Advancing a Liberal Digital Order in the Indo-Pacific

Lisa Curtis, Joshua Fitt, and Jacob Stokes

CNAS

About the Authors

Lisa Curtis is the Senior Fellow and Director of the Indo-Pacific Security Program at CNAS. Curtis has over two decades of experience working for the U.S. government, including as Deputy Assistant to the President and National Security Council Senior Director for South and Central Asia from 2017–2021. Curtis also worked at the CIA, State Department, Senate Foreign Relations Committee, and as Senior Fellow for South Asia at the Heritage Foundation from 2006–2017.

Joshua Fitt is a Research Associate with the Indo-Pacific Security Program at CNAS. He focuses on U.S. East Asian security strategy and specializes in Japanese and Korean Peninsular affairs. Before joining CNAS, Fitt was a campaign field organizer during the 2018 midterm elections in the Upper Midwest, an earthquake and tsunami disaster relief volunteer with IsraAID in Japan, and an intern with the Council on Foreign Relations' Japan Program. He earned his BA in East Asian studies from Yale University.

Jacob Stokes is a Fellow in the Indo-Pacific Security Program at CNAS, where his work focuses on Chinese foreign policy and East Asian security affairs. He previously served in the White House on the national security staff of then-Vice President Joe Biden. He has also worked as a professional staff member for the U.S.-China Economic and Security Review Commission, an advisor for U.S. Senator Amy Klobuchar, and a senior analyst in the China program at the United States Institute of Peace.

About the Indo-Pacific Security Program

The CNAS Indo-Pacific Security Program addresses opportunities and challenges for the United States in the region, with a growing focus on issues that originate in the Indo-Pacific but have global implications. It draws on a team with deep government and nongovernment expertise in regional studies, U.S. foreign policy, international security, and economic statecraft. The Indo-Pacific Security Program analyzes trends and generates practical and creative policy solutions around four main research priorities: U.S.-China strategic competition, India's growing role in the Indo-Pacific, the North Korea threat, and American alliances and partnerships.

Acknowledgments

The authors are grateful to the many officials and experts—both in the United States and elsewhere—who shared their perspectives over the course of this project. Additionally, this report would not have been possible without assistance from a variety of current and former CNAS colleagues, including Melody Cook, Isha Dalal, Christopher Estep, Allison Francis, Kara Frederick, Coby Goldberg, Kristine Lee, Maura McCarthy, Martijn Rasser, Ely Ratner, Paul Scharre, and Emma Swislow. The views presented here are the authors' alone and do not represent those of CNAS or any other organization. The authors are solely responsible for any errors in fact, analysis, or omission.

TABLE OF CONTENTS

Executive Summary

The United States and other regional democracies risk losing ground in the competition to shape Asia's digital future. China is making rapid inroads in developing the region's 5G infrastructure and is playing an increasingly expansive role in the broader digital ecosystems of Indo-Pacific countries.

Beijing's position at the center of Asia's developing digital order poses a series of challenges to the interests of America and its democratic allies and partners—ranging from the potential compromise of critical networks to the development of new technology standards that favor Chinese companies and undermine civil liberties. Policymakers are scrambling to ascertain how to compete effectively with China in the digital space, when Chinese companies and technology are already interwoven into the digital landscape. These Chinese companies are obligated to assist China on national security, intelligence, and cyber security issues, raising the prospect that they could be employed to carry out espionage or sabotage in the service of Chinese Communist Party (CCP) geopolitical goals.

In the case of 5G telecommunication network development, the United States will need to expand its campaign to promote additional trusted vendors who can supply safe, reliable, and cost-effective alternatives to Chinese offerings. Shaping the 5G ecosystem now will set the stage for how the broader U.S.-China technology competition will play out over the next decade. Undersea fiber-optic cables represent another area of technology infrastructure that is being contested between China and the United States. With nearly 95 percent of intercontinental internet data flowing through these undersea cables, it is imperative that they be treated and protected like other critical technologies and infrastructure.

Washington must recognize that many issues in digital development remain ambiguous, and it must craft policies that account for the field's complexity. For example, some countries will seek to maintain a relatively liberal political environment while embracing Chinese technology for economic development purposes. Others will seek out alternatives to Chinese suppliers as a means of maintaining their own security and independence but might still employ those technologies in illiberal ways in order to suppress dissent and maintain political control at home. Moreover, the fast-moving nature of innovation in digital technologies means that technological development will often outpace the creation of liberal political, legal, and regulatory regimes—even in the United States. The development of democratic norms and best practices to combat disinformation, restrict surveillance technologies, and give individuals the right to control their own data is still in a nascent stage. In other words, much of what constitutes a liberal digital order is still being defined.

The challenges to ensuring a future liberal digital order are immense; to meet them, the United States must develop a multifaceted approach that prioritizes coordination with democratic allies and partners. The Quadrilateral Security Dialogue between Australia, India, Japan, and the United States, or the Quad, will play a key role in ensuring protection of emerging and critical technologies through its newly formed working group, announced following the first-ever leaders-level Quad summit in mid-March. Working closely with other technologically advanced Indo-Pacific allies and partners such as South Korea and Taiwan on digital development initiatives will also be important. The degree to which the United States can work with democratic allies and partners to pool resources and capabilities, while also setting mutually agreed standards and guidelines for use of digital technologies, will determine whether those technologies are harnessed in a way that advances free and open societies or contributes to strengthening autocratic regimes.

To ensure digital development ultimately serves the purposes of building a liberal regional order, the United States needs to act with like-minded partners to:

> **The COVID-19 pandemic has accelerated Beijing's efforts to place digital technologies at the center of its strategy to enhance its geopolitical influence, particularly in the Indo-Pacific.**

Prioritize results-oriented diplomacy on digital issues.

- Follow through immediately on operationalizing the Quad working group on emerging and critical technologies.
- Increase diplomatic engagement on digital issues in both bilateral and multilateral settings, and in new purpose-built groups that focus on technology topics, such as the proposed "Technology 10" made up of the Group of Seven (G7) states plus South Korea, Australia, and India.
- Take a leadership role within international organizations involved in digital development, especially the International Telecommunications Union (ITU).

Develop digital technology investment standards and provide technology infrastructure alternatives to those offered by China.

- Catalyze the development of alternative 5G telecommunications equipment vendors.
- Forge a consensus on security standards for 5G networks by building on the process started at the Prague Conferences held in 2019 and 2020.
- Incentivize Indo-Pacific nations to invest in trusted and secure technologies and digital infrastructure.
- Develop assessment frameworks and standards to vet digital development projects.
- Assist other countries in implementing effective investment screening programs.

Shield democracy from digital threats while advancing internet freedom.

- With countries across the Indo-Pacific, enhance diplomatic engagements and assistance programs that deepen understanding about the need to balance the rule of law and prevention of violence with protecting civil rights, including that of free and peaceful speech.
- Build local resilience and capabilities of civil society, watchdog groups, and journalists to monitor digital development.
- Encourage U.S. technology companies to also engage with local civil society leaders, academics, and journalists to better understand and learn to identify disinformation.
- Draw from other countries' experience in combating disinformation.

Define and implement a digital governance model that reflects liberal values and can keep up with technological innovation.

- Lead a multinational effort to establish digital governance guidelines.
- Support technology innovation domestically and in contested spaces.
- Ensure adequate funding and resources for U.S. agencies—such as the U.S. Agency for International Development (USAID), U.S. International Development Finance Corporation (DFC), Millennium Challenge Corporation, and U.S. Trade and Development Agency—to implement digital development programs in Indo-Pacific countries.
- Use digital technology to empower the traditionally disempowered.

Introduction

The United States and other regional democracies risk losing ground in the competition to shape Asia's digital future. China is making rapid inroads in developing the region's 5G infrastructure and is playing an increasingly expansive role in the broader digital ecosystems of Indo-Pacific countries. The COVID-19 pandemic has accelerated Beijing's efforts to place digital technologies at the center of its strategy to enhance its geopolitical influence, particularly in the Indo-Pacific. In hastening the development of its Digital Silk Road, Beijing is assisting the developing economies in Southeast Asia with their digital transitions.

Beijing's position at the center of Asia's developing digital order poses a series of challenges to the interests of America and its democratic allies and partners—ranging from the potential compromise of critical networks to the development of new technology standards that favor Chinese companies and undermine civil liberties. The digital competition with China is occurring across multiple domains, from smart city infrastructure and telecommunications networks to video streaming websites and short form video sharing applications. Policymakers are scrambling to ascertain how to compete effectively with China in the digital space, when Chinese companies and technology are already interwoven into the digital landscape. These Chinese companies are obligated to assist China on national security, intelligence, and cyber security issues, raising the prospect that they could be employed to carry out nefarious activities, namely espionage or sabotage, in the service of Chinese Communist Party (CCP) geopolitical goals.

In the case of 5G telecommunication network development, the United States will need to expand its campaign to promote additional trusted vendors that can provide safe, reliable, and cost-effective alternatives to Chinese offerings. The United States must push back against efforts to discourage new 5G market entrants and ensure that Indo-Pacific countries have greater freedom of choice about their digital network decisions. The Chinese government has provided an estimated $75 billion in state subsidies to Chinese telecommunications equipment manufacturer Huawei and has unduly influenced the 5G standard-setting process. The only other companies offering alternatives to Huawei in radio access network equipment are Sweden-based Ericsson, Finland-based Nokia, and South Korea–based Samsung. Several countries in addition to the United States have already restricted Huawei's participation in their 5G ecosystems, including Japan, Australia, Sweden, and, more recently, India and the United Kingdom.[1] In a CNAS report published last year titled, "Open Future: The Way Forward on 5G," CNAS Senior Fellow Martijn Rasser makes the case for open radio access networks (OpenRAN) systems as a solution to the 5G conundrum. The idea behind OpenRAN is to establish an open architecture interoperability standard that allows operators to choose from multiple vendors, rather than having to depend on a sole vendor for hardware and software.[2] This is important, since it changes marketplace dynamics and restructures the industry around open interfaces that will stimulate competition. Shaping the 5G ecosystem now will set the stage for how the broader U.S.-China technology competition will play out over the next decade.

The fast-moving nature of innovation in digital technologies means that technological development will often outpace the creation of liberal political, legal, and regulatory regimes.

Another area of technology infrastructure that is being contested between China and the United States is the use of undersea fiber-optic cables. Given the enormous role of undersea cable infrastructure in facilitating the flow of growing amounts of data and information, it is imperative that undersea cables be treated and protected like other critical technologies and infrastructure. Ninety-five percent of intercontinental global data transmissions rely on undersea cables. The effort to protect and secure undersea cables is complicated by the fact that they are often constructed by multinational consortiums with no single legal framework to govern their use, because the cable lines join different continents and traverse international waters.[3]

A further challenge to ensuring that digital development remains aligned with democratic principles is the growing number of Chinese officials playing leading roles in technology standard-setting bodies, which provides China influence in shaping digital policy norms.[4] Chinese companies also often vote in blocs in favor of Chinse standards.[5] Fifty-five companies from the United States and allied countries participate in technology standard-setting bodies, compared to 128 Chinese companies.[6]

As Chinese companies entrench themselves at the heart of regional and national technology ecosystems, they bring with them Chinese conceptions of authoritarian governance as well as leverage and influence for the CCP. China's lack of transparency about the origins and spread of COVID-19, along with its military and political aggression toward its neighbors, both highlight the need for the United States and its allies and partners to ensure that global digital advancement facilitates prosperity and reinforces a liberal political order in this vital region.

The United States will need to help assemble overlapping coalitions with like-minded partners and allies to offer concrete alternatives to Chinese technology. The Quad will play a key role in ensuring protection of emerging and critical technologies through its newly formed working group, announced following the first-ever leaders-level Quad summit in mid-March. Working closely with other technologically advanced Indo-Pacific allies and partners, such as South Korea and Taiwan, on digital development initiatives will also be important.

The U.S. strategy to meet the challenges from China's expanding digital footprint will also require working closely with the American private sector, as well as civil society leaders, when it comes to setting standards and protecting civil liberties. These dialogues began to take shape under the previous U.S. administration, and the Biden team must intensify and elevate them as part of its strategy to compete more effectively with China in developing the digital economies of the Indo-Pacific.

Washington must recognize that many issues in digital development are ambiguous, and it must craft policies that account for the field's complexity. For example, some countries, such as Indonesia, will seek to maintain a relatively liberal political environment while also embracing Chinese technology for economic development purposes. Other countries, for instance Vietnam, will seek out alternatives to Chinese suppliers as a means of maintaining their own security and independence, but might still employ those technologies in illiberal ways in order to suppress dissent and maintain political control at home. Moreover, the fast-moving nature of innovation in digital technologies means that technological development will often outpace the creation of liberal political, legal, and regulatory regimes—even in the United States and other wealthy democracies. The development of democratic norms and best practices to combat disinformation, restrict surveillance technologies such as facial recognition, and give individuals the right to control their own data is still at a nascent stage. In other words, much of what constitutes a liberal digital order is still being defined.

The technology future of the region will directly impact the national security of the United States. Washington will not outspend Beijing dollar for dollar. Instead, America will have to leverage its private sector and civil society and allied and partner coalitions, while encouraging local, national, and regional efforts focused on building a more secure digital future that fosters democratic development and institutions.

Chapter One: China's Digital Footprint in the Indo-Pacific

China's expanding digital footprint abroad involves many aspects of digital ecosystem development across the Indo-Pacific region, from smart city and surveillance technology to new social media and entertainment platforms. Beijing's strategic toolkit for expanding its global technological presence comprises all these aspects—which contribute to normalizing illiberal digital practices. Challenges that have been on the periphery for some time, such as China's push to expand its digital presence through public health infrastructure development, have reached new significance with the advent of the COVID-19 pandemic. To formulate an effective response, it is essential to understand the underlying challenges triggered by each part of Beijing's involvement in the surrounding digital ecosystem. This chapter explores some of the most notable elements of Beijing's digital footprint.

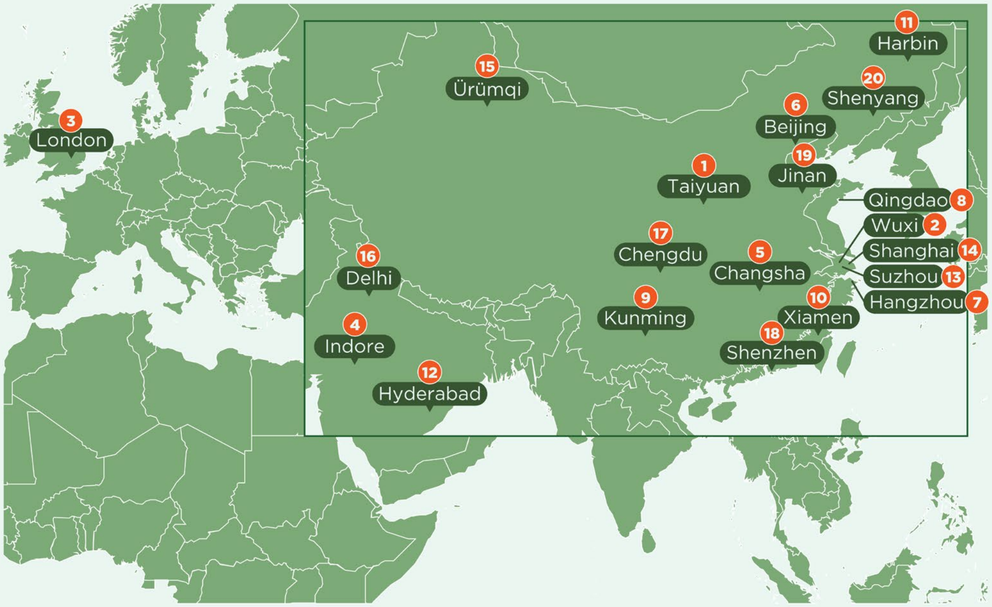
Smart Cities and Surveillance Technology

Similarly to how the Chinese Communist Party has created a comprehensive digital control architecture in which it can observe and limit the web activity of Chinese citizens, it has also ramped up its physical surveillance capabilities. A 2019 estimate placed the total number of surveillance cameras in China at nearly 350 million and predicted that the number would double by 2021.[7] With 16 of the top 20 most surveilled cities in the world located in China, these cameras capture a colossal amount of data about citizens' offline behaviors that previously stood beyond the reach of digital authoritarian control.[8]

To arrive at this point, China has been ramping up domestic smart city development. It has accomplished this by investing billions of dollars in new systems that use algorithms based on historical trends and real-time data to make the administration of everything from traffic control to law enforcement as efficient as possible.

In turn, China's leading surveillance camera manufacturers and developers of facial- and voice-recognition technology derive a significant share of their profits from government contracts.[9] Leveraging that financial support, these technology companies hone their products within China, benefiting from access to immense data pools. They profit further by being able to market their products abroad after they have been refined in domestic trials.[10]

CHINA TAKES THE LEAD IN MOST-SURVEILLED CITIES IN THE WORLD[11]



THE 20 MOST-SURVEILLED CITIES IN THE WORLD – CAMERAS PER 1,000 PEOPLE

1	Taiyuan, China	117.02
2	Wuxi, China	90.49
3	London, England	73.31
4	Indore, India	64.43
5	Changsha, China	55.81
6	Beijing, China	55.03
7	Hangzhou, China	50.98
8	Qingdao, China	45.62
9	Kunming, China	43.95
10	Xiamen, China	39.57
11	Harbin, China	38.13
12	Hyderabad, India	36.52
13	Suzhou, China	36.35
14	Shanghai, China	35.98
15	Ürümqi, China	35.21
16	Delhi, India	33.73
17	Chengdu, China	33.32
18	Shenzhen, China	31.77
19	Jinan, China	29.02
20	Shenyang, China	27.12

China has the lion's share of cities with the highest number of CCTV cameras per 1,000 people. Only four of the top 20 most-surveilled cities in the world are located outside of China.

With significant official support, Chinese companies have become global leaders in surveillance by forming partnerships with foreign governments and private companies to export cutting-edge surveillance technology.[12] This works because China's smart city exports are fulfilling demand for better urban governance abroad. However, in many cases, the surveillance technology also is appealing to emerging authoritarian leaders who seek new means of exerting control under the guise of good governance.

In the wrong hands, the technology easily facilitates greater social control and repression. That is exactly China's goal with its own smart cities. By using facial-, voice-, and gait-recognition software in combination with a network of surveillance cameras, Beijing eventually hopes to implement a dystopian artificial intelligence (AI)–driven predictive policing system that can detect criminal patterns before crimes are even committed.[13] It is therefore critical to understand whether other countries intend to use China's smart city technology and related AI projects for improving governance, or for controlling populations and stifling public dissent.

The Information Space

The combination of laws, censorship, and digital surveillance that forms the basis of Beijing's control over the internet in China has famously been dubbed "the Great Firewall," elements of which have been imitated in democracies and non-democracies alike. Under the guise of stopping the spread of disinformation on under-regulated online platforms, some Southeast Asian governments have implemented heavy-handed digital regulations modeled on Chinese law. Malaysia and Singapore both enacted far-ranging "fake news laws" that granted the government the ability to define and censor false online speech.[14] Likewise, Vietnam has drawn upon China's concept of "internet sovereignty" to implement data localization laws that support the government's censorship apparatus, although it has since walked back parts of the mandate that applied to the vast majority of foreign technology companies.[15]

While WeChat remains most popular in China, TikTok has found favor in markets abroad, including the Philippines, the United States, and Indonesia. TikTok was banned in India despite its initial success in the country. (Kevin Frayer/Getty Images)

As Chinese platforms gain a foothold in the still nascent Southeast Asian streaming market, their ability to shape the region's television and movie landscape in the long term will grow exponentially.

Chinese social media companies only occupy a small piece of the Indo-Pacific market, so Beijing's attempts to manipulate the social network information space often happens on platforms that it does not directly control. China's heavily censored national messaging app WeChat has struggled to make inroads outside of China, with some limited success in markets such as Malaysia largely due to local ethnic Chinese populations.[16] Instead, Chinese digital influence campaigns often take place on Facebook and Twitter, the platforms of choice in most of the Indo-Pacific.[17] However, as Facebook and Twitter have become increasingly aware that their platforms can be manipulated in foreign digital influence campaigns, they often identify and isolate the offending accounts. Last fall, Facebook removed accounts executing a campaign that targeted the Philippines, in which China-linked accounts attempted to garner support for Philippines President Rodrigo Duterte's relatively unpopular overtures toward Beijing.[18]

Though Beijing has been relatively unsuccessful in gaining its own foothold in much of the social media space, Chinese companies are performing well in the competition for video streaming markets. As quality 4G and eventually 5G networks enable more people to access fast download speeds, video streaming and sharing platforms will continue their meteoric rise in countries with newfound connectivity. Chinese video sharing platforms such as TikTok and Likee were among the 10 most downloaded apps in major regional markets including Indonesia and the Philippines.[19] But in India, where TikTok initially found its greatest foreign success,

China utilizes multilateral forums to advance national priorities. In July 2019, Foreign Minister Wang Yi met with the newly elected President of the United Nations General Assembly Tijjani Muhammad-Bande in Beijing. (Mark Schiefelbein/Pool/Getty Images)

a government ban has removed it from the market, along with a number of other Chinese apps.

Chinese companies are making a concerted effort to expand subscription-based video streaming platforms in international markets. Whereas American platforms including Netflix and Disney+ have well-established and reliable footholds in the Americas, Europe, and even the Middle East, they have not gained the same traction in the Indo-Pacific, although Disney+ launched operations in India a year ago. Netflix's market penetration in the Indo-Pacific is half of that in the Middle East, and one-quarter of that in Latin America.[20] Spying an opportunity, premium Chinese streaming platform iQIYI established its first overseas headquarters in Singapore and built offices across Southeast Asia, making plans to add Japanese- and Korean-language content to its predominantly Chinese-language catalog.[21] In Malaysia, iQIYI is partnering with the country's leading television services provider, Astro, to acclimate to the local market. Tencent Video, iQIYI's largest Chinese competitor, has also prioritized Southeast Asian markets including Thailand and Indonesia.[22] As Chinese platforms gain a foothold in the still nascent Southeast Asian streaming market, their ability to shape the region's television and movie landscape in the long term will grow exponentially.

The Digital Silk Road and Norms

Digital infrastructure is rapidly replacing China's former focus on traditional overseas infrastructure development projects. After several high-profile Belt and Road deals garnered global attention as possible examples of "debt-trap diplomacy" or failed to deliver the promised results, scrutiny and criticism from around the world drove Beijing to shift toward the Digital Silk Road (DSR)—Belt and Road's digital corollary.[23] These projects are less likely to fall apart in the same way, because digital infrastructure is often cheaper and logistically simpler to sustain than traditional Belt and Road projects.[24] Additionally, Chinese digital development products are often cheaper, faster, and come with greater regulatory flexibility than U.S., Japanese, or European alternatives. Cost is an especially important factor, as the COVID-19 pandemic has lessened the fiscal appetite for traditional infrastructure projects that carry heavy debt burdens. At the same time, COVID-19 has increased the urgency of effecting digital transitions among the world's developing economies. Most importantly, the digital focus of the projects provides a much greater strategic value to Beijing, because it establishes access to a country's digital ecosystem through hardware and software maintenance and upgrades.[25]

Underpinning Beijing's pivot toward the DSR are its efforts in multilateral settings—particularly inside the United Nations—to legitimize its projects and preferred technical norms through targeted financial support and strategic acquisition of leadership positions.[26] At the 2017 Belt and Road Forum, International Telecommunications Union Secretary General Houlin Zhou granted legitimacy to DSR projects by signing a memorandum on behalf of his agency that pledged the ITU's assistance to Chinese efforts to build information and communications technology networks in other countries.[27] To date, China has acquired more than two dozen similar memoranda in support of aspects of Belt and Road with other U.N. agencies and commissions.[28] Beijing has also attempted to use the United Nations system to normalize concepts such as internet sovereignty, which empower governments to expand their online censorship mandate and limit access to websites hosted abroad.

> **Most importantly, the digital focus of the projects provides a much greater strategic value to Beijing, because it establishes access to a country's digital ecosystem through hardware and software maintenance and upgrades.**

DSR projects are not all headline-grabbing 5G or smart city contracts—sometimes they are less flashy projects, for instance an undersea fiber-optic cable connection.[29] However, these projects deserve just as much scrutiny, because the viability of a country's 5G network depends on strong connectivity through undersea cables.[30] Ultimately, whether a DSR agreement is for a small-scale e-commerce partnership or a Huawei 5G rollout, it is a stepping-stone for further digital entanglement with Beijing—which is inadvisable at a time when China is increasingly relying on economic coercion against regional countries to achieve geopolitical goals.

Public Health

China began counting health technology among its global ambitions with the rollout of Beijing's Health Silk Road (HSR) in 2017. Initially a partnership between China and the World Health Organization to promote public health–related Belt and Road projects, the initiative evolved as Beijing realigned its infrastructure development priorities. As the DSR started to gain prominence, 5G became a central part of the Health Silk Road—with offerings from robotic nurses to remote consultations.[31] In the face of growing resistance to Chinese 5G equipment, Beijing tried to use benefits from the HSR as carrots to offer in exchange for signing a 5G deal with a Chinese company.

With the official blessing of the World Health Organization, Beijing has sought to strategically position itself at the heart of emerging health needs. The COVID-19 crisis has only increased the urgent need for public health infrastructure in much of the Indo-Pacific. After recovering from the pandemic in a relatively short time, China has attempted to take advantage of the opportunity to advertise HSR technologies and launder its public health image through mask diplomacy.[32] Beyond 5G, the global health emergency has created opportunities for surveillance companies to feature prominently under the HSR banner. Despite being on U.S. sanctions lists for their role in the oppression of minorities in Xinjiang, two of China's largest surveillance equipment companies—Hikvision and Dahua—have secured contracts to sell thermal imaging equipment overseas in the name of public health. Alibaba seeks to contract its cloud services for pandemic modeling exercises.[33] Such agreements give China's technology companies stronger footholds abroad, create opportunities for widespread international data collection, and facilitate greater social control and repression in countries with weak privacy and civil rights protections.

Chapter Two: Indo-Pacific Countries and Their Paths to Digital Development

The outcome of the competition between China and the United States to shape Indo-Pacific digital development will be a defining factor in the broader geopolitical struggle between Beijing and Washington to shape the regional order. The digital economies of the region are witnessing intense growth and expansion, as the number of internet users and use of hand-held devices have exploded in recent years, bringing the total size of the regional digital economies to around $400 billion.[34] U.S. technology companies maintain an extensive presence that will continue to expand, and to shape digital trends that impact society and governance. In most Indo-Pacific countries, WhatsApp, Facebook, Facebook Messenger, and Instagram represent the most used digital applications. Facebook has around 241 million users in Southeast Asia, or about 60 percent of the 400 million Southeast Asians who are online.

However, China's significant digital investments in the region during the past five years are beginning to challenge U.S. digital leadership and raise security concerns. Huawei has established itself as a leader in the race to introduce 5G coverage, and Huawei Marine has completed dozens of undersea fiber-optic cables in Southeast Asia in the past few years. Chinese e-commerce companies have also been more aggressive than their U.S. counterparts in regional expansion. In the past five years, Tencent and Alibaba have invested $12 billion in Southeast Asia. As China strengthens its digital position, countries become reliant on Chinese digital infrastructure and vulnerable to Chinese political influence and economic coercion.

China's bid for technology primacy in the region is not the only concern when it comes to assessing whether digitalization will contribute to or weaken liberalism in these countries. The manner in which individual countries choose to manage their own digital platforms also matters. The second part of this chapter explores the challenges digital expansion poses to governance and human rights in several Indo-Pacific nations.

Digital Development and Security

As countries in the Indo-Pacific expand their digital capabilities, many grapple with the potential national security implications of aligning themselves with Chinese technology. Chinese companies are required to share data with the government and have close ties with the CCP, forcing regional countries to weigh whether inexpensive technologies offered by Chinese companies merit the risk of enabling China to strengthen its grip on their technology ecosystems. Countries across the Indo-Pacific are dealing with this dilemma as they expand 5G coverage, integrate social media platforms, train their workforces to become more technically literate, and encourage private sector technology innovation. While U.S. allies and partners such as Australia, Japan, India, and Taiwan are taking measures to counteract China's growing regional digital footprint, other countries have either sought to take a middle-ground position to deal with the U.S.-China technology competition or are openly seeking Chinese support to propel digital trade.

5G telecommunications networks. One of the technology areas of greatest concern has been the Chinese push to dominate the development of 5G next generation telecommunications networks. The Trump administration led a campaign to discourage countries from relying on Huawei for 5G support, citing national security concerns, including the potential for Chinese surveillance, espionage, and sabotage—not to mention coercion, should a country become reliant on China for critical technology. The United States has taken a number of steps to disrupt Huawei's ability to operate in global markets. In 2019, the Department of Commerce placed Huawei on its Entity List, prohibiting U.S. firms from selling goods and services to Huawei without a license. Beginning in May 2020, the Unites States implemented a series of export controls targeting Huawei's ability to access semiconductor chips necessary for producing telecommunications gear for 5G networks.[35]

The Trump administration pursued diplomatic initiatives to raise awareness about the dangers of relying on Chinese 5G technology and encourage like-minded nations to develop alternatives to Chinese 5G offerings. The initial U.S. focus on promoting a ban on Huawei equipment started to evolve in mid-2020, culminating in support for OpenRAN as an alternative to Huawei end-to-end services. The U.S. government provided strong support for the Prague 5G Security Conferences held in May 2019 and September 2020, when international representatives from governments and industry, along with researchers, gathered to discuss the development, financing, and deployment of secure and trusted 5G telecommunications networks.[36] Following the 2019 meeting, the conference chairman issued a statement that included a non-binding set of principles—known as the Prague Proposals—in the categories of policy, technology, economy, security, privacy, and resilience.[37] Officials from various countries—including several Indo-Pacific countries such as Japan, Australia, South Korea, Singapore, New Zealand, and the United States—attended the conferences or have referred to those proposals as important guidelines for 5G development. At the 2020 Prague Security Conference (held virtually), there was discussion of OpenRAN as a potential solution to the 5G conundrum.[38] Additionally, the U.S. Clean Network initiative was established to develop common standards

> **Given that 95 percent of intercontinental data flow through undersea cables, it is imperative that these cable lines be treated and protected like other critical technologies and infrastructure.**

for secure 5G networks.[39] The Biden administration has not yet indicated whether it will continue to support the Clean Network initiative, but early signs point to a continuation of the concept in some form, though likely under a new name.[40]

Building telecommunications networks that are secure, technologically cutting-edge, and affordable will require sustained cooperation among like-minded countries. The recently released UK Telecoms Diversification Task Force Report presents a practical and comprehensive roadmap for ensuring the security of the UK telecommunications sector and enabling a competitive market supply of telecommunications equipment.[41] The United States must engage in subtle diplomacy so that states have feasible ways of choosing alternatives to Chinese suppliers without fear of reprisals from Beijing.

Undersea cables. Another area of technology infrastructure that is being contested between China and the United States is that of undersea fiber-optic cables. Given that 95 percent of intercontinental data flow through undersea cables, it is imperative that these cable lines be treated and protected like other critical technologies and infrastructure. Since they are often constructed by multinational consortiums, there must be cooperation among like-minded countries in leading and managing their construction**.** Further complicating the effort to protect and secure undersea cables is the fact that these massive cable lines join different continents and traverse international waters. This means there is no single governing system or legal framework to ensure their protection or guide their use.[42]

China is aggressively pursuing undersea cable construction across the globe. Huawei Marine (until recently a subsidiary of Chinese telecommunications giant Huawei) has built or repaired nearly 100 of the world's 400 undersea cables.[43] However, U.S. companies including Google, Facebook, Microsoft, and Amazon own or lease nearly half of the global undersea bandwidth.[44] The Chinese appear to view undersea cable laying as a strategic operation in a battle over data and information control.[45] In 2020, following U.S. sanctioning of Huawei Technologies, that company divested Huawei Marine, which is now majority-owned by another Chinese firm. Despite the divestment scheme, Huawei Marine is still listed in the U.S. Department of Commerce Entity List, which restricts the sale of U.S. goods and technology to the company.[46]

Another leader in resisting China's attempt to dominate the undersea cable industry has been Australia, which in January 2018 took control of a project, originally led by Huawei Marine, to build a cable from Australia to the Solomon Islands.[47] In October 2020, the United States worked with Australia and Japan to finance a submarine internet cable spur to the Pacific Island nation of Palau. This cooperation was possible under a memorandum of understanding (MOU) the three countries signed in 2018. The MOU enabled the U.S. Development Finance Corporation, the Japan Bank for International Cooperation, and Australia's Department of Foreign Affairs and Trade and Export Finance and Insurance Corporation to work together to mobilize private capital that would support major infrastructure projects in the region.

Taiwan's digital democracy shows strength under pressure. Taiwan is a frontline digital democracy. Since emerging in 1987 from decades of brutal military rule, the self-governing island has become a bastion of free speech in Asia.[48] Taiwan's democratic political system and vibrant media environment create the conditions for a liberal digital order there that, in many ways, serves as a regional model. At the same time, the island faces intense strategic pressure from China, which seeks to coerce Taipei into accepting rule from Beijing. As the Committee to Protect Journalists has noted, this creates a dilemma of how to protect freedom of speech while guarding against Beijing's attempts to interfere in Taiwan's political system by taking advantage of its openness.[49] That Taiwan's economy is deeply intertwined with China's complicates matters further. One report from the University of Gothenburg in Sweden finds that Taiwan is the target of more disinformation than any other liberal democracy in the world.[50]

Taiwan's government under President Tsai Ing-wen has taken steps to counter disinformation coming from Beijing and its proxies.[51] The government appointed a digital minister, Audrey Tang; supported initiatives to rapidly identify and fact-check false and misleading reports; and imposed fines for outlets and individuals who spread such reports.[52] Taiwan also places restrictions on media ownership and advertising by People's Republic of China state entities.[53] The task of countering disinformation remains a difficult one, however, because Beijing continues to improve its political influence operations and make them more sophisticated.[54] Content is difficult to trace on social media and can be posted using fabricated accounts. In addition, some press freedom groups have criticized steps the Taipei government has taken to counter Beijing's influence as constituting censorship—which underscores the difficulty of finding the right balance.

REGIONAL DEMOCRACIES WORKING TO COUNTER DISINFORMATION

Indo-Pacific democracies have identified disinformation as an important issue, and one the coronavirus pandemic has made even more pressing. Quad leaders included countering disinformation among the topics they discussed in ministerial-level meetings in fall 2020 and spring 2021.[60] But each of the four countries is in different stages of the process of developing and implementing responses to disinformation. Because steps to address the challenge often touch on related domestic policy topics such as media industry regulation and concerns about technology firms' user policies and business practices, they require balancing the interests of a number of stakeholders. Australia has made some progress by working with technology companies to develop a voluntary code of conduct, released in February 2021, for combatting disinformation and misinformation. This will be implemented by major platforms such as Twitter, Google, Facebook, Microsoft, and TikTok, and overseen by the government's Communication and Media Authority.[61] Japan's government has explored setting up a similar arrangement, but the effort has not yet come to fruition.[62] U.S. technology policy, which responds to disinformation from domestic as well as foreign sources, lags behind Australia's, even as some platforms, such as Twitter, have taken unilateral steps to regulate content on their sites in response to public pressure. India similarly faces foreign disinformation challenges that are difficult to separate from false or misleading reports spread by domestic actors.

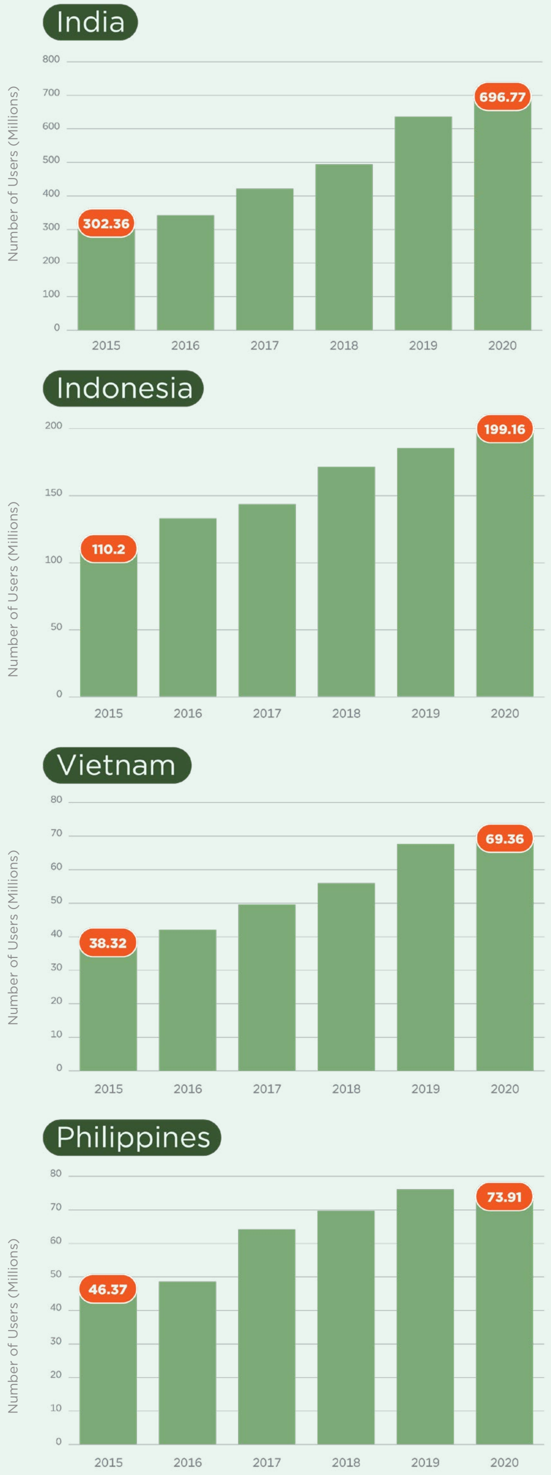
Restricting the use of hardware and software that do not meet rigorous security standards is another pillar of Taiwan's digital strategy. In December 2018, Taiwan reinforced its ban on network equipment made by Chinese companies Huawei Technologies and ZTE Corporation, which had been put into place five years prior.[55] In July 2019, the government in Taipei announced an expanded blacklist of Chinese companies whose products Taiwan's government agencies were prohibited from purchasing or using. These included Huawei and ZTE as well as Hikvision.[56] In April 2020, Taiwan banned the government use of platforms with security concerns, including the videoconferencing program Zoom, due to concerns about traffic being routed through servers in China and company employees being based there.[57] In August 2020, Taiwan announced new restriction on Taiwanese firms doing business with Chinese streaming services Tencent Holdings and iQIYI.[58] In addition, Washington and Taipei announced in August 2020 that Taiwan would join the U.S. Clean Network initiative for building secure 5G networks, with all five of Taiwan's local 5G telecommunications providers designated as trusted providers.[59]

An Indian army convoy on a highway bordering China carrying reinforcements and supplies toward Leh in September 2020. After the China-India border crisis in 2020, India began to distance itself further from Chinese technology. For example, Indian companies decided against using Chinese technology companies such as Huawei and ZTE.

India shifts away from Chinese technology. Prime Minister Narendra Modi has long recognized that technology will shape India's future and contribute to lifting millions of Indians out of poverty. As India pushes forward to become a digitally empowered society, it has recently begun distancing itself from Chinese technology, largely as a result of the 2020 India-China border crisis. In late June 2020—shortly after an India-China border clash left 20 Indian soldiers and at least four Chinese troops dead—two Indian companies linked to the Indian government announced they would forgo Huawei and ZTE services to upgrade their mobile coverage to 4G.[63] During the same timeframe, India ordered its state-owned telecommunications firms to stop sourcing gear from Chinese companies and banned nearly 200 Chinese apps from the country, blocking both new downloads and access to the apps for existing users.[64] This came as a blow to Chinese tech firms looking to introduce their products to the untapped market potential in India.[65]

In just the past five years, 560 million Indians have gained access to the internet, with 450 million Indians using smart phones.[66] Before the China-India border crisis, China's investments in India's technology sector totaled around $4 billion, and as of March 2020, 18 of India's 30 unicorns (privately held start-up companies) were funded by Chinese investors.[67] Before India banned the Chinese apps, Tencent had been the biggest Chinese technology investor in India, with investments ranging from food delivery and gaming to music streaming and news aggregation. Its largest investment ($700 million) was in the e-commerce platform Flipkart.[68] Experts have indicated that Tencent is likely to decrease its investments in India due to the app ban but is still looking for ways to maintain a presence in the Indian market.[69] Last September, Tencent invested $62.8 million in Flipkart, and reportedly continues to hold a 5 percent stake in Flipkart through a Singapore-based subsidiary.[70]

RAPIDLY INCREASING INTERNET CONNECTIVITY ACROSS THE INDO-PACIFIC[71]



Over the past five years, the number of internet users in the Indo-Pacific has skyrocketed. In India, the number of users more than doubled. In Indonesia, Vietnam, and the Philippines, the number of users nearly doubled. As countries build out their digital ecosystems, people can more easily take advantage of new services.

However, Chinese technology investments in India were still relatively low when compared with investments from U.S. companies. For example, U.S. investments since 2014 in India's start-up and technology industries total around $30 billion. This includes Facebook's April 2020 announcement of a $5.7 billion investment in India's Jio Reliance Industries, and Google's July 2020 pledge to invest $10 billion over five years to accelerate the proliferation of digital services in India.[72]

Although China's inexpensive services offered by companies such as Huawei were once attractive to India,[73] that nation now seeks to counter China's digital influence. Under new procurement rules expected to come into force in June 2021, India will likely prevent its mobile carriers from using Huawei equipment. According to two officials from India's telecommunications department, after June 15, Indian telecommunications carriers will be allowed to purchase certain equipment only from "trusted" vendors.[74]

Part of India's strategy to counter Chinese digital influence is to partner more closely with Japanese companies.[75] Japan and India are jointly seeking to develop 5G and 6G infrastructure and develop health technology and digital literacy training programs. Japan will export new technologies to India, including 5G wireless networks and submarine fiber-optic cables, while India has agreed to help build digital prowess among the Japanese workforce to foster innovation in that country.[76] India will rely on Rakuten, a Japanese electronic commerce and retail company, to export a "cloud-based mobile network" to India, which will reduce the costs of installing and operating 5G networks.[77] Although India's implementation of 5G is still some time away, Rakuten has already opened a laboratory in the southern Indian city of Bengaluru to sell 5G to Indian telecom carriers. With the support of both the Indian and Japanese governments, the Japanese information technology company NEC laid an underwater fiber-optic cable to connect mainland India with the Andaman and Nicobar Islands.[78]

South Korea builds digital independence. South Korea has established itself as a digital development leader in the region, forging its path with nationwide plans including the Korean New Deal. It was the first country to roll out 5G in 2019 and leads both the region and the world in coverage. However, Chinese companies have played a key role in South Korea's path to becoming a digital leader, and they have developed close partnerships with Korean companies on 5G development.[79] South Korean

> **Vietnam has not issued a formal ban on Huawei but appears unlikely to use its equipment in its 5G networks.**

companies provide Huawei with component parts, including semiconductors, memory chips, and smartphone displays. Huawei, in turn, opened a lab in Seoul for South Korean companies to test their 5G capabilities. The South Korean company TMax Data is projected to use Huawei for a cloud services center.[80] Despite the robust partnerships between South Korean companies and Huawei, South Korea has not developed sole dependence on Huawei. Two of the three South Korean telecommunications companies rely on Samsung equipment for their 5G capabilities, with only one, LG Uplus, relying on Huawei.

South Korea's sophisticated digital ecosystem and continued investment in its development will allow Seoul to forge an independent digital path. Seoul announced the Korea New Deal in 2020, an economic plan based on two component parts: the Green New Deal and the Digital New Deal. The latter was announced to catalyze digital innovation and economic growth in the country by building 5G and cloud computing infrastructure and developing the nexus between 5G and AI.[81] The administration of President Moon Jae-in plans to allocate more than $2.2 billion toward the initiative. In 2019, the South Korean government announced the AI national strategy in hopes of catching up in these capabilities with the United States. South Korea aims to raise its digital competitiveness by 2030. Geared toward transforming the nation into a global AI leader, the strategy calls for spending $820 million over 10 years to support the development of the AI semiconductor industry.[82] The South Korean government also hopes to develop "smart" memory chips and build an AI cluster in the southwestern city of Gwangju.[83]

Vietnam keeps Chinese tech at arm's length. In a surprise development last December, Vietnam's state-owned telecommunications giant Viettel announced it had launched a 5G commercial trial in parts of Hanoi, making Vietnam one of the first countries in the world to deploy 5G services. The company said it had used both imported and indigenous technology to make the digital transformation, which will enable the rapid advancement of digital services, providing a boost to the economy. According to the government, the rollout of 5G will begin in urban areas, followed by deployment in industrial parks, research zones, and universities to aid innovation.[84] Viettel said it would provide unlimited 5G data services free of charge during the trial period, which will test the stability of the equipment before taking it to full commercialization. Vietnam has not issued a formal ban on Huawei but appears unlikely to use its equipment in its 5G networks.[85] The nation has conducted 5G trials with Nokia and Ericsson equipment.

Singapore emerges as a hub for Chinese technology. Singapore, viewed as an attractive regional base to access the growing number of digital users throughout Southeast Asia, has become a hub for Chinese technology companies such as Tencent, Alibaba, and ByteDance. With Chinese technology companies investing billions into the city-state, Singapore now houses a larger number of Chinese technology companies than any other country outside China.[86] Singapore's stable politics and predictable legal system make it an attractive foreign investment destination, and the perception that Singapore has taken a neutral stance amid rising U.S.-China tensions has further encouraged Chinese technology firms to set up shop in the country. Launching from their Singapore headquarters, Chinese companies are able to access regional markets in the Philippines, Indonesia, Vietnam, and other Southeast Asian nations.[87]

Singapore is partnering with a host of countries, including China, in its push to develop 5G telecommunications networks, AI, and the Internet of Things, especially in the wake of the global pandemic. For example, the Singapore government pledged $40 million to promote 5G innovation and create 1,000 new positions centered around 5G expertise after the announcement of an initiative between InfoComm Media Development Authority and mobile network operators. While Singapore allowed Chinese companies to participate in its 5G trials, it ended up choosing Ericsson and Nokia.[88]

> **Singapore's stable politics and predictable legal system make it an attractive foreign investment destination, and the perception that Singapore has taken a neutral stance amid rising U.S.-China tensions has further encouraged Chinese technology firms to set up shop in the country.**

Indonesia opens doors to Chinese tech. Indonesia's government under President Joko Widodo has put digital development at the center of its economic growth strategy and has undertaken relatively robust cooperation with China on digital issues.[89] During Chinese State Councilor and Foreign Minister Wang Yi's state visit to Indonesia in January 2021, the two countries signed an MOU on developing cybersecurity capacity building and technical cooperation.[90] *Global Times*, a semi-official Chinese state paper, described it as the "first-of-its-kind internet security agreement China signed with a foreign country" and a "strategic counterattack" against the U.S. Clean Network program.[91] Chinese vendors, namely Huawei and ZTE, have a large presence in Indonesia, have supplied much of the country's existing telecommunications equipment from 2G to 4G, and are now poised to play a major role in 5G infrastructure.[92]

The Philippines relies on Chinese technology, straining ties with the United States. China's heavy hand in the Philippines' digital expansion raises questions about cybersecurity implications for a country that is a treaty ally of the United States. The Philippines was the first Southeast Asian nation to roll out 5G coverage in 2019. It did so with a Philippine telecommunications company in which Telecom, a Chinese company, has a 40 percent stake. In November 2017, Philippine President Rodrigo Duterte, in a meeting with Chinese premier Li Keqiang, offered China the opportunity to operate a Philippine telecommunications carrier. China's Telecom chose as its local partner a Philippine company with no experience in telecommunications, but whose owner had contributed to Duterte's election campaign.[93]

Another major concern is President Duterte's enthusiastic embrace of Chinese surveillance technology. During Xi Jinping's state visit in November 2018, Duterte signed 29 agreements, including a "Safe Philippines Project," contracting Huawei and China International Telecommunication and Construction Corporation to construct a 12,000-camera surveillance system across metropolitan Manila and other cities. The project, intended to help police fight crime with facial-recognition technology, will be funded by Chinese loans. Congressional critics in the Philippines tried to block it, citing privacy and security concerns, but Duterte vetoed their decision. He has run a ruthless anti-drug campaign, including thousands of extra-judicial killings, and has arrested political opponents who have been critical of his human rights record. The United States last year sanctioned a senior official who had served as police chief during the period when the extra-judicial killings occurred. The exchange of surveillance technology provides China the opportunity not only to export its autocratic governing techniques, but also to solidify ties with a fellow illiberal leader.

Malaysia closely partners with Chinese technology companies. Malaysia is working closely with China on its digital development as it focuses on advancing 4G capabilities, and seeks to create employment opportunities, simplify banking and finance transactions, provide increased access to virtual education, and bring medical facilities to remote towns.[94] Malaysia worked with China to establish a Digital Free Trade Zone (DFTZ) to help small and medium enterprises expand their operations through streamlining e-commerce functions and removing high tax rates and customs clearances and inspections. The DFTZ, backed by companies such as China's Alibaba Group and Malaysia's Digital Economic Corporation, aims to boost international e-commerce between China and Malaysia.

In 2019, Malaysia also announced the development of an AI park, an initiative relying heavily on investment from China. Malaysian company G3 Global Bhd and two Chinese companies, the SenseTime Group and Harbour Engineering, are collaborating on the park, which is expected to become a center of technology development and research, with investments totaling $1 billion over five years. Together the Malaysian and Chinese firms are developing AI solutions to bolster Malaysia's electronics industry, including its nascent semiconductor industry, and position the country to eventually compete with neighbors Indonesia and Singapore as a digital investment hub.[95]

WeChat Pay MY became one of Malaysia's top e-wallet operators a year after it entered the market, owing to the large Chinese diaspora located there.[96] Given WeChat's track record of censorship—for instance, during the 2019 democracy protests in Hong Kong, Tencent suspended the accounts of WeChat users who criticized Beijing—Malaysians could be putting themselves at risk for future CCP punishment and coercion.[97]

Digital Development and Governance

While China's aggressive push to dominate digital development in the Indo-Pacific is a key challenge for advancing a democratic digital order, the illiberal manner in which some Indo-Pacific countries manage their own digital platforms also poses concern. There is a need to explore how technology development affects governance and civil liberties across this vital region. While there is consensus among democratic nations that at least some degree of regulation is necessary for managing social media and digital applications, the level and type of regulation is under debate, and countries are implementing their own national policies, regulations, and legislation for dealing with the rapidly evolving digital landscape. The swift progress in the evolution of digital technology is outpacing multilateral coordination on setting international, widely accepted guidelines and standards for governing its use.

In the Philippines, social media platforms were weaponized during President Rodrigo Duterte's campaign, fueling hate in the country. On December 10, 2019, International Human Rights Day, thousands of Duterte's critics marched to condemn human rights violations that had occurred under his rule. (Ezra Acayan/Getty Images)

Meanwhile, online communications platforms are reshaping politics and political discourse throughout the Indo-Pacific. For instance, in 2018 WhatsApp helped topple 50 years of one-party rule in Malaysia, and Tinder, the dating application, played a role in the 2020 Thai protest movement. Social media has imperiled elections in Indonesia and the Philippines and has been abused to stoke ethnic and religious violence in India and Burma. While a degree of regulation is necessary to ensure the rule of law and prevention of violence, some states have gone too far in their restrictions on access to social media and online communication and have violated individual liberties and restricted peaceful and lawful free speech.

Philippines exploits social media during elections, fuels hate. In the Philippines, where 97 percent of people with internet access used Facebook in 2019, fake news operations coordinated and funded by Rodrigo Duterte's PDP-Laban Party backed his presidential campaign. They continued to fuel his violent anti-drug war after he took office. In September 2020, Facebook belatedly took down hundreds of accounts with links to China, the Armed Forces of the Philippines, and Duterte's social media strategist, arguing they violated its policy on "coordinated inauthentic behavior on behalf of a foreign or government entity."[101]

Indonesian extremist group peddles anti-Christian conspiracy theories. A group called the Muslim Cyber Army used Facebook and Twitter to disseminate conspiracy theories about the Christian governor of Jakarta, Basuki Tjahaja Purnama, derailing his 2017 re-election bid and leading to his arrest on blasphemy charges. Indonesian police later arrested more than a dozen members of the extremist network, which had been orchestrating online disinformation campaigns in an attempt to push the country in an Islamist direction.[102]

Burmese military misuses social media and instigates ethnic cleansing. In 2017, the Burmese military weaponized Facebook by setting up fake accounts to spread hate speech about the Rohingya ethnic minority. Military officials took advantage of Facebook's role as the de facto internet in Burma. They set up fake troll accounts tied to celebrities and the entertainment industry to spread incendiary posts against the Rohingya.[103] The accounts run by the military generated more than a

THE MILK TEA ALLIANCE: CIVIL SOCIETY AND DIGITAL ORGANIZING IN THE INDO-PACIFIC

Recent years have seen young Asian pro-democracy activists protesting repression by authoritarian governments across the region. Protestors from Hong Kong, Taiwan, Thailand, and Myanmar have contributed to an online solidarity movement known as the Milk Tea Alliance, named after the popular drink in those places.[98] Members of the group send each other messages of support—for example, photos of them making the three-finger salute that has become the movement's symbol—and work together to counter pro-regime supporters online. They also share tactical tips on how to evade digital surveillance and carry out effective and sustainable demonstrations.[99] Some activists hope the group can become a pan-Asian youth democracy movement, although skeptics note that primarily online support has inherent limitations that will be hard to overcome in the face of the physical violence by government security forces in Hong Kong, Thailand, and Myanmar.[100]

The Myanmar February 2021 military coup has led to the deaths of hundreds of protestors. Residents protest the coup during a candlelight vigil in Yangon. (Getty Images)

million followers and contributed to violence against the ethnic minority group, leading to the exodus of more than 700,000 Rohingya from the country. The United Nations called it "a textbook ethnic cleansing."[104] In November 2018, an independent human rights organization—commissioned by Facebook—published its findings about how the social media platform was used to instigate the violence. Recommendations were provided for Facebook to improve enforcement of its content policies and increase engagement with local stakeholders.[105] Facebook, acknowledging it had not done enough in Burma to prevent violence against the Rohingya, took down the pages of the army chief, several other military officials, and hundreds of fake accounts being used to spread hate speech. Facebook also added more Burmese-speaking content moderators for the country.[106]

Over the past several months, Facebook struggled with how to balance speech protection for democratic politicians and democracy activists on the one hand, and on the other cooperation with the military regime to prevent shutdowns of the platform, which is the main source of information for most of Burma's population.[107] Facebook sought to prevent misuse of its platform by the Burmese military both during and following the country's November 2020 election. Before the election, Facebook announced it had taken down a network of 70 fake accounts and pages operated by the military. After the election, a Facebook spokesperson announced the company would remove any content that sought to delegitimize the outcome.

Following February's military coup, Facebook has taken several steps to protect democracy supporters. Immediately following the coup on February 1, a civil disobedience page gained 200,000 followers, and a related hashtag was used more than 1 million times. This prompted the military to temporarily ban Facebook in order to restrict the flow of information and prevent the political opposition from using the platform to organize.[108] Three weeks after the coup, Facebook removed Burmese military and military-controlled pages from both its Facebook and Instagram sites, and banned all ads from military-linked businesses.[109] In a statement following the move, the company said, "Events since the February 1 coup, including deadly violence, have precipitated a need for this ban. We believe the risks of allowing the Tatmadaw [Burmese military] on Facebook and Instagram are too great." Facebook continues to provide updates on its actions in Burma. On March 31, it announced that it would remove content that violates the company's community standards, and that it had added a new safety feature allowing Burmese users to lock their profiles. On April 14, Facebook announced it would remove posts praising or supporting violence by Burmese security forces and against civilians.[110]

India's frequent internet shutdowns stymie free speech. Democracies do not always agree on how to regulate social media platforms and set standards for digital development, and nowhere has this been more evident than in India's repeated shutdowns of the internet. According to digital rights group Access Now, by 2020 India had imposed the highest number of internet shutdowns (109) of any country for the third consecutive year. Yemen came in second place with six, and Ethiopia in third place with four.[111]

Those who have suffered the most from India's aggressive internet disruptions are the Kashmiris. In August 2019, following the Indian government's decision to rescind Jammu and Kashmir's autonomous status, New Delhi halted all broadband and mobile internet services and maintained a complete lockdown in the region to avoid protests and violence. In January 2020, the government resumed 2G internet service in the region but kept social media restrictions in place. Civil society leaders and nongovernmental organizations filed petitions with India's Supreme Court against the internet restrictions, but failed to convince it to force the government to rescind the internet shutdown order.

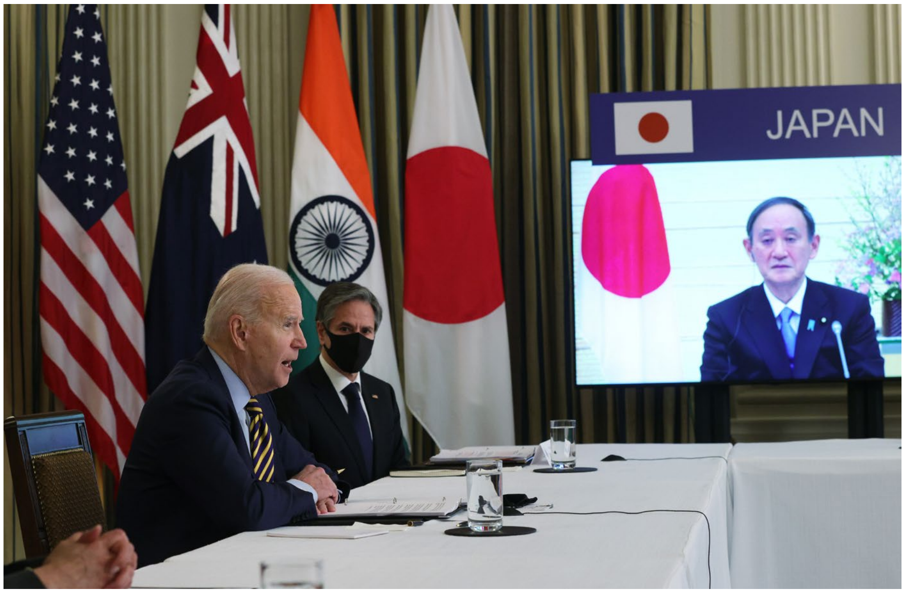
In February 2021, India unexpectedly announced new social media regulations, the Intermediary Guidelines and Digital Media Ethics Code. The new regulations require Facebook, Twitter, and YouTube to appoint India-based compliance officers, who will provide monthly reports detailing complaints received and actions taken by the company to address them. The social media companies must remove content within 36 hours of receiving a legal order from authorities and will be required to reveal the originator of the content. While these new regulations may have some merit, the hurried manner in which they were announced, with little to no warning to the affected companies, does not bode well. Many observers view the rushed new orders as a response to a recent dispute between the Indian government and Twitter regarding hashtags related to farmer protests that have rocked the government since last fall.

Chapter Three: The Way Forward: Elements of Establishing a Liberal Digital Order in the Indo-Pacific

The challenges to ensuring a future liberal digital order are immense and require the United States to develop a multifaceted approach that prioritizes coordination with democratic allies and partners. As the United States gets a handle on the scope of the problem, it should prioritize working with the other Quad countries—Australia, India, and Japan. The announcement of a Quad working group to focus on critical and emerging technologies following the first-ever Quad summit (in mid-March) is encouraging. It offers a unique multilateral venue to begin examining the challenges and exploring potential solutions. However, working and coordinating with partners outside the Quad, such as digitally advanced Asian ally South Korea and partner Taiwan, as well as the UK and European Union (EU), which recently released its Indo-Pacific strategy, also is critical. The degree to which the United States can work with these countries and partners to pool resources and capabilities while setting mutually agreed-upon standards and guidelines will determine whether digital technology is harnessed in a way that advances free and open societies or contributes to strengthening autocratic regimes.

Washington must recognize that many issues in digital development are ambiguous, and it must craft policies that account for the field's complexity. For example, some countries, such as Indonesia, will seek to maintain a relatively liberal political environment while embracing Chinese technology for economic development purposes. Others, such as Vietnam, will seek out alternatives to Chinese suppliers as a means of maintaining their own security and independence, but might still employ those technologies in illiberal ways to suppress dissent and maintain political control at home. Moreover, the fast-moving nature of innovation in digital technologies means that technological development will often outpace the creation of liberal political, legal, and regulatory regimes—even in the United States and other wealthy democracies. The development of democratic norms and best practices to combat disinformation, restrict surveillance technologies such as facial recognition, and give individuals the right to control their own data is still at a nascent stage. In other words, much of what constitutes a liberal digital order is still being defined.

To ensure that digital development ultimately serves the purpose of building a liberal regional order, the United States should:



At the first Quad summit, held in March 2021, President Joe Biden, left, and Secretary of State Anthony Blinken, right, met with the leaders of Australia, India, and Japan. (Alex Wong/Getty Images)

Leverage relationships with allies and partners for results-oriented diplomacy on digital issues.

- *Follow through immediately on operationalizing the Quad working group focused on emerging and critical technologies.* The National Security Council (NSC) should guide U.S. inter-agency efforts to operationalize the Quad working group on emerging and critical technologies that was announced following the first-ever Quad summit held in mid-March. The working group should immediately identify which areas of technological development are most critical to maintaining a free and open political order, and then develop a common understanding of the challenge. The four countries should decide on a coordinated policy approach and then consider how to expand multilateral action within a wider group of democratic nations.
- *Prioritize digital issues in bilateral engagements and in multilateral groupings.* Coordination with allies and partners on digital issues must be prioritized. This includes South Korea and Taiwan bilaterally, multilaterally through the EU, and in new purpose-built groups focusing on technology topics, for instance the proposed Technology 10, made up of the G7 states plus South Korea, Australia, and India.[112] Washington should practice positive "forum-shopping" that chooses venues based on their ability to get real-world results. In late April the EU released its Indo-Pacific strategy. It highlighted the need to work with partners who share principles on quality and sustainable connectivity based on international norms, and to promote digital governance in line with a free and open cyber space.[113]
- *Take a leadership role within international organizations involved in digital development, especially the ITU.* In addition to playing a larger direct role in shaping international standards that govern digital development, the United States should seek to expand the diversity of nongovernmental organization and private company membership within the ITU to ensure that authoritarian actors cannot dominate the organization. Furthermore, USAID and the International Development Finance Corporation (DFC) should coordinate directly with the ITU Development Sector (ITU-D), which provides technical assistance and service delivery to bolster telecommunications equipment and networks in developing countries. USAID could establish a partnership with ITU-D to conduct joint needs assessments and programming. This will provide a valuable opportunity to inculcate U.S. digital values and best practices within the multilateral organization. Other international organizations that are involved in addressing global digital challenges include the G20, the Organization for Economic Co-operation and Development (OECD), and U.N. agencies such as the U.N. Development Program, which recently released a new digital strategy to develop innovation, digital literacy, digital communication, and digital ecosystems. One recent example of multilateral work in the digital space is the July 2020 G20 ministers' announcement of support for an "open, fair, and non-discriminatory" environment.[114]

Work with allies and partners, in close coordination with the U.S. private sector, to develop both standards for digital technology investments and technology infrastructure alternatives to those offered by China.

- *Catalyze the development of alternative 5G telecommunications technology vendors.* U.S. policymakers must better understand and respond to the preferences of governments that consider Chinese suppliers. For developing countries in particular, factors such as price, speed of project approval and construction, and technical support are often as important as security. Security advantages alone will often not be enough to shift their decision-making calculus. A promising way forward on 5G telecommunications development is explained in a CNAS report published last year titled, "Open Future: The Way Forward on 5G," by CNAS Senior Fellow Martijn Rasser. He makes the case for OpenRAN systems as a solution to the 5G conundrum.[115]
- *Continue to forge an international consensus on security standards for 5G networks.* The NSC should lead an inter-agency process to determine if it will continue the Clean Network initiative, or something similar to it, and whether it will maintain strong support for the Prague Process. While several countries have been reluctant to sign on to the Prague Proposals for developing and deploying 5G infrastructure, the conferences have provided useful forums for raising awareness about 5G security challenges and discussing potential solutions such as OpenRAN.[116]
- *Incentivize Indo-Pacific nations to invest in trusted and secure technologies and digital infrastructure.* Since many of these countries have not yet committed to either a closed or an open digital development path, it is crucial for the United States to develop tailored approaches that influence the private sectors and key decisionmakers in these countries. Specifically, the United States should use the expanded authorities of the DFC to provide financial support or incentives for

U.S. companies, or to select digital firms from allied or partner countries that are well-positioned to provide trusted alternatives to Chinese digital investments. The DFC can help galvanize the entry of U.S. international technology firms into higher-risk markets, where they can compete with Chinese companies.

- *Develop assessment frameworks and standards to vet digital development projects.* Along the lines of the Blue Dot Network—a concept developed by the previous U.S. presidential administration to certify transparent, sustainable, and inclusive infrastructure projects—the State Department, USAID, and DFC should collaborate to develop standards specific to digital infrastructure projects that can be coordinated with allies and partners. After the standards are developed, the State Department can spearhead an effort to encourage Indo-Pacific countries to sign on to the framework by emphasizing the benefits of cultivating open digital ecosystems for economic growth, job creation, innovation, and capacity building.
- *Encourage private U.S. investments in Indo-Pacific technology companies.* The Commerce Department, working in conjunction with relevant interagency partners, should facilitate U.S. and allied investments in Indo-Pacific technology firms to provide an alternative to Chinese capital, and to blunt the power that Beijing exercises through its investments in the region's digital economy.
- *Assist other countries in implementing effective investment screening programs.* The Treasury Department's Office of International Affairs should establish a technical assistance program to share expertise and provide capacity-building support for partner countries that want to create new investment screening processes or improve existing ones along lines of the Committee on Foreign Investment in the United States.

Shield democracy from digital threats while advancing internet freedom.

- *With countries across the Indo-Pacific, enhance diplomatic engagements and assistance programs that deepen understanding of the need to balance rule of law and prevention of violence with protecting civil rights to free and peaceful speech.* The State Department and USAID should highlight these issues in their diplomatic engagements and foreign assistance programs. The conversation must involve private sector companies and civil society groups from the United States as well as the Indo-Pacific region. While laws and regulations will continue to vary across nations, the United States can lead an international conversation that begins to illuminate a framework for considering these issues.
- *Build local resilience and capabilities of civil society, watchdog groups, and journalists to monitor digital development.* The State Department and USAID should support and educate journalists and local civil society groups to play a watchdog role over technology development. These organizations will help to ensure that technology ecosystems are developed in a way that protects civil rights and benefits local communities. The State Department Bureau of Economic and Cultural Affairs and Global Engagement Center could also develop a plan for engagement in the Indo-Pacific region to highlight the path toward building a free, open, and inclusive digital future. And USAID could play a role in educating local governments, nongovernmental organizations, and the development community about the importance for sustainable economic development of nurturing an open and inclusive digital ecosystem.
- *Encourage U.S. technology companies to also engage with local civil society leaders, academics, and journalists to better understand and learn to identify disinformation.* The State Department should work with the local affiliates of technology companies to organize roundtable discussions about preventing abuse of social media platforms.
- *Draw from other countries' experience in combating disinformation.* In addition, the experiences of Taiwan, Australia, and others in countering disinformation's effects on democracy must be leveraged. Those efforts should be embedded into a larger internet freedom agenda.

Define and implement a digital governance model that reflects liberal values and can keep up with technological innovation.[117]

- *Lead a multinational effort to establish digital governance guidelines.* The NSC should spearhead a policy process to develop a whole-of-government strategy that can serve as a framework for international discussions on the topic. Many allies and partners in the Indo-Pacific and across the rest of the world have digital strategies. Coordinating efforts—particularly in Southeast Asia—will be a potent force multiplier. The strategy should identify ways to modernize regulation of the technology industry so that issues such as surveillance, data privacy, and impact on the media industry are handled in ways that support a liberal political and social model, in direct contrast with China's digital authoritarianism. The digital governance framework should also include a set of guiding principles for the use of social media and digital communications to help prevent unnecessary restrictions that harm civil rights to free and peaceful speech.

- *Support technology innovation domestically and in contested spaces.* The U.S. government should invest in developing technology alternatives that are based on privacy and other democratic digital governance norms. Once a problematic technology is identified on the international market, organizations including the Defense Advanced Research Projects Agency, In-Q-Tel, or the Intelligence Advanced Research Projects Activity can work to develop these alternatives. In addition, the State Department Bureau of Global Public Affairs should support technology hackathons throughout Southeast Asia to encourage and facilitate the growth of responsible technology innovation in the region.
- *Ensure adequate funding and resources for U.S. agencies supporting digital development in Indo-Pacific countries.* Several different U.S. government agencies, including the U.S. Agency for International Development, U.S. International Development Finance Corporation, Millennium Challenge Corporation, and U.S. Trade and Development Agency, have a role in supporting liberal digital governance as well as in developing digital ecosystems that support innovation, build trusted networks, and protect individual data.
- *Use digital technology to empower the traditionally disempowered.* Through private-public partnerships between organizations such as the State Department Bureau of Democracy, Human Rights, and Labor and the U.S. Open Technology Fund, the United States should work to distribute tools—for example, virtual private networks—that support the free flow of information to people in constrained information environments.

Conclusion

The United States is in a multifaceted competition with China that spans the economic, diplomatic, and military domains. The competition to influence global digital ecosystems, particularly in the Indo-Pacific, is consequential to defining the extent to which liberal or authoritarian governance models will prevail in the region, perhaps for decades to come. In order to meet the global digital development challenges posed by Chinese advancements in the technological and standard-setting arenas, the United States must work closely with like-minded partners and allies. This cooperation is necessary to pool capabilities and resources and also to bring to bear shared democratic values that must guide digital development. The pace of digital innovation and the rapid increase of reliance on digital systems worldwide—spurred by the global pandemic—makes U.S. attention to this critical national security issue all the more urgent.

1. Peter Cowhey and the Working Group on Science and Technology in U.S.-China Relations, “Meeting the China Challenge: A New American Strategy for Technology Competition” (Asia Society Center on U.S.-China Relations and the UC San Diego 21st Century China Center, November 2020), 35, https://asiasociety.org/sites/default/files/inline-files/report_meeting-the-china-challenge_2020.pdf.

2. Martijn Rasser and Ainikki Riikonen, “Open Future: The Way Forward on 5G” (Center for a New American Security, July 2020), https://www.cnas.org/publications/reports/open-future.

3. Paul Scharre and Lisa Curtis, “Shaping a Techno-Democratic Future” (Australia National University National Security College Futures Hub, March 2021), https://futureshub.anu.edu.au/shaping-a-techno-democratic-future/.

4. Cowhey et al., “Meeting the China Challenge,” 35.

5. Valentina Pop, Sha Hua, and Daniel Michaels, “From Lightbulbs to 5G, China Battles West for Control of Vital Technology Standards,” The Wall Street Journal, February 8, 2021, https://www.wsj.com/articles/from-lightbulbs-to-5g-china-battles-west-for-control-of-vital-technology-standards-11612722698.

6. Cowhey et al., “Meeting the China Challenge,” 35.

7. Thomas Ricker, “The U.S., Like China, Has about One Surveillance Camera for Every Four People, Says Report,” The Verge, December 9, 2019, https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens.

8. Holly Chik, “China Is Home to 18 of the 20 Most Surveilled Cities in the World,” Inkstone, July 27, 2020, https://www.inkstonenews.com/society/china-home-18-20-most-surveilled-cities-world/article/3094805; Paul Bischoff, “Surveillance Camera Statistics: Which City Has the Most CCTV Cameras?” Comparitech, July 22, 2020, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

9. Mara Hvistendahl, “How a Chinese AI Giant Made Chatting—And Surveillance—Easy,” Wired, May 18, 2020, https://www.wired.com/story/iflytek-china-ai-giant-voice-chatting-surveillance/; Danielle Cave et al., “Mapping China’s Tech Giants” (Australian Strategic Policy Institute, April 2019), https://www.aspi.org.au/report/mapping-chinas-tech-giants.

10. Joshua Fitt, “Stemming the Flow: The United States Needs a Strategy to Address China’s Strategic Exportation of Digital Authoritarianism,” Georgetown Journal of International Affairs, February 25, 2021, https://gjia.georgetown.edu/2021/02/25/stemming-the-flow-the-united-states-needs-a-strategy-to-address-chinas-strategic-exportation-of-digital-authoritarianism/.

11. Paul Bischoff, “Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?” Comparitech, July 22, 2020, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

12. Cave et al., “Mapping China’s Tech Giants.”

13. Jeffrey Ding, “Deciphering China’s AI Dream” (Future of Humanity Institute, University of Oxford, March 2018), https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.

14. J. C. Ong and Ross Tapsell, “Mitigating Disinformation in Southeast Asian Elections: Lessons from Indonesia, Philippines and Thailand” (NATO StratCom Centre of Excellence, May 2020), https://www.stratcomcoe.org/mitigating-disinformation-southeast-asian-elections; Coby Goldberg and Kristine Lee, “Retooling Democratic Good Governance” (Center for a New American Security, December 2020), https://www.cnas.org/publications/commentary/retooling-democratic-good-governance.

15. Dien Luong, “Vietnam’s Internet Is in Trouble,” The Washington Post, February 19, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/02/19/vietnam-internet/; Arindrajit Basu, “The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam,” The Diplomat, January 10, 2020, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/; Jeff Olson and Mai Phuong Nguyen, “Vietnam Quick to Enforce New Cybersecurity Law,” Engage, March 6, 2019, https://www.engage.hoganlovells.com/knowledgeservices/news/vietnam-quick-to-enforce-new-cybersecurity-law.

16. Duckju Kang, “Battle of Social Networks in Asia: Who Is Winning?” ValueChampion, August 31, 2016, https://www.valuechampion.sg/battle-social-networks-asia-who-winning; “Weixìn 2000 wan malaixiya yonghu laizì nali? [Where do Wechat’s 20 million Malaysian users come from?], Hexun Minjia, November 23, 2017, http://news.hexun.com/2017-11-23/191747567.html.

17. Vincenzo Cosenza, “World Map of Social Networks,” January 2021, Vincos Blog, https://vincos.it/world-map-of-social-networks/.

18. Helen Davidson and Carmela Fonbuena, “Facebook Removes Fake Accounts with Links to China and Philippines,” The Guardian, September 23, 2020, https://www.theguardian.com/technology/2020/sep/23/facebook-removes-fake-accounts-with-links-to-china-and-philippines.

19. “Data: Top Ten Most Downloaded Apps in Six Emerging Markets,” Macro Polo, August 2020, https://macropolo.org/the-chinese-and-us-apps-winning-the-next-billion-users/; Similarweb, Mobile App Ranking: Top App Store Apps in Philippines, https://www.similarweb.com/apps/top/apple/store-rank/ph/all/top-free/iphone/.

20. Chen Dazhi, “ai qi yi chuhai yi nian: yinru nai fei BBC gao guan, weilai jihua jinjun ri han he zhongdong gao guan [iQIYI one year overseas: Netflix, BBC, and plans to enter Japan, South Korea, and the Middle East in the future],” 36kr, July 29, 2020, https://36kr.com/p/815868611120513.

21. Zacks Equity Research, “iQIYI’s Overseas Expansion to Stir Up Streaming Competition,” Nasdaq, January 7, 2020, https://www.nasdaq.com/articles/iqiyis-overseas-expansion-to-stir-up-streaming-competition-2020-01-07; Dazhi, “[iQIYI one year overseas].”

22. “Tengxun shipin haiwai ban guan xuan, jinjun dongnanya wu guo shichang” [Tencent Video’s official announcement of its overseas version entering the market of five Southeast Asian countries], 36kr, March 5, 2020, https://www.36kr.com/p/1725212590081.

23. Robert Greene and Paul Triolo, “Will China Control the Global Internet via Its Digital Silk Road?” Carnegie Endowment for International Peace, May 8, 2020, https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857; Wade Shepard, “Inside the Belt and Road’s Premier White Elephant: Melaka Gateway,” Forbes, January 31, 2020, https://www.forbes.com/sites/wadeshepard/2020/01/31/inside-the-belt-and-roads-premier-white-elephant-melaka-gateway/; “China-Led $280 Million Kyrgyzstan Project Abandoned after Protests,” Reuters, February 18, 2020, https://www.reuters.com/article/us-kyrgyzstan-china-investment-protests/china-led-280-million-kyrgyzstan-project-abandoned-after-protests-idUSKBN20C1HA; Shihar Aneez, “China’s ‘Silk Road’ Push Stirs Resentment and Protest in Sri Lanka,” Reuters, February 1, 2017, https://www.reuters.com/article/us-sri-lanka-china-insight-idUSKBN15G5UT.

24. Jude Blanchette and Jonathan Hillman, “China’s Digital Silk Road after the Coronavirus,” On the Horizon, Center for Strategic & International Studies, commentary, April 13, 2020, https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus.

25. Kristine Lee et al., “Digital Entanglement: Lessons Learned from China’s Growing Digital Footprint in South Korea” (Center for a New American Security, October 2020), https://www.cnas.org/publications/reports/digital-entanglement.

26. Kristine Lee and Alex Sullivan, “People’s Republic of the United Nations: China’s Emerging Revisionism in International Organizations” (Center for a New American Security, May 2019), https://www.cnas.org/publications/reports/peoples-republic-of-the-united-nations.

27. Houlin Zhao, “China’s One Belt, One Road Can Improve Lives at Scale through ICT Investment,” ITUNews, May 16, 2017, https://news.itu.int/chinas-one-belt-one-road-can-improve-lives-at-scale-through-ict-investment/.

28. Kristine Lee, “Coming Soon to the United Nations: Chinese Leadership and Authoritarian Values,” Foreign Affairs, September 16, 2019, https://www.foreignaffairs.com/articles/china/2019-09-16/coming-soon-united-nations-chinese-leadership-and-authoritarian-values.

29. Joshua Kurlantzick, “China’s Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom?” The Diplomat, December 17, 2020, https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/.

30. Andrew Kitson and Kenny Liew, “China Doubles Down on Its Digital Silk Road,” Reconnecting Asia, Center for Strategic & International Studies, analysis, November 14, 2019, https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/.

31. Kristine Lee and Martijn Rasser, “China’s Health Silk Road Is a Dead-End Street,” Foreign Policy, June 16, 2020, https://foreignpolicy.com/2020/06/16/china-health-propaganda-covid/.

32. Lee and Rasser, “China’s Health Silk Road Is a Dead-End Street.”

33. Blanchette and Hillman, “China’s Digital Silk Road after the Coronavirus.”

34. Trisha Ray et al., “The Digital Indo-Pacific: Regional Connectivity and Resilience” (Observer Research Foundation, February 2021), https://www.orfonline.org/research/the-digital-indo-pacific-regional-connectivity-and-resilience/.

35. Chad Brown, “The U.S. Is Trying to Use Export Controls to Restrict Huawei’s Access to Semiconductors,” Peterson Institute for International Economics, October 13, 2020, https://www.piie.com/research/piie-charts/us-trying-use-export-controls-restrict-huaweis-access-semiconductors.

36. Ajit Pai, “Remarks by FCC Chairman Ajit Pai to the Prague 5G Security Conference,” September 24, 2020, Prague 5G Security Conference, Prague, Czechia, https://docs.fcc.gov/public/attachments/DOC-367117A1.pdf.

37. “Prague 5G Security Conference 2019,” Czech National Cyber and Information Security Agency, May 3, 2019, https://nukib.cz/en/infoservis-en/conferences/prague-5g-security-conference-2019/#:~:text=An%20international%20expert%20conference%20on,of%20Prime%20Minister%20Andrej%20Babi%C5%A1.

38. Mike Dano, “Prague 5G Security Debates Center on China, Open RAN,” LightReading, September 25, 2020, https://www.lightreading.com/security/prague-5g-security-debates-center-on-china-open-ran/d/d-id/764222.

39. “The Clean Network,” U.S. Department of State (2017–21 archived content), August 5, 2020, https://2017-2021.state.gov/the-clean-network/index.html.

40. Nick Wadhams and Jenny Leonard, “Biden Builds Out China Team with Staff Who Reflect Tougher Tone,” Bloomberg Quint, February 18, 2021, https://www.bloombergquint.com/global-economics/biden-builds-out-china-team-with-staff-who-reflect-tougher-tone.

41. “Telecoms Diversification Task Force: Findings and Report,” UK Department for Digital, Culture, Sports & Media, April 20, 2021, https://www.gov.uk/government/publications/telecoms-diversification-taskforce-findings-and-report/telecoms-diversification-taskforce-findings-and-report.

42. Scharre and Curtis, “Shaping a Techno-Democratic Future.”

43. Nadia Schadlow and Brayden Helwig, “Protecting Undersea Cables Must Be Made a National Security Priority,” DefenseNews, July 1, 2020, https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/.

44. Schadlow and Helwig, “Protecting Undersea Cables.”

45. Schadlow and Helwig, “Protecting Undersea Cables.”

46. Jonathan Barrett, “Exclusive: U.S. Warns Pacific Islands about Chinese Bid for Undersea Cable Project—Sources,” Reuters, December 17, 2020, https://www.reuters.com/article/us-china-pacific-exclusive-idUSKBN28R0L2; Winston Qiu, “Global Marine Group Fully Divests Stake in Huawei Marine Networks,” Submarine Networks, June 6, 2020, https://www.submarinenetworks.com/en/vendors/huawei-marine/global-marine-completes-sale-of-30-stake-in-huawei-marine-networks-for-85-million.

47. “Solomon Islands Drops Chinese Tech Giant Huawei for Billion-Dollar Undersea Cable, Signs Australia,” South China Morning Post, June 13, 2018, https://www.scmp.com/news/asia/diplomacy/article/2150616/solomon-islands-drops-chinese-tech-giant-huawei-billion-dollar.

48. Chris Horton and Austin Ramzy, “Asia’s Bastion of Free Speech? Move Aside, Hong Kong, It’s Taiwan Now,” The New York Times, April 14, 2018, https://www.nytimes.com/2018/04/14/world/asia/china-taiwan-hong-kong-free-speech.html.

49. Steven Butler, “One Country, One Censor: How China Undermines Media Freedom in Hong Kong and Taiwan,” Committee to Protect Journalists, December 16, 2019, https://cpj.org/reports/2019/12/one-country-one-censor-china-hong-kong-taiwan-press-freedom/#taiwan.

50. “Democracy Facing Global Challenges: V-Dem Annual Democracy Report 2019” (V-Dem Institute, May 2019), 36, https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf.

51. “Democracy Facing Global Challenges,” 36.

52. Emily Feng, “Taiwan Gets Tough on Disinformation Suspected from China ahead of Elections,” National Public Radio, December 6, 2019, https://www.npr.org/2019/12/06/784191852/taiwan-gets-tough-on-disinformation-suspected-from-china-ahead-of-elections; Andrew Leonard, “How Taiwan’s Unlikely Digital Minister Hacked the Pandemic,” Wired, July 23, 2020, https://www.wired.com/story/how-taiwans-unlikely-digital-minister-hacked-the-pandemic/.

53. Butler, “One Country, One Censor.”

54. Feng, “Taiwan Gets Tough on Disinformation.”

55. “Taiwan Reinforces Ban on Huawei Network Equipment,” AP News, December 10, 2018, https://apnews.com/article/138ce8db78224ee9ac4f3efb33ab5bec.

56. Duncan DeAeth, “Taiwan Prepares Expanded Blacklist of Chinese Telecom Products,” Taiwan News, July 18, 2019, https://www.taiwannews.com.tw/en/news/3747220.

57. “Zoom Banned by Taiwan’s Government over China Security Fears,” BBC News, April 7, 2020, https://www.bbc.com/news/technology-52200507.

58. Sherisse Pham, “Taiwan Announces Ban on Chinese Streaming Services Tencent and iQIYI,” CNN Business, August 19, 2020, https://www.cnn.com/2020/08/19/tech/iqiyi-tencent-taiwan-china-tech-ban-hnk-intl/index.html.

59. “American Institute in Taiwan and the Taipei Economic and Cultural Representative Office Joint Declaration on 5G Security,” American Institute in Taiwan, press release, August 26, 2020, https://www.ait.org.tw/ait-tecro-joint-declaration-5g-security/?_ga=2.209567826.1380703427.1617625202-1754139913.1617625202; “Remarks by AIT Director W. Brent Christensen at the Announcement of the AIT-TECRO Joint Declaration on 5G Security,” American Institute in Taiwan, press release, August 26, 2020, https://www.ait.org.tw/remarks-by-ait-director-christensen-ait-tecro-declaration-5g-security/?_ga=2.254815432.1380703427.1617625202-1754139913.1617625202.

60. “Secretary Blinken’s Call with Quad Ministers,” U.S. Department of State, press release, February 18, 2021, https://www.state.gov/secretary-blinkens-call-with-quad-ministers/; Andrew Tillett, “Supply Chains, Disinformation on Quad Agenda,” Australian Financial Review, October 2, 2020, https://www.afr.com/politics/federal/supply-chains-disinformation-on-quad-agenda-20201002-p561c3.

61. James Purtill, “Facebook, Google, Twitter Release Industry Code to Fight Spread of Disinformation,” ABC Science Australia, February 22, 2021, https://www.abc.net.au/news/science/2021-02-22/facebook-google-release-voluntary-industry-code-disinformation/13178488.

62. "Japan to Ask GAFA to Join Team to Fight Fake News," Nippon.com, November 29, 2019, https://www.nippon.com/en/news/yjj2019112901178/japan-to-ask-gafa-to-join-team-to-fight-fake-news.html.

63. Alan Burkitt-Gray, "India-Chinese Fighting Means Huawei and ZTE Blocked from Indian 4G Tenders," Capacity Media, July 3, 2020, https://www.capacitymedia.com/articles/3825871/india-chinese-fighting-means-huawei-and-zte-blocked-from-indian-4g-tenders.

64. Liza Lin and Newley Purnell, "India Ban Disrupts TikTok Users and China's Digital Ambitions," The Wall Street Journal, June 30, 2020, https://www.wsj.com/articles/india-ban-hurts-chinese-tech-in-worlds-biggest-untapped-market-11593522311.

65. Lin and Purnell, "India Ban Disrupts TikTok Users and China's Digital Ambitions."

66. David Fischer, "Facebook Invests $5.7 Billion in India's Jio Platforms," Facebook Newsroom, April 21, 2020, https://about.fb.com/news/2020/04/facebook-invests-in-jio/; Manish Singh, "Google to Invest $10 Billion in India," Techcrunch, July 13, 2020, https://techcrunch.com/2020/07/13/google-to-invest-10-billion-in-india/.

67. Ray et al., "The Digital Indo-Pacific."

68. Ray et al., "The Digital Indo-Pacific."

69. Priyanka Boghani and Stefen Joshua Rasay, "Alibaba, Tencent to Curtail Investment in India after Chinese Apps Ban—Experts," S&P Global Market Intelligence, July 24, 2020, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/alibaba-tencent-to-curtail-investment-in-india-after-chinese-apps-ban-8211-experts-59459027.

70. Sanchita Dash, "Amid India-China Standoff, Tencent Is Back with an Investment in Flipkart," Business Insider India, September 16, 2020, https://www.businessinsider.in/business/startups/news/amid-india-china-standoff-tencent-is-back-with-an-investment-in-flipkart/articleshow/78140794.cms.

71. Number of Internet Users in India from 2015 to 2020 with a Forecast Until 2025," Statista, October 16, 2020, https://www.statista.com/statistics/255146/number-of-internet-users-in-india/; "Number of Internet Users in Indonesia from 2015 to 2025," Statista, August 13, 2020, https://www.statista.com/statistics/254456/number-of-internet-users-in-indonesia/; "Forecast of the number of internet users in Vietnam from 2010 to 2025," Statista, February 11, 2021, https://www.statista.com/forecasts/1147008/internet-users-in-Vietnam; and "Number of Internet Users in the Philippines as of January 2020, Statista, March 5, 2021, https://www.statista.com/statistics/221179/internet-users-philippines/.

72. Fischer, "Facebook Invests $5.7 Billion in India's Jio Platforms;" Singh, "Google to Invest $10 Billion in India."

73. Scharre and Curtis, "Shaping a Techno-Democratic Future."

74. Aftab Ahmed and Sankalp Phartiyal, "India Likely to Block China's Huawei over Security Fears: Officials," Reuters, March 11, 2021, https://www.reuters.com/article/us-india-china-huawei/india-likely-to-block-chinas-huawei-over-security-fears-officials-idUSKBN2B31PU.

75. Yohei Hirose and Akihiro Ota, "Japan to Help India with 5G to Counter China's Growing Influence," Nikkei Asia, November 29, 2020, https://asia.nikkei.com/Business/Technology/Japan-to-help-India-with-5G-to-counter-China-s-growing-influence2.

76. Hirose and Ota, "Japan to Help India with 5G."

77. Hirose and Ota, "Japan to Help India with 5G."

78. Hirose and Ota, "Japan to Help India with 5G."

79. Lee et al., "Digital Entanglement."

80. Lee et al., "Digital Entanglement."

81. Troy Stangarone, "South Korea's Digital New Deal," The Diplomat, June 25, 2020, https://thediplomat.com/2020/06/south-koreas-digital-new-deal/.

82. Stangarone, "South Korea's Digital New Deal."

83. Stangarone, "South Korea's Digital New Deal."

84. Dashveenjit Kaur, "Vietnam Is ahead of the Game with Commercial 5G," Techwire Asia, December 1, 2020, https://techwireasia.com/2020/12/vietnam-is-ahead-of-the-game-with-commercial-5g/.

85. Raymond Zhong, "Is Huawei a Security Threat? Vietnam Isn't Taking Any Chances," The New York Times, July 18, 2019, https://www.nytimes.com/2019/07/18/technology/huawei-ban-vietnam.html.

86. Joe Devanesan, "How Singapore Has Become a Safe Harbour for Tech Giants," Techwire Asia, September 21, 2020, https://techwireasia.com/2020/09/singapore-is-becoming-a-safe-harbour-for-tech-giants/.

87. Justin Harper, "Singapore Becomes Hub for Chinese Tech amid U.S. Tensions," BBC News, September 16, 2020, https://www.bbc.com/news/business-54172703.

88. "Singapore Telcos Pick Nokia, Ericsson over Huawei to Build Main 5G Networks," Reuters, June 24, 2020, https://www.reuters.com/article/us-singapore-telecoms-5g/singapore-telcos-pick-nokia-ericsson-over-huawei-to-build-main-5g-networks-idUSKBN23V1PG.

89. Muhammad Zulfikar Rakhmat and Yeta Purnama, "For Indonesia, Chinese 5G Cooperation Brings Promise and Peril," The Diplomat, January 20, 2021, https://thediplomat.com/2021/01/for-indonesia-chinese-5g-cooperation-brings-promise-and-peril/.

90. "Wang Yi Meets with Indonesia's Coordinator for Cooperation with China and Coordinating Minister Luhut Binsar Pandjaitan," Ministry of Foreign Affairs of the People's Republic of China, press release, January 13, 2021, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1846201.shtml.

91. "China, Indonesia Sign MoU on Internet Security amid Washington pressure on Beijing's 5G technology," Global Times, January 13, 2021, https://www.globaltimes.cn/page/202101/1212657.shtml.

92. Resty Woro Yuniar, "Is Indonesia Becoming too Reliant on Huawei?" South China Morning Post, December 4, 2020, https://www.scmp.com/week-asia/economics/article/3112634/indonesia-becoming-too-reliant-huawei.

93. Niharika Mandhana, "In Global Tech Battle, a Balky U.S. Ally Chooses China," The Wall Street Journal, July 15, 2019, https://www.wsj.com/articles/in-global-tech-battle-the-philippines-has-chosen-sides-not-the-u-s-11563205891?st=70ltk0qsd7oiv7f.

94. Adib Povera and Ayisy Yusof, "PM Launches MyDigital, Malaysia's Digital Economy Blueprint," New Straits Times, February 18, 2021, https://www.nst.com.my/news/nation/2021/02/666982/pm-launches-mydigital-malaysias-digital-economy-blueprint.

95. Joe Devanesan, "New AI Park Could Add Tech Muscle to Malaysia," Techwire Asia, October 27, 2020, https://techwireasia.com/2020/10/new-ai-park-could-add-tech-muscle-to-malaysia/.

96. Preetam Kaushik, "The New Frontier: Malaysia Is WeChat's Stepping Stone to Southeast Asian Markets," ASEAN Today, April 6, 2019, https://www.aseantoday.com/2019/04/the-new-frontier-malaysia-is-wechats-stepping-stone-to-southeast-asian-markets/.

97. Isobel Asher Hamilton, "WeChat Users in the U.S. Say the App Is Censoring Their Messages about Hong Kong," Business Insider, November 26, 2019, https://www.businessinsider.com/us-wechat-users-censored-messages-hong-kong-china-2019-11.

98. Emmy Sasipornkarn, "Asia's 'Milk Tea' Activists Give Cross-Border Support for Democratic Change," DW News, March 8, 2021, https://www.dw.com/en/asias-milk-tea-activists-give-cross-border-support-for-democratic-change/a-56806229.

99. "What Is the Milk Tea Alliance?" The Economist, March 24, 2021, https://www.economist.com/the-economist-explains/2021/03/24/what-is-the-milk-tea-alliance.

100. Timothy Mclaughlin, "How Milk Tea Became an Anti-China Symbol," The Atlantic, October 13, 2020, https://www.theatlantic.com/international/archive/2020/10/milk-tea-alliance-anti-china/616658/.

101. Goldberg and Lee, "Retooling Democratic Good Governance."

102. Vincent Bevins, "Indonesian Police Arrest 14 Suspected Members of Radical Islamist Cyber Network," The Washington Post, March 1, 2018, https://www.washingtonpost.com/world/asia_pacific/indonesia-police-break-up-islamist-cyber-network-promoting-extremism/2018/03/01/ff575b00-1cd8-11e8-98f5-ceecfa8741b6_story.html.

103. Paul Mozur, "A Genocide Incited on Facebook, with Posts from Myanmar's Military," The New York Times, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

104. Goldberg and Lee, "Retooling Democratic Good Governance."

105. Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar," Facebook Newsroom, November 5, 2018, https://about.fb.com/news/2018/11/myanmar-hria/.

106. Fanny Potkin, "Facebook Faces a Reckoning in Myanmar after Blocked by Military," Reuters, February 4, 2021, https://www.reuters.com/article/us-myanmar-politics-facebook-focus/facebook-faces-a-reckoning-in-myanmar-after-blocked-by-military-idUSKBN2A42RY.

107. Potkin, "Facebook Faces a Reckoning."

108. Potkin, "Facebook Faces a Reckoning."

109. Victoria Milko, "Why Is Facebook Banning Myanmar Military Pages?" Explaining the News, AP News, February 25, 2021, https://apnews.com/article/why-facebook-ban-myanmar-military-15f4c26c442c0d8af110594a5bb72c45.

110. Rafael Frankel, "An Update on the Situation in Myanmar," Facebook Newsroom, April 14, 2021, https://about.fb.com/news/2021/02/an-update-on-myanmar/.

111. "Over 100 Instances of Internet Shutdown in India in 2020, Says New Report," The Wire, March 4, 2021, https://thewire.in/tech/over-100-instances-of-internet-shutdown-in-india-in-2020-says-new-report.

112. Anja Manuel, "U.S., Europe and UK Must Unite to Keep Chinese Tech at Bay," Financial Times, October 5, 2020, https://www.ft.com/content/bc7abf86-f13e-4025-a120-004361aef21a.

113. Council of the European Union, Outcome Proceedings: EU Strategy for Cooperation in the Indo-Pacific, 7914/21 (April 16, 2021), https://data.consilium.europa.eu/doc/document/ST-7914-2021-INIT/en/pdf.

114. Kristen Cordell and Kristine Lee, "Harnessing Multilateralism for Digital Development" (Center for a New American Security, January 2021), https://www.cnas.org/publications/commentary/harnessing-multilateralism-for-digital-development.

115. Rasser and Riikonen, "Open Future: The Way Forward on 5G.".

116. Dano, "Prague 5G Security Debates Center on China."

117. Goldberg and Lee, "Retooling Democratic Good Governance."

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.

As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, CNAS maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

Center for a
New American
Security