To supplement the offerings from the largest Chinese ICT companies, Indonesia would welcome additional offers of training and ICT infrastructure from the United States and its allies and partners.

About the Authors

Gatra Priyandita is an analyst at the International Cyber Policy Centre at the Australian Strategic Policy Institute, where he leads a project researching cyber-enabled intellectual property theft. He is a political scientist by training and specializes in the study of foreign policy and security in Southeast Asia. He holds a PhD in political science from the Australian National University.

Dirk van der Kley is a research fellow jointly appointed to the National Security College and the School of Regulation and Global Governance at the Australian National University. He specializes in the theory of geoeconomics, international economic sanctions, the Chinese government's international economic policy, and the effects of industrial policy on geopolitics.

Benjamin Herscovitch is a research fellow jointly appointed to the National Security College and the School of Regulation and Global Governance at the Australian National University. His primary areas of research are Australia-China relations, China's economic statecraft, and Australian foreign and defense policy.

Notes

1 Ben Bland, Evan Laksmana, and Natasha Kassam, "Indonesia Poll 2021: Charting Their Own Course: How Indonesians See the World," Lowy Institute, April 2022, 13, https://interactives.lowyinstitute.org/features/indonesia-poll-2021.

2 Muhammad Zulfikar Rakhmat and Yeta Purnama, "The China Factor in Indonesia's New Capital City Plan," *Diplomat*, February 11, 2022, https://thediplomat.com/2022/02/the-china-factor-in-indonesias-new-capital-city-plan.

3 The authors asked every interviewee whether Huawei or ZTE had poor reputations. Every interviewee replied that neither company has a negative image. Certainly, individuals are critical of reliance on Chinese technology. But there are very few examples, if any, of popular protests against Huawei or ZTE and very few examples of it being an election issue. Protests of other types of investments from Chinese companies are common. For example, see Amy Chew, "Indonesian Students in Sulawesi Continue Protests Against Chinese Workers," *South China Morning Post*, July 16, 2020, https://www.scmp.com/week-asia/politics/article/3093345/indonesian-students-sulawesi-continue-protests-against-chinese.

4 Authors' interview with a senior Indonesian government official conducted in February 2022.

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

6 This point was made by most interviewees, regardless of how they viewed Huawei's and ZTE's involvement in Indonesia's digital infrastructure. Authors' interviews with a range of senior Indonesian officials, academics, and industry sources, December 2021 to March 2022.

7 Yohana Arthur Uly, "Garap Pasar 5G Indonesia, Ini Strategi Huawei," [Working on the Indonesian 5G Market, This is Huawei's Strategy], *Kompas*, January 15, 2021, https://money.kompas.com/read/2021/01/15/121300626/garap-pasar-5g-indonesia-ini-strategi-huawei?page=all.

8 For example, Huawei's 2021 annual report states, "In Indonesia, we renewed the Memorandum of Understanding (MoU) on cyber security cooperation with the National Cyber and Crypto Agency (BSSN), reaffirming our commitment to the sharing of cyber security knowledge, and supporting Indonesia's plan to develop cyber security and digital transformation professionals." See Huawei Investment and Holding Company, "Huawei Annual Report," Huawei Investment and Holding Company, 85, https://web.archive.org/web/20220403102653/https://www-file.huawei.com/minisite/media/annual_report/annual_report_2021_en.pdf.

9 Kiki Siregar, "Spate of Cyberattacks in Indonesia Shines Spotlight on Complacency, Public Education," *Channel News Asia*, December 18, 2021, https://www.channelnewsasia.com/asia/indonesia-cyberattacks-complacency-education-bssn-bnpb-2386586.

10 Authors' interview with a cybersecurity specialist in February 2022.

11 Authors' interviews with Indonesian government officials, December 2021 to March 2022.

12 This is calculated from World Bank data. According to the data, in 2020 the United States had a GDP per capita (in current U.S. dollars) of $63,593, and Indonesia had a GDP per capita of $3,870. In 1991, the United States had a GDP per capita of $24,342 and Indonesia had a GDP per capita of $632. See World Bank, "World Development Indicators," World Bank, 2020, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=US-ID-KR.

13 Bain and Company, "Technology Report 2021: The '20s Roar," Bain and Company, 2021, 3, https://www.bain.com/globalassets/noindex/2021/bain_report_technology-report-2021.pdf.

14 Sanya DS, Fardah, "Digital Technology Has Potential to Create 20-45 Million New Jobs," *Antara News*, February 21, 2022, https://web.archive.org/web/20220317093045/https://en.antaranews.com/news/216457/digital-technology-has-potential-to-create-20-45-million-new-jobs; and Indonesian

Investment Coordinating Board, "Making Indonesia 4.0: Indonesia's Strategy to Enter the 4th Generation of Industry Revolution," Indonesian Investment Coordinating Board, April 27, 2018, https://web.archive.org/web/20220217114250/https://www9.investindonesia.go.id/en/why-invest/indonesia-economic-update/making-indonesia-4.0-indonesias-strategy-to-enter-the-4th-generation-of-ind.

15 The International Trade Administration, "Indonesia: Digital Economy Opportunities," U.S. Department of Commerce, December 9, 2021, https://www.trade.gov/market-intelligence/indonesia-digital-economy-opportunities.

16 Indonesian Ministry of Communication and Informatics, "National E-Government Road Map 2016-2019," Indonesian Ministry of Communication and Informatics, January 21, 2016, https://web.archive.org/web/20220622152138/https://kominfo.go.id/content/detail/6620/siaran-pers-nollpihkominfol2016-tentang-pemerintah-selesaikan-petajalan-iegovernmenti-2016-2019-yang-bernuansa-nawacita-dengan-menyerapinisiatif-dari-semua-kementerian-dan-lembaga-terkait/0/siaran_pers.

17 Medha Basu, "Indonesia Reveals Digital Economy Targets," GovInsider, April 21, 2017, https://govinsider.asia/innovation/indonesia-reveals-digital-economy-targets.

18 Indonesian Investment Coordinating Board, "Making Indonesia 4.0."

19 Anthony Iswara, "Indonesia Sets Sights on Artificial Intelligence in New National Strategy," *Jakarta Post*, August 14, 2020, https://www.thejakartapost.com/news/2020/08/13/indonesia-sets-sights-on-artificial-intelligence-in-new-national-strategy.html.

20 Arindra Meodia, "Ministry Drafts Roadmap for Indonesia Digital 2021-2024," *Antara News*, February 1, 2021, https://en.antaranews.com/news/167151/ministry-drafts-roadmap-for-indonesia-digital-2021-2024; and Lifia Putri and Fadhli Ruhman, "Minister Outlines Priorities Within Digital Indonesia Road Map," *Antara News*, March 23, 2022, https://en.antaranews.com/news/221329/minister-outlines-priorities-within-digital-indonesia-road-map.

21 World Bank, "Preparing ICT Skills for Digital Economy: Indonesia Within the ASEAN Context," World Bank, March 8, 2018, https://blogs.worldbank.org/sites/default/files/preparing_ict_skills_for_digital_economy-revised_7mar2018.pdf.

22 World Bank, "Population, Total – Indonesia," World Bank, 2020, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=ID.

23 Eisya A. Eloksari, "Indonesian Internet Users Hit 196 Million, Still Concentrated in Java: APKII Survey," *Jakarta Post, November 11, 2020,* https://www.thejakartapost.com/news/2020/11/11/indonesian-internet-users-hit-196-million-still-concentrated-in-java-apjii-survey.html.

24 Darlena Cunha, "The Common Room: How an Artist Is Connecting Rural Indonesia One Village at a Time," Internet Society, April 28, 2021, https://www.internetsociety.org/blog/2021/04/the-common-room-how-an-artist-is-connecting-rural-indonesia-one-village-at-a-time; and authors' interview with Indonesian cybersecurity specialist, January 2022.

25 Authors' interviews with a range of senior Indonesian officials, academics, and industry sources, December 2021 to March 2022.

26 Onno W. Purbo, "Narrowing the Digital Divide," in *Digital Indonesia: Connectivity and Divergence, edited by Edwin Jurriens and Ross Tapsell (Singapore: ISEAS, 2017): 75–92; and Indonesian Embassy in the United States, "Facts and Figures," Indonesian Embassy in the United States,* https://web.archive.org/web/20220619160848/https://www.embassyofindonesia.org/basic-facts/.

27 Eloksari, "Indonesian Internet Users Hit 196 Million, Still Concentrated in Java."

28 Aadarsh Baijal, Alessandro Cannarsi, and Florian Hoppe, "e-Conomy SEA 2020," Google, Temasek, and Bain and Company, November 10, 2020, 96, https://www.bain.com/insights/e-conomy-sea-2020.

29 Ibid.

30 Ibid., 32.
31 "Indonesia's Digital Economy to Reach $146 Billion in 2025: President," *Antara News, December 15, 2021,* https://en.antaranews.com/news/204589/indonesias-digital-economy-to-reach-146-billion-in-2025-president.
32 United Nations Department of Economic and Social Affairs, Population Division, "Indonesia," in *World Population Prospects 2019, Volume II: Demographic Profiles*, 2019, https://population.un.org/wpp/Graphs/1_Demographic%20Profiles/Indonesia.pdf.
33 Statista, "Number of Social Network Users in Selected Countries in 2021 and 2026," July 2021, https://www.statista.com/statistics/278341/number-of-social-network-users-in-selected-countries/#:~:text=China%20is%20the%20biggest%20social,million%20current%20social%20media%20users.
34 Petir Garda Bhwana, "SOEs Minister Says Expect Number of Unicorns to Increase," *Tempo*, January 16, 2022, https://en.tempo.co/read/1550480/soes-minister-says-expect-number-of-unicorns-to-increase.
35 Joko Widodo, "Remarks of President of the Republic of Indonesia in Virtual ASEAN Business and Investment Summit," Presidential Palace, October 25, 2021, https://web.archive.org/web/20220622152732/https://setkab.go.id/en/remarks-of-president-of-the-republic-of-indonesia-in-virtual-asean-business-and-investment-summit-25-october-2021-at-bogor-presidential-palace-west-java-province/.
36 Kayla Goode and Heeu Millie Kim, "Indonesia's AI Promise in Perspective," Georgetown University Center for Security and Emerging Technology, 2021, 20, https://doi.org/10.51593/2021CA001.
37 Henry Tugendhat, "How Huawei Succeeds in Africa: Training and Knowledge Transfers in Kenya and Nigeria," Johns Hopkins University School of Advanced International Studies, China Africa Research Initiative, Working Paper No. 2020/34, https://www.econstor.eu/bitstream/10419/248162/1/sais-cari-wp34.pdf.
38 Ibid.
39 Stefan Pongratz, "Key Takeaways – 2021 Total Telecom Equipment Market," Dell'Oro Group, March 14, 2022, https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market.
40 Authors' interviews with a range of senior Indonesian officials, academics, and industry sources, December 2021 to March 2022.
41 A private research report purchased by the authors from 6WResearch.
42 Authors' email correspondence with Huawei personnel, July 2022.
43 Uday Rayana, "Sejarah ZTE di Indonesia, Kerjasama dengan Smartfren Menjadi Titik Balik Pertumbuhan," [History of ZTE in Indonesia, Cooperation With Smartfren Turning Point for Growth]," *Selular*, April 20, 2022, https://selular.id/2022/04/sejarah-zte-di-indonesia-kerjasama-dengan-smartfren-menjadi-titik-balik-pertumbuhan.
44 Chinese Ministry of Foreign Affairs, "Ambassador Xiao Qian Visits Huawei Indonesia," May 28, 2018, https://web.archive.org/web/20220622151112/https://www.fmprc.gov.cn/ce/ceindo/eng/sgdt/t1562928.htm.
45 Koesmarihati Sugondo and Risa Bhinekawati, "Indonesia: Telecommunications on a Road to Reforms," in *Telecommunications Reform in the Asia-Pacific Region, edited by Allan Brown, Moazzem Hossain, and Duc-Tho Nguyen (Cheltenham, UK: Edward Elger, 2004), 102.*
46 Ahmad Budi Setiawan, Onny Rafizan, and Ashwin Sasongko Sastrosubroto, "Development of the Information and Communication Technology Service Industry in Indonesia," *Journal of Telecommunications and the Digital Economy 5, no. 3 (2017): 56–60.*
47 Merlyna Lim, "The Internet, Social Networks, and Reform in Indonesia," in *Contesting Media Power: Alternative Media in a Networked World, edited by Nick Couldry and James Curran (Oxford: Rowman and Littlefield Publishers, 2003), 276.*

48 "Huawei Wins Contract from Indonesia," *SinoCast China IT Watch*, (found on Factiva), June 23, 2003.
49 Jessica Ramakrishnan, "ZTE Wins CDMA 1X Contract From Indosat," *IHS Markit*, (found on Factiva), February 16, 2004.
50 "Telkom Awards Turnkey Cable Contract to Huawei Subsidiary," Comms Update, December 15, 2009, https://www.commsupdate.com/articles/2009/12/15/telkom-awards-turnkey-cable-contract-to-huawei-subsidiary; "Huawei Marine Upgrades PT Telkom 3rd Route Submarine Cable," Offshore Energy, March 27, 2014, https://www.offshore-energy.biz/huawei-marine-upgrades-pt-telkom-3rd-route-submarine-cable; and "Serat Optik Mataram-Kupang Beroperasi April 2011," [Mataram-Kupang Optical Fiber to be Operational in April 2011], *Kompas*, March 1, 2011, https://money.kompas.com/read/2011/03/01/22130497/index-html.
51 "Uji Coba Jaringan LTE, ZTE Jalin Kerjasama dengan Telkomsel" [LTE Network Trial, ZTE Cooperates With Telkomsel), *Tempo*, September 21, 2010, https://tekno.tempo.co/read/279413/uji-coba-jaringan-lte-zte-jalin-kerjasama-dengan-telkomsel; "Smartfren Launches LTE-A in Jakarta," Comms Update, August 21, 2015, https://www.commsupdate.com/articles/2015/08/21/smartfren-launches-lte-a-in-jakarta; and "Smartfren 4G LTE Rollout Reaches 85 Cities," Comms Update, January 27, 2016, https://www.commsupdate.com/articles/2016/01/27/smartfren-4g-lte-rollout-reaches-85-cities.
52 "ZTE Supported Makassar Smart City Solution," IndoTelko.com, August 19, 2015, accessed 15 May 2022, https://www.indotelko.com/read/1439949857/zte-makassar-smart-city-solution.
53 Rhenald Kasali, *Cracking Zone* (Jakarta: PT Gramedia, 2010), 50.
54 Authors' interview with government officials and cybersecurity specialists, December 2021 to March 2022.
55 Ali Farhoomand and Phoebe Ho, "Huawei: Cisco's Chinese Challenger," University of Hong Kong, 2006, https://hbsp.harvard.edu/product/HKU599-PDF-ENG.
56 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 27, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736; and Alan Weissberger, "WSJ: China's Financial Support Aided Huawei's Rise to #1 Telecom Vendor in the World," IEEE Communications Society Technology Blog, December 26, 2019, https://techblog.comsoc.org/2019/12/26/wsj-chinas-financial-support-aided-huaweis-rise-to-1-telecom-vendor-in-the-world.
57 Ibid.
58 "Chinese Government Pledges to Extend 200 Million USD Export Credit to Indonesia," AidData, https://china.aiddata.org/projects/38656/; "Chinese Government Pledges to Provide $300 Million Preferential Buyer's Credit Loan for Earthquake Reconstruction Activities," AidData, https://china.aiddata.org/projects/35147/; and Sumner Lemon, "China to Finance $1.1B in Telecom Equipment Exports," InfoWorld.com, February 20, 2004, https://www.infoworld.com/article/2667946/china-to-finance--1-1b-in-telecom-equipment-exports.html.
59 Industrial and Commercial Bank of China, "The World's First Renminbi Export Buyer's Credit Business Settled in ICBC," Industrial and Commercial Bank of China, August 18, 2010, https://web.archive.org/web/20220622171922/http://www.icbc-ltd.com/icbc/en/newsupdates/icbc%20news/The%20Worlds%20First%20Renminbi%20Export%20Buyers%20Credit%20Business%20Settled%20in%20ICBC.htm.
60 "CDB Provides $29.75 Million Buyer's Credit Loan for ZTE Fiber-to-the-Home (FTTH) Network Project," AidData, https://china.aiddata.org/projects/66446.
61 "Huawei Wins Contract From Indonesia," *SinoCast China IT Watch*, (found on Factiva), June 23, 2003.
62 "ZTE Opens Telecoms Training Centre in Indonesia," *DMAsia*, (found on Factiva), May 8, 2006.
63 Yudha Pratomo, "BSSN dan Huawei Kerja Sama Kembangkan SDM untuk Keamanan Siber," [BSSN and Huawei Cooperate to Develop Human Resources for Cybersecurity], *Kompas*, October 29, 2019,

https://tekno.kompas.com/read/2019/10/29/15460047/bssn-dan-huawei-kerja-sama-kembangkan-sdm-untuk-keamanan-siber; and Yuni Arisandy Sinaga, "Huawei Strengthens Cyber Security Cooperation With Indonesia," *Antara News*, September 28, 2021, https://web.archive.org/web/20220211113933/https://en.antaranews.com/news/191381/huawei-strengthens-cyber-security-cooperation-with-indonesia.

64 Koya Jibiki and Takashi Kawakami, "Huawei's 5G Deal With Indonesia Spearheads Southeast Asia Push," *Nikkei Asia*, December 2, 2020, https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-5G-deal-with-Indonesia-spearheads-Southeast-Asia-push; and "ZTE and Telkomsel Present 5G Use Cases at Telkomsel 5G Launch Event," *Jakarta Globe*, July 2, 2021, https://jakartaglobe.id/tech/zte-and-telkomsel-present-5g-use-cases-at-telkomsel-5g-launch-event/.

65 Australian Trade and Investment Commission, "Digital Technology to Indonesia: Trends and Opportunities," Australian Trade and Investment Commission, https://www.austrade.gov.au/australian/export/export-markets/countries/indonesia/industries.

66 Ibid.

67 Uly, "Garap Pasar 5G Indonesia, Ini Strategi Huawei," [Working on the Indonesian 5G Market, This is Huawei's Strategy].

68 "Program Huawei Seeds for the Future Ajak Mahasiswa Terbaik Indonesia Belajar Inovasi Teknologi di Tiongkok," [Huawei Seeds for the Future Program Invites the Best Indonesian Students to Study Technological Innovation in China], *Daily Social Newswire*, December 10, 2015, https://dailysocial.id/wire/program-huawei-seeds-for-the-future-ajak-mahasiswa-terbaik-indonesia-belajar-inovasi-teknologi-di-tiongkok.

69 "Huawei Seeds for the Future 2021 Readies Digital Talents for Future of Work," *Jakarta Globe*, November 2021, https://jakartaglobe.id/special-updates/huawei-seeds-for-the-future-2021-readies-digital-talents-for-future-of-work/#:~:text=Jakarta.,in%20Indonesia%20and%20the%20world.

70 Ratri Adityarani, "China's Huawei Opens Technology Training Center in Indonesia," Tech in Asia, April 12, 2011, https://www.techinasia.com/china-huawei-opens-technology-training-center-in-indonesia.

71 "Huawei Brings Digital Economy-Based Training and Wealth to State Colleges," *China Daily*, May 15, 2017, https://web.archive.org/web/20200417065638/https://www.chinadaily.com.cn/cndy/2017-05/15/content_29345046.htm.

72 "BSSN dan Huawei Kerja Sama Kembangkan SDM untuk Keamanan Siber," [BSSN and Huawei Cooperate to Develop Human Resources for Cyber Security], *Kompas*, October 29, 2019, https://tekno.kompas.com/read/2019/10/29/15460047/bssn-dan-huawei-kerja-sama-kembangkan-sdm-untuk-keamanan-siber.

73 "Huawei Strengthens Contribution and Cooperation in Indonesia Cyber Security," Huawei, September 28, 2021, https://web.archive.org/web/20211004105819/https://www.huawei.com/en/news/2021/9/tripartite-cooperation-agreement-indonesia-cyber-security.

74 Uly, "Garap Pasar 5G Indonesia, Ini Strategi Huawei," [Working on the Indonesian 5G Market, This is Huawei's Strategy].

75 Jayanty Nada Shofa, "Huawei Affirms Support for Indonesia's Digital Transformation With New Academy," *Jakarta Globe*, January 26, 2021, https://jakartaglobe.id/tech/huawei-affirms-support-for-indonesias-digital-transformation-with-new-academy.

76 "Dukung Pengembangan Teknologi Tanah Air, ZTE Dirikan Public Training Center di Indonesia," [Supporting National Technology Development, ZTE Establishes Public Training Center in Indonesia], *Kompas*, June 24, 2021, https://biz.kompas.com/read/2021/06/24/142410328/dukung-pengembangan-teknologi-tanah-air-zte-dirikan-public-training-center-di.

77 ZTE, "ZTE Opens Telecoms Training Centre in Indonesia," ZTE, June 19, 2006, https://web.archive.org/web/20220622154724/https://www.zte.com.cn/global/about/magazine/zte-technologies/2006/6/en_156/161603.html.

78 Gayatri Suroyo, "Alibaba's Jack Ma Says in Talks With Indonesia on Tech Training Institute," Reuters, October 13, 2018, https://www.reuters.com/article/us-imf-worldbank-tech-alibaba/alibabas-jack-ma-to-open-institute-for-tech-entrepreneurs-in-indonesia-idUSKCN1MN08U.
79 Huawei, "Huawei Strengthens Contribution and Cooperation in Indonesia's Cybersecurity."
80 Binus University and Apple offer a free joint ten-month developer program designed to get developers working on apps in Apple's ecosystem. See "Frequently Asked Questions," Binus Development Academy, May 24, 2022, https://web.archive.org/web/20220622175740/https://developeracademy.apps.binus.ac.id/faq/.
81 Brandon Vigliarolo, "The Apple Developer Program: What Professionals Need to Know," Tech Republic, June 4, 2021, https://www.techrepublic.com/article/the-apple-developer-program-what-professionals-need-to-know/#:~:text=This%20is%20the%20unfortunate%20part,the%20form%20of%20app%20 purchases; and authors' interview with Onno W. Purbo, February 2022.
82 Authors' interview with Onno W. Purbo, February 2022.
83 Authors' interview with Onno W. Purbo, February 2022.
84 "Huawei Strengthens Contribution and Cooperation in Indonesia's Cybersecurity," *Jakarta Globe*.
85 Authors' interviews with a range of senior Indonesian officials, academics, and industry sources, December 2021 to March 2022.
86 Authors' interviews with a range of senior Indonesian officials, academics, and industry sources, December 2021 to March 2022.
87 Authors' interview with Onno W. Purbo, February 2022.
88 Tugendhat, "How Huawei Succeeds in Africa: Training and Knowledge Transfers in Kenya and Nigeria."
89 Chinese Ministry of Foreign Affairs, "China-ASEAN Cooperation in 2012," Chinese Ministry of Foreign Affairs, November 19, 2012, https://web.archive.org/web/20220622173218/https://www.mfa.gov.cn/ce/cela//eng/news/t990470.htm.
90 Niva Yau and Dirk van der Kley, "China's Global Network of Vocational Colleges to Train the World, *Diplomat*, November 11, 2021, https://thediplomat.com/2021/11/chinas-global-network-of-vocational-colleges-to-train-the-world.
91 Yau and van der Kley, "China's Global Network of Vocational Colleges to Train the World"; Chinese Ministry of Education, "Luban Workshop——China's Vocational Education Going Global," *China Education Daily* (published on the ministry's website), May 11, 2018, https://web.archive.org/web/20220622173342/http://en.moe.gov.cn/Specials/Specials_40th/Achievements/201805/t20180531_337956.html.
92 Yau and van der Kley, "China's Global Network of Vocational Colleges to Train the World."
93 Chinese Ministry of Education, "Luban Workshop—China's Vocational Education Going Global."
94 "China Sets Up Tech Transfer Centers With ASEAN Countries," State Council, June 17, 2015, https://web.archive.org/web/20220622173621/http://english.www.gov.cn/news/top_news/2015/06/17/content_281475129044252.htm.
95 Xiaolin Zhou," Case Study From China: CATTC - China-ASEAN Technology Transfer Center," Organisation for Economic Co-operation and Development's TIP Co-Creation Project, December 9, 2020, 1, https://stip.oecd.org/stip/knowledge-transfer/case-studies.
96 "Zhongguo: Dongmeng Wangluo Anquan Jiaoliu Peixun Zhongxin Zhengshi Jiepai," [China-ASEAN Cybersecurity Exchange and Training Center Officially Opens], Sohu, October 29, 2019, https://web.archive.org/web/20220622173922/https://www.sohu.com/a/350380499_114731.
97 For example, the Swiss government has invested in skills training in Indonesia. See P. John Williams and Shaun Wellbourne-Wood, "Opportunities for Western Australian VET Providers in East Java," Western Australian Department of Jobs, Tourism, Science, and Innovation and Austrade, February 4, 2022, 45, https://www.wa.gov.au/system/files/2021-01/Opportunities%20for%20WA%20VET%20providers%20in%20East%20Java.pdf.

98 See the "Security and Threats" section in the following publication. Bland, Laksmana, and Kassam, "Indonesia Poll 2021: Charting Their Own Course."

99 *Rencana Kerja Pertahanan Negara Tahun 2013* [National Defence Strategic Plan, 2013] (Jakarta: Ministry of Defence, 2013), 12.

100 *Buku Putih Pertahanan Indonesia 2008* [2008 Indonesian Defence White Paper] (Jakarta: Ministry of Defence, 2008) https://web.archive.org/web/20220622174232/https://www.kemhan.go.id/ppid/wp-content/uploads/sites/3/2015/12/04f92fd80ee3d01c8e5c5dc3f56b34e3.pdf; and "Spotlight on Indonesia: Seizing the Digital Transition Opportunity Now," GSMA, https://www.gsma.com/spectrum/wp-content/uploads/2020/02/Indonesia-Digital-Dividend.pdf.

101 Buku Putih Pertahanan Indonesia 2008 [2008 Indonesian Defence White Paper], 38.

102 Goode and Kim, *Indonesia's AI Promise in Perspective, 20.*

103 "China-Indonesia Technology Transfer Center," Chinese Embassy in Indonesia, April 22, 2014, https://web.archive.org/web/20220622174500/https://www.fmprc.gov.cn/ce/ceindo/eng/whjy/kjjl/t1149138.htm.

104 Danielle Cave, Elsa Kania, Tom Uren, Fergus Hanson, Peter Jennings, Michael Shoebridge, Samantha Hoffman, Jessica Clarence and Greg Austin, "Huawei and Australia's 5G Network," Australian Strategic Policy Institute, 2018, https://www.aspi.org.au/report/huawei-and-australias-5g-network.

105 Danielle Cave, "The African Union Headquarters Hack and Australia's 5G Network," *Strategist, July 13, 2018,* https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network.

106 Jordan Robertson and Jamie Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack," Bloomberg, December 17, 2021, https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack; and Jordan Robertson and Jamie Tarabay, "Chinese Spies Accused of Using Huawei in Secret Australia Telecom Hack," BNN Bloomberg, December 16, 2021, http://origin.bnn.ca/chinese-spies-accused-of-using-huawei-in-secret-australia-telecom-hack-1.1697167.

107 Peter Hartcher, "Huawei? No Way! Why Australia Banned the World's Biggest Telecoms Firm," *Sydney Morning Herald, May 21, 2021,* https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html.

108 White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china; and Steve Holland and Doina Chiacu, "U.S. and Allies Accuse China of Global Hacking Spree," Reuters, July 20, 2021, https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/.

109 A range of Indonesian government officials and cybersecurity experts interviewed for this paper noted that Chinese intelligence services were likely responsible for several cyber attacks that had not been publicly attributed. Authors' interviews with several Indonesian officials and cybersecurity experts, December 2021 to March 2022.

110 Resty Woro Yuniar, "Indonesia Denies Report of Chinese Hacking Group Breaching Intelligence Agency Servers," *South China Morning Post, September 14, 2021,* https://www.scmp.com/week-asia/politics/article/3148680/indonesia-denies-report-chinese-hacking-group-breaching.

111 A range of Indonesian government officials and cybersecurity experts interviewed for this paper noted the extent of the cybersecurity threat from China but were uncertain about whether the use of Huawei and ZTE equipment would significantly aggravate this threat. Authors' interviews with several Indonesian officials and cybersecurity experts, December 2021 to March 2022.

112 See, for example, *ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021 (Australia Cyber Security Centre, Canberra: 2021),* https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf.

113 Evan A. Laksmana, "Pragmatic Equidistance: How Indonesia Manages Its Great Power Relations," in *China, the United States, and the Future of Southeast Asia, edited by David Denoon (New York: New York University Press, 2017), 113*–135, https://ssrn.com/abstract=2761998.

114 Philip Dorling, "Edward Snowden Leak: Australia Spied on Indonesian Phones and Data," *Sydney Morning Herald, February 17, 2014,* https://www.smh.com.au/politics/federal/edward-snowden-leak-australia-spied-on-indonesian-phones-and-data-20140216-32tux.html; and Ewen MacAskill and Lenore Taylor, "Australia's Spy Agencies Targeted Indonesian President's Mobile Phone," *Guardian, November 18, 2013,* https://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone.

115 Ewen MacAskill, "NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies," *Guardian, August 24, 2013,* https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

116 Christopher Knaus, "Witness K and Lawyer Bernard Collaery Helped Correct What They Saw as a Gross Injustice. They Now Face Jail Time," *Guardian, August 10, 2019,* https://www.theguardian.com/australia-news/2019/aug/10/witness-k-and-the-outrageous-spy-scandal-that-failed-to-shame-australia; and "NSA Australia Allies 'Spied on US Law Firm' in Indonesia Row," *BBC News, February 16, 2014,* https://www.bbc.com/news/world-us-canada-26216883.

117 Greta Nabbs-Keller and RM Wibawanto Nugroho Widodo, "Indonesia Responds to the Cyber Dark Side," Lowy Institute's *Interpreter, May 13, 2021,* https://www.lowyinstitute.org/the-interpreter/indonesia-responds-cyber-dark-side.

118 Jayanty Nada Shofa, "Huawei Affirms Support for Indonesia's Digital Transformation With New Academy," *Jakarta Globe*, January 26, 2021, https://jakartaglobe.id/tech/huawei-affirms-support-for-indonesias-digital-transformation-with-new-academy/.

119 "Indonesia Overtakes China as Top Source of Cyber Attack Traffic," *ABC, October 18, 2013,* https://www.abc.net.au/news/2013-10-18/an-indonesia-overtakes-china-as-top-source-of-cyber-attack-traf/5032428.

120 Hoor Halimah Anjani, "Policy Brief: Cybersecurity Protection in Indonesia," Center for Indonesian Policy Studies, Policy Brief No. 9, July 11, 2011, https://www.econstor.eu/bitstream/10419/249442/1/CIPS-PB09.pdf.

121 "Indonesia World's No. 1 Target for Cyber Attacks," *Asmag*, December 31, 2013, https://www.asmag.com/showpost/28975.aspx.

122 Thomas Paterson, "Indonesian Cyberspace Expansion: A Double-Edged Sword," *Journal of Cyber Policy* 4, no. 2 (2019): 216–234.

123 Adam Segal, Samantha Hoffman, Fergus Hanson, and Tom Uren, "Hacking for Ca$h," Australian Strategic Policy Institute, September 25, 2018, https://www.aspi.org.au/report/hacking-cash.

124 Fransiska Nangoy and Agustinus Da Costa, "Two Major Indonesian Hospitals Attacked in 'Ransomware' Storm," Reuters, May 13, 2017, https://www.reuters.com/article/us-cyber-attack-indonesia-idUSKBN1890AX.

125 Paul Mozur and Chris Buckley, "Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship," *New York Times*, August 26, 2021, https://www.nytimes.com/2021/08/26/technology/china-hackers.html.

126 Ibid.

127 Ibid.

128 According to statements of attribution from the United States and a range of its allies and partners, some of China's state-based espionage has been conducted in collaboration with cyber criminals. See Australian Ministry for Foreign Affairs, "Australia Joins International Partners in Attribution of Malicious Cyber Activity to China," Australian Ministry for Foreign Affairs, July 19, 2021, https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china. Jakarta probably nevertheless still judges that the primary threat it faces is from cyber crime rather than state-based espionage and security threats. Jakarta may well also believe that China would not use such tactics against Indonesia.

129 Huawei, "Huawei Strengthens Contribution and Cooperation in Indonesia Cyber Security."

130 Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," National Bureau of Asian Research Special Report no. 87, August 25, 2020, https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/.

131 On China-ASEAN cyber governance cooperation, see, for example, Chinese Ministry of Foreign Affairs, "Co-Chairs' Statement on the 1st ASEAN-China Cyber Dialogue," Chinese Ministry of Foreign Affairs, December 16, 2020, https://web.archive.org/web/20220622174812/https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202012/t20201216_599781.html; ASEAN-China Centre, "The China-ASEAN Information Harbor Digital Silk Road Industry Cooperation Forum Successfully Held," ASEAN-China Centre, November 25, 2020, https://web.archive.org/web/20220622174930/http://www.asean-china-center.org/english/2020-11/5581.html; and General Office of Hubei Provincial People's Government, "China-ASEAN Digital Economy Development and Cooperation Forum to Be Held in Wuhan," General Office of Hubei Provincial People's Government, July 14, 2021, https://web.archive.org/web/20220622175454/http://en.hubei.gov.cn/news/newslist/202107/t20210714_3644952.shtml.

132 "Memorandum of Understanding Between the National Cyber and Crypto Agency of the Republic of Indonesia and the Cyberspace Administration of the People's Republic of China on Cooperation in Developing Cyber Security Capacity and Technology." Authors had private access to this document.

133 Huawei, "Huawei Strengthens Contribution and Cooperation in Indonesia Cyber Security."

134 Eduard Lazarus, "The Authoritarian Threat of Indonesia's Latest Internet Bill," Lowy Institute's *Interpreter*, June 7, 2021, https://www.lowyinstitute.org/the-interpreter/authoritarian-threat-indonesia-s-latest-internet-bill.

135 "Indonesia," Freedom House Index, 2019, https://freedomhouse.org/country/indonesia/freedom-net/2019.

136 Eduard Lazarus, "The Authoritarian Threat of Indonesia's Latest Internet Bill," Lowy Institute's *Interpreter*, June 7, 2021, https://www.lowyinstitute.org/the-interpreter/authoritarian-threat-indonesia-s-latest-internet-bill.

137 "Vietnam Shuns Huawei as It Seeks to Build Southeast Asia's First 5G Network," *South China Morning Post*, August 27, 2019, https://www.scmp.com/news/asia/southeast-asia/article/3024479/vietnam-shuns-huawei-it-seeks-build-aseans-first-5g; and Aftab Ahmed and Sankalp Phartiyal, "India Likely to Block China's Huawei Over Security Fears -Officials," Reuters, March 11, 2021, https://www.reuters.com/world/china/india-likely-block-chinas-huawei-over-security-fears-officials-2021-03-11/.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org