GLOBAL CHINA
ASSESSING CHINA'S GROWING ROLE IN THE WORLD

DEALING WITH DEMAND FOR CHINA'S GLOBAL SURVEILLANCE EXPORTS

SHEENA CHESTNUT GREITENS

APRIL 2020

EXECUTIVE SUMMARY

Countries and cities worldwide now employ public security and surveillance technology platforms from the People's Republic of China (PRC). The drivers of this trend are complex, stemming from expansion of China's geopolitical interests, increasing market power of its technology companies, and conditions in recipient states that make Chinese technology an attractive choice despite security and privacy concerns. Both "push" and "pull" factors contribute to growing use of Chinese surveillance technology: countries that are strategically important to the PRC are comparatively more likely to adopt it, but so are countries with high crime rates.

Major questions remain about the implications and advantages that China could derive from these developments, including how dominance in this sector and access to data could shape the contours of strategic competition between China and the United States. Questions also remain about what impact these technologies will have on data privacy/security, human rights, and democracy. There is relatively little correlation between the level of democracy in a country and the likelihood that it will adopt Chinese surveillance technology, but we do not yet know whether introduction of that technology will somehow subsequently corrode democratic institutions or civil liberties. While leaders in adopting countries share some concerns about data security, civil liberties, and democracy, many of them also focus on these platforms' potential to solve urgent public problems, such as violent crime. Understanding the impacts of these technologies will be important for crafting effective policy.

This evidence also suggests that a one-size-fits-all message from U.S. policymakers about the risks of Chinese technology needs to be differentiated and adapted to each country in which such concerns are raised. These messages need to be paired with a nuanced understanding of the priorities and incentives of the officials making adoption decisions — often subnational officials rather than foreign policy or national security experts. Finally, the U.S. must address Chinese technology companies' ongoing efforts to shape the global regulatory environment; to do so, policymakers will need to articulate and execute a comprehensive strategy to promulgate standards compatible with American values and interests.

INTRODUCTION

Countries and cities around the world have increasingly opted to employ public security and surveillance technology platforms from China. The drivers of this trend are complex, stemming from the expansion of China's geopolitical interests, the increasing market power of its technology companies, and conditions in recipient states that make Chinese technology an attractive choice despite concerns about security and privacy. The global adoption of these platforms therefore raises thorny policy questions for the United States and the international community: how to best shape debates over global norms and standards on data security and privacy; how to address the role of technology in U.S.-China strategic competition; and how to manage risks of authoritarian backsliding and human rights infringement. How should American and international policymakers respond to these challenges?

News articles and policy analyses warn of the dangers of high-tech surveillance and artificial intelligence (AI) approaches to policing in autocrats' hands;[1] document the rise of a "dystopian surveillance state" inside China itself, especially in Xinjiang;[2] and provide evidence of the use of Chinese surveillance technology in places like Venezuela, Ecuador, Zimbabwe, and Uganda.[3] At a May 2019 hearing of the House Permanent Select Committee on Intelligence on "China's Digital Authoritarianism," Chairman Rep. Adam Schiff (D-CA) noted, "Th[e] coupling of innovation and authoritarianism is deeply troubling and has spread beyond China itself... Export of this technology gives countries the technological tools they need to emulate Beijing's model of social and political control." Ranking Member Rep. Devin Nunes (R-CA) followed by warning about "Chinese adoption and exportation of invasive surveillance measures designed to optimize political control."[4]

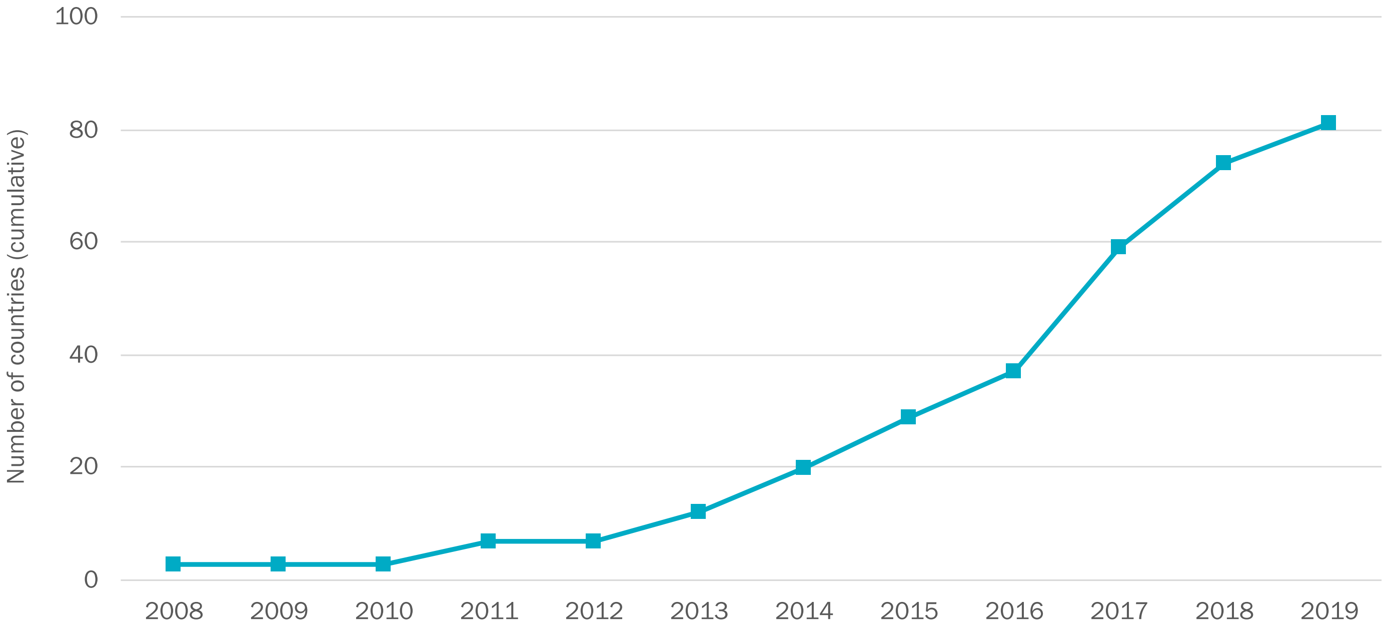
This paper examines the spread of surveillance and public security technology from China to the world. It begins by charting global patterns of technology adoption in the surveillance and policing sector, and then examines potential drivers of this expansion. The final section discusses possible implications of these findings for both American and international policy.

CHARTING THE ADOPTION OF CHINA'S SURVEILLANCE AND SECURITY PLATFORMS

Despite a high degree of concern about Chinese surveillance technology, current policy discourse in the U.S. and abroad may actually have underestimated the scope and speed of its spread. A Freedom House report discussed adoption of Chinese surveillance technology in 18 countries in 2018, an April 2019 Australian Strategic Policy Institute report by the covered 43 countries, and a fall 2019 Center for Strategic and International Studies report discussed 52 countries.[5] By contrast, Huawei's 2018 annual report noted that its "safe city solutions now serve over 700 cities across more than 100 countries and regions, including Brazil, Mexico, Serbia, Singapore, Spain, South Africa, and Turkey," triple the number reported in its 2015 report, and somewhere between two and five times the numbers reported in contemporaneous Western policy analyses.[6] Because Huawei and other Chinese tech companies have incentives to emphasize or exaggerate the popularity of their technology for marketing purposes, the true number of global adoptions likely falls somewhere between these two sets of estimates.

To increase empirical understanding of this phenomenon, this report's author led a research team that compiled a new dataset on the adoption of Chinese surveillance and public security technology platforms, using corporate, government, and media reporting in English, French, Spanish, and Chinese.[7] The dataset shows that Chinese surveillance and public security technology platforms have been adopted in at least 80 countries since 2008. The majority of these adoptions have occurred in the last several years (see Figure 1).

FIGURE 1: ADOPTION OF CHINESE SURVEILLANCE & PUBLIC SECURITY TECHNOLOGY PLATFORMS (2008-2019)



Source: Author's dataset

These estimates focus on surveillance technology platforms used specifically for policing and public security. In that sense, the measurement is different from some other think tank studies that discuss the broader use of AI or surveillance technology by China and other countries: the term "platform" indicates a higher threshold for coding adoption than, for example, a city simply having purchased closed-circuit television (CCTV) cameras manufactured by Hikvision.[8] The projects centered on the kinds of platforms indicated above are commonly referred to as "Safe City" (安全城市) projects — the term used by these platforms' largest global supplier, Huawei — which involve a data integration and analytics platform that supports one or more high-tech command-and-control centers. The platform collects, integrates, and analyzes data from a wide range of sources, such as criminal records, other government databases, networked surveillance cameras, facial and license plate recognition applications, and other sources. Huawei, for example, describes its Safe City Solutions as providing:

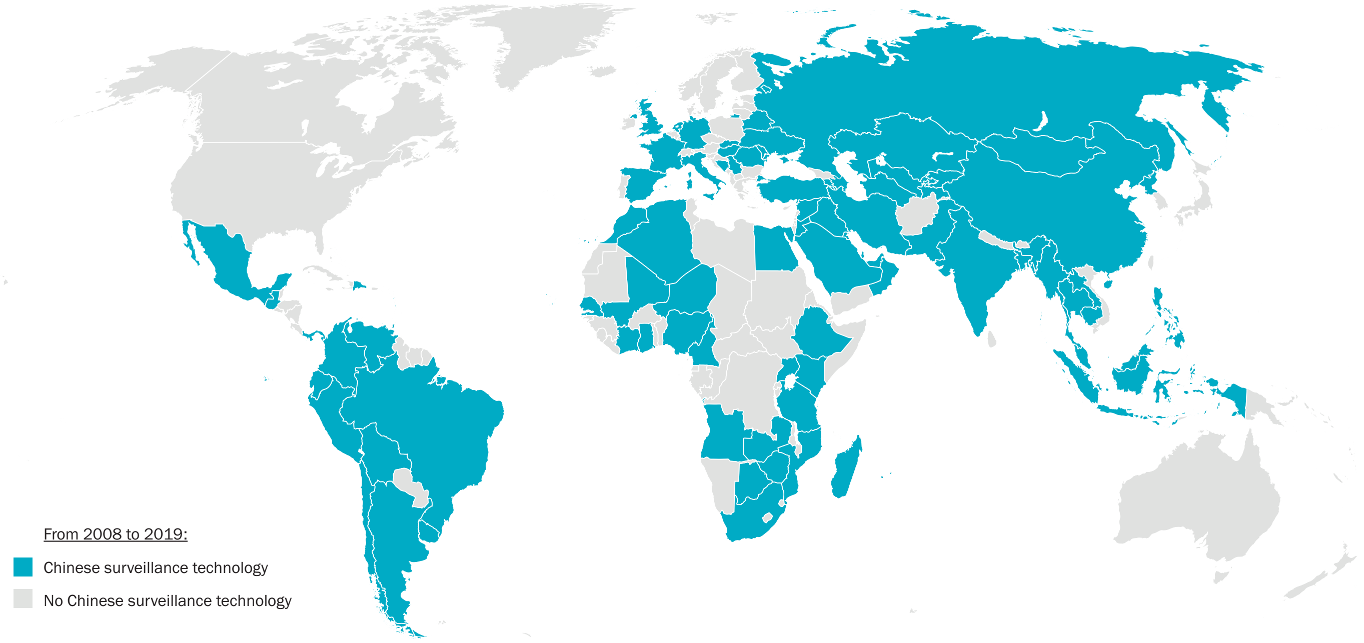
> "[W]orld-leading Collaborative-C4ISR [Command, Control, Communication, Cloud, Intelligence, Surveillance, and Reconnaissance] solutions that enable crucial visualization and convergence to maximize public safety... The safe city solutions jointly developed by Huawei and our partners enable advance prevention, precise resource allocation, efficient analysis, visualized command, and efficient coordination among multiple departments. They help governments reduce crime rates and prevent and respond to crises more effectively, ensuring a safer environment for all."[9]

Such projects are often multilayered, meaning that one company will provide the core platform, while additional companies may be involved in other aspects, extensions, or subcomponents of the project. Systematic, fine-grained data on which companies provide which layers of a particular city-project's tech stack is not yet available; in many cases, there are multiple Chinese tech companies involved, but there are also anecdotal reports of cases where cities incorporate both Chinese and Western technology into different layers of the tech stack. Project contracts sometimes include technical consulting in addition to sales of platforms themselves.

In addition to Huawei, Chinese companies such as Hikvision, ZTE, Dahua, China National Electronics Import and Export Corporation (CEIEC), and others are often involved. The identity of some of the companies involved in the export of surveillance technologies is one factor that has raised concerns in the U.S. national security and foreign policy community. At least some of the companies are directly linked to the People's Republic of China's (PRC) defense-industrial complex. CEIEC, for example, has contributed significantly to public security technology projects in several countries in Latin America; it is a state-owned enterprise under China Electronics Corporation that concentrates on defense electronics, and was previously sanctioned by the U.S. for nonproliferation violations.[10] Others, such as Hikvision and Dahua, have been implicated in and sanctioned for human rights violations — as the filing termed it, "the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance" — in Xinjiang.[11]

Chinese surveillance and public security technology platforms have been adopted in countries across the globe, as illustrated by Figure 2:

FIGURE 2: PRESENCE OF CHINESE SURVEILLANCE & PUBLIC SECURITY TECHNOLOGY PLATFORMS (2008-2019)[12]


From 2008 to 2019:
🟦 Chinese surveillance technology
⬜ No Chinese surveillance technology

Source: Author's dataset

DRIVERS OF CHINA'S GLOBAL EXPORTS: PUSH AND PULL FACTORS

What is driving the increased global adoption of Chinese surveillance and public security technologies? Critics in the United States and elsewhere tend to see Chinese geopolitical strategy and authoritarian instincts at work: a supply-side or "push factor" explanation.[13] As one recent report phrased it, "China is a major driver of AI surveillance worldwide."[14] The report notes that over half of the countries in which it found Chinese-sourced AI technology were signatories to President Xi Jinping's flagship geopolitical project, the Belt and Road Initiative (BRI), and suggests that Chinese government loans may be used to subsidize countries' acquisition of repressive technologies.[15] Another report notes that Beijing views information technology not just in terms of economic development but "its value to Chinese foreign policy and strategy… exporting its information technology is not only about securing important new sources of revenue and data, but also generating greater strategic leverage vis-à-vis the West."[16] In this view, the global adoption of these platforms is China-driven, as Beijing pushes their use for its own geopolitical strategic objectives.

Statements by Chinese tech companies and Chinese technology adopters, however (often regional or municipal officials in recipient countries), commonly focus on the demand side or "pull" factors. This family of explanations tends to outline and focus on problems that this technology can address in recipient cities or countries. Huawei's marketing materials, for example, describe market drivers of Safe City technology as differing by country and/or region, emphasizing extremist threats in the Middle East, crime in Latin America, and data management and environmental sustainability in Europe.[17] Statements by officials whose jurisdictions have pursued Chinese public security and surveillance projects, such as Kenya, Ecuador, and Myanmar, have also typically emphasized the importance of crime control for public safety and attracting investment. [18] Thus, in this view, adoption of Chinese surveillance and public security technology is driven by demand factors in recipient countries that "pull" this technology from China to solve local governance challenges, in ways that may or may not intersect with Beijing's grand strategy or geopolitical priorities.

The ongoing debate over Huawei's Safe City projects in the Philippines illustrates how demand for crime-fighting governance solutions can intersect with both Chinese statecraft and domestic concerns about threats from Chinese technology. Huawei, which also has a major telecommunications presence in the Philippines via companies Smart and Globe, had previously begun a Safe City project in Bonifacio, a business and residential district in Metro Manila.[19] (IBM also has smart city projects in Makati, Cebu, and Davao, according to media reports.[20]) Huawei's role in Philippine surveillance and public safety significantly expanded, however, during Xi Jinping's state visit in November 2018. During Xi's visit, the two countries signed 29 agreements, one of which established a "Safe Philippines Project," in which the Philippines' Department of the Interior and Local Government (DILG) agreed to partner with Huawei and China International Telecommunication and Construction Corporation (CITCC) to construct a 12,000-camera surveillance system aimed at public safety and security. The deal set targets of a 15% crime reduction and 25% improvement in response time, and was financed primarily by a loan from China Eximbank (19.11 billion Philippine pesos, PHP, of the 20.31 billion PHP project, close to $400 million). They agreed to construct an integrated command, communications, and operations center (later referred to as an Intelligent Command, Control, and Communications Center, IC4) that will handle video monitoring, critical communication, and information management and analytics, linking the Philippine National Police, DILG, the national 911 system, and fire and prison agencies.

In the months after the announcement, Philippine legislators raised concerns about the deal. They cited concerns about data privacy and cybersecurity, based on reports about Huawei's corporate practices and requirements to provide data included in the PRC's 2017 National Intelligence Law, questioning whether these issues made the technology incompatible with Philippine cybersecurity regulations. In response, Interior Secretary Eduardo Año said that all data and project management would be handled by Filipinos. Construction is set to begin in early 2020, with a fully operational system by 2022.[21] In the case of the Philippines, recipient government interest in reducing crime and Chinese willingness to provide development funding for the project helped to move it toward reality, while concerns about the security and privacy of Chinese tech have created considerable debate and opposition within the Philippine legislature.

Contestation over such projects is not occurring only in the Indo-Pacific. In Malta, the government established a company called "Safe City Malta," which in turn engaged in a public-private partnership with Huawei (Huawei also has a 5G project in Malta). Citizens objected to the use of facial recognition, however, and U.S. officials expressed concern the Maltese press that the data "could end up back in Beijing… [and be] exploited for authoritarian purposes." The project's director subsequently stated that Huawei would not operate the equipment and would not have direct access even to provide technical support, adding that "data will be stored in Malta and will stay in Malta, governed by a security and data retention policy."[22] Similarly, Huawei's Safe City project in the Serbian capital of Belgrade has become a point of contention between the Serbian Ministry of Internal Affairs and civil society watchdogs, which have raised concerns about the compatibility of video surveillance with Serbian laws on data protection and privacy.[23]

> **"A tailored, country-specific approach to these issues is likely necessary, rather than applying one-size-fits-all rhetoric centered on American concerns about China.**

What these cases, and overall patterns of adoption data suggest, is that both China-centered push factors and recipient-centered demand factors matter. Countries with high crime rates are comparatively more likely to adopt these technologies — but so are countries that are strategically important to the PRC.[24] Moreover, the level of democracy or freedom in potential recipients of this technology is not particularly strongly correlated with platform adoption: Safe City-type projects have appeared in free or democratic countries like France and Germany, "partly free" or anocratic countries like Uganda and Pakistan, and unfree authoritarian states like Laos and Saudi Arabia.[25] Understanding the complexity of the factors shaping adoption — and the fact that these decisions are not solely driven by China or Chinese companies, but by recipient demand — suggests that a tailored, country-specific approach to these issues is likely necessary, rather than applying one-size-fits-all rhetoric centered on American concerns about China.

Important questions also remain unanswered, the most central of which is about these technologies' effects. Put simply: do they work? At present, rigorous empirical evidence on the effect of Chinese surveillance technology platforms outside China is thin to nonexistent. Corporate marketing materials tout technology-based success stories in reducing crime rates (as in Kenya and Ecuador), while critics point to cases where these tools have been used for politically motivated surveillance and repression (Uganda, Zambia, and also Ecuador). These effects, however, are not mutually exclusive: improved surveillance may enhance public safety in general while also contributing to targeted repression of political opposition or other marginalized groups.

Especially given that these technology platforms are now being employed by democracies and autocracies alike, the question *du jour* of whether China is "exporting digital authoritarianism" or "making the world safe for autocracy" is less a matter of divining Beijing's intent in providing the technology to others, and more an empirical question of the scale and direction of its impact in different political environments. These are vital questions for those who seek to protect democracy, whether in the United States or abroad, and they require careful thinking and analytical precision going forward.

IMPLICATIONS FOR U.S. AND INTERNATIONAL POLICY

This analysis raises a number of issues, both for U.S. foreign and security policy and for the international community. These can broadly be grouped into three clusters: concerns over the role of technology in a global environment increasingly characterized by U.S.-China strategic competition, concerns about data security and privacy, and additional concerns about the possibility of authoritarian backsliding and human rights infringement.

The first dimension of concern has to do with data privacy and security: whether Chinese dominance of the global surveillance technology industry could create vulnerabilities among U.S. allies and other countries in terms of data privacy, data security, and resilience to hacking and other cybersecurity risks. In early 2020, Trump administration officials asserted that Huawei could covertly access mobile communications through "back doors" designed for law enforcement; typically, use of these interfaces by the equipment-makers after installation is restricted by law, but American officials claimed that the access points had not been disclosed either to local customers or to "host nation national-security agencies."[26] Huawei has rejected these allegations, and — as illustrated in the cases of the Philippines and Malta — at least some recipient countries claim that data is managed by their own nationals and stored locally, thereby obviating many of the privacy concerns raised by critics. There is no systematic, publicly available information on how many "Safe City"-type agreements contain such data protection measures, and the U.S. has not released information on whether and how often it has observed backdoor access being used to covertly gather information. Should a Chinese company have access to user information, however, that information would be available to the Chinese government under the provisions of the 2017 National Intelligence Law.[27]

The second cluster of concerns has to do with whether the use of this technology will contribute to democratic backsliding, autocratization, and human rights violations, strengthening the hand of repressive actors in weak democracies or competitive authoritarian countries, and making autocrats worldwide more capable of implementing their repressive aims. Recent policy discourse expresses strong concern that autocrats may effectively leverage technology to promote disinformation, implement repression, and prolong their rule.[28] As noted above, however, this is an empirically question about which relatively little hard data exists; it is important to obtain answers to these questions to inform future U.S. national security policy as well as democracy and human rights promotion.

The third set of concerns has to do with U.S.-China strategic competition, and the perceived centrality of technology and innovation in that competition.[29] The Pentagon has already flagged the risk that China's expansion into the overseas "Safe City" market could increase Chinese tech companies' "access to foreign talent and data" in ways that are detrimental to the U.S. or its partners[30] — presumably through research partnerships involving foreign data scientists, recruitment through programs like Huawei's "Seeds for the Future Program" or the establishment of overseas offices, and agreements that allow Chinese companies to use overseas data to improve their products.

Second, analysts debate whether access to large amounts of global data will enable Chinese researchers and government bodies to rapidly improve their algorithms and machine learning processes in ways that have implications — particularly given China's focus on military-civil fusion[31] — not just for the Chinese Communist Party's (CCP) own strategies of domestic control, but for security and military competition with the United States. Whether this is true or not at a technical level remains contested, but the potential remains for Chinese companies and government actors to leverage this technology to generate intelligence insights on important countries and populations, which could have secondary effects on strategic competition with the United States. Still other analysts have noted that the growing use of Chinese surveillance technologies in third countries, combined with American pushback on this trend, could bifurcate the world into adopters and non-adopters in ways that are not yet fully understood.[32]

> **"The correlation that exists between levels of violent crime and the adoption of Chinese surveillance and policing technology suggests that many countries see these platforms as providing a real potential solution to important problems facing their populations.**

How should the United States respond? First, current discussions in Washington that focus largely on Chinese intent are understandable, but the findings above suggest that the current strong focus on Beijing's priorities should be complemented by more nuanced and case-by-case discussions of why third countries find Chinese surveillance platforms appealing enough to adopt. In particular, the correlation that exists between levels of violent crime and the adoption of Chinese surveillance and policing technology suggests that many countries see these platforms as providing a real potential solution to important problems facing their populations (while in some cases, of course, also providing regimes or incumbents with political advantage vis-à-vis their potential opponents). To be effective, U.S. policy initiatives and messaging will need to acknowledge these realities, and engage in dialogue with recipient-country counterparts based on a nuanced and accurate view of the tradeoffs that leaders in each of these countries face, many of which have little to do with China at all.

Here, it is especially important to note that the officials who make the initial decisions on platform adoption are often subnational officials — typically municipal mayors, provincial governors, or the heads of public safety departments for various jurisdictions. These officials are often elected or appointed to address different outcomes than the priorities emphasized by foreign policy and national security experts: reducing crime, boosting tourism and investment, and promoting local employment and job growth. Local officials can also have highly varying levels of familiarity with and expertise on national security and cybersecurity issues, which runs the risk of exacerbating communication mismatches and lowering receptivity to American expressions of concern if those concerns are framed too much around China, foreign policy, and security risks without adequate incorporation of local context. Finally, timetables matter: it may be important to subnational officials to deliver positive results on their key priorities on a specific electoral timetable. This means that China's closed and "off-the-shelf" systems, which are quicker to get up and running, may have a competitive advantage over the open systems preferred by the U.S., even if they have drawbacks in terms of long-term adaptability and scalability.[33]

For all of these reasons, a one-size-fits-all message about the risks of Chinese technology needs to be differentiated and adapted for each country in which these concerns are raised. The U.S. and associated democracies will need to think carefully about how to connect with and convey their concerns not just to counterparts in foreign ministries and national security apparatuses, but to local, subnational officials — while also listening to and taking seriously the needs and incentives of those leaders.

The United States will also need to be aware of how its messaging on surveillance technology can run up against competing policy priorities in different regions and countries. In Latin America, for example, U.S. officials may want to think about how it communicates the objective of reducing or slowing the proliferation of Chinese surveillance technology in a way that does not generate tension with another major foreign policy priority of the Trump administration — decreasing local crime and drug-related activity in order to lower migration pressures on the United States' southern border.

At the global level, the spread of Chinese (and other) public security technology has sparked debate over what norms and mechanisms, if any, should govern the market for and use of these platforms, within and across state borders. United Nations official David Kaye, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, recently described these technologies as operating in a "free for all" environment, spreading "technology that is causing immediate and regular harm to individuals and organizations that are essential to democratic life."[34] He called for the development of global standards and publicly-owned mechanisms to limit both the domestic use and international export of private surveillance technology. A recent Brookings report similarly urged policymakers to move beyond a focus on the CCP's intent to think more broadly about the long-term and "cumulative impact of its modeling and export of mass surveillance."[35]

Yet Chinese companies appear to be outpacing the United States, and other countries, in setting emerging global standards for the use of these technologies. Indeed, the PRC has pursued a highly strategic approach to global standard-setting for some time now; it has organized domestic groups that include multiple ministries and major Chinese tech companies to develop China's own ideas about domestic standards, especially on issues like 5G and AI, and has then actively promoted these standards via different international organizations and mechanisms.[36] The Financial Times, for example, reported in late 2019 that Chinese tech companies had made the only submissions to the UN's International Telecommunications Union (ITU) for international standards in surveillance technology since 2016; half of those proposals have since been approved.[37] China's active engagement and leadership at the ITU, as well as in other international technology standard-setting bodies, has helped it to quietly and quickly shape the global regulatory environment in its favor, a strategy that is likely to assist its companies in maintaining or increasing their access to markets worldwide.

Setting and strengthening global regulatory frameworks in ways that are compatible with American values is important for achieving U.S. objectives abroad, now and for years to come. To catch up, the United States needs to articulate and execute a clear strategy: It must decide which forums should set standards for which technologies, and work collaboratively but aggressively to promote standards that are compatible with human rights, civil liberties, privacy, and democracy.[38] This effort could be led by the State Department's International Communications and Information Policy team, but will likely require high-level leadership to be effective. The more that the United States can collaborate on this strategy with like-minded democratic partners, the better its chances of success will be; for example, the European Union's important role in regulatory norms and standard-setting make it a prime candidate for this kind of mutually beneficial partnership.[39] Finally, the United States should consider deploying its foreign assistance partners and programs to work with emerging, weak, or backsliding democracies to craft legal and regulatory safeguards around the use of these technologies that will protect citizen rights and democratic institutions.

One factor that has the potential to complicate standard-setting for surveillance technology in the coming months is the intersection of surveillance technology tools with urgent global public health concerns around COVID-19. Tools such as contact tracing, which require intensive surveillance of and information collection on citizens, pulled together by sophisticated data analysis platforms, are being employed by democracies as well as autocracies (Taiwan and South Korea are notable democratic examples), and have received attention for their apparent effectiveness in managing the pandemic.[40] Indeed, materials on the ITU's webpage highlight China's use (and others') of mobile phone contact tracing initiatives as an example of "an effective way of containing the spread of the disease."[41]

While a full examination of the ways in which the COVID-19 outbreak may shape different countries' approaches to surveillance technology is beyond the scope of this report, two points are worth noting. First is the ongoing debate over which governance models are more capable of addressing this kind of crisis, and why. The way the United States handles COVID-19 has implications not only for the fate of American citizens, but for America's perceived global leadership role.[42]

Second, it is not a stretch to say that the tools used to monitor and enforce citizen behavior during the pandemic are tied to overall models of domestic security and regime control. In fact, the Chinese phrase "prevention and control" (防控), now used to describe the PRC's public health strategy, was previously used to describe the containment and management of domestic political unrest; information gathered through newly deployed health apps, for example on citizen movements, is accessible to local police almost immediately.[43] Tools that gain credibility as effective for public health purposes now will become difficult to roll back in a post-pandemic environment, even if they are subsequently used for less benign and more repressive purposes.[44] The United States should begin thinking now about what tradeoffs on privacy and other civil liberties it is willing to accept in the name of public health, how to craft technological solutions that protect American lives and values simultaneously, and what the U.S. can do to shape and lead international responses to the crisis in ways that favor a global balance of freedom.

This is not an exhaustive list of policy recommendations. Tools such as export controls, sanctions, and restrictions on foreign investment in surveillance technology companies whose practices are not compatible with democracy, human rights, and American national security interests are all valuable, and should be incorporated into the toolkit — preferably in partnership with the private sector, including American technology companies — and coordinated multilaterally with like-minded democratic partners around the world. But perhaps paradoxically, the above analysis suggests that in order to succeed in strategic competition with China, the U.S. may want to talk less about China itself, and more about the compelling alternatives it can offer, both for individual partners, and for confronting shared global challenges. The above steps are designed to facilitate that approach.

REFERENCES

[1] Richard Fontaine and Kara Frederick, “The Autocrat’s New Tool Kit,” *The Wall Street Journal*, March 15, 2019, https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637.

[2] Louise Lucas and Emily Feng, “Inside China’s Surveillance State,” *Financial Times*, July 19, 2018, https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543; Paul Mozur, “Inside China’s Dystopian Dreams,” *The New York Times*, July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html; Paul Mozur, “Made in China, Exported to the World: The Surveillance State,” *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html; Chris Buckley, Paul Mozur, and Austin Ramzy, “How China Turned a City Into a Prison,” *The New York Times*, April 4, 2019, https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html; Josh Chin and Clement Burge, “Twelve Days in Xinjiang,” *The Wall Street Journal*, December 19, 2017, https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355; Maya Wang, “China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App,” (New York: Human Rights Watch, May 2019), https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance; Joe Parkinson, Nicholas Bariyo, and Josh Chin, “Huawei Technicians Helped African Governments Spy on Political Opponents,” *The Wall Street Journal*, August 14, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[3] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, “Mapping China’s Tech Giants,” (Barton, Australia: Australian Strategic Policy Institute, April 18, 2019), https://www.aspi.org.au/report/mapping-chinas-tech-giants; Adrian Shahbaz, “Freedom on the Net 2018: The Rise of Digital Authoritarianism,” (Washington, DC: Freedom House, October 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Jonathan E. Hillman and Maesea McCalpin, “Watching Huawei’s ‘Safe Cities,’” (Washington, DC: Center for Strategic and International Studies, November 4, 2019), https://www.csis.org/analysis/watching-huaweis-safe-cities; Steven Feldstein, “The Global Expansion of AI Surveillance,” (Washington, DC: Carnegie Endowment for International Peace, September 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847. See also Ty Joplin, “China’s Newest Export? Policing Dissidents,” Al Bawaba, May 31, 2018, https://www.albawaba.com/news/china%E2%80%99s-newest-global-export-policing-dissidents-1139230; Chris Daw, “Watch out: Everything we do and say can now be monitored and stored for future reference,” *The Spectator*, July 6, 2019, https://www.spectator.co.uk/2019/07/chinas-surveillance-technology-is-terrifying-and-on-show-in-london/amp/.

[4] “Hearing: China’s Digital Authoritarianism: Surveillance, Influence, and Social Control (Open),” Permanent Select Committee on Intelligence, U.S. House of Representatives, May 16, 2019, https://intelligence.house.gov/calendar/eventsingle.aspx?EventID=632.

[5] Adrian Shahbaz, “Freedom on the Net 2018: The Rise of Digital Authoritarianism”; Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, “Mapping China’s Tech Giants”; Jonathan E. Hillman and Maesea McCalpin, “Watching Huawei’s ‘Safe Cities.’”

[6] Huawei declined to provide a list of the 100+ countries (Huawei, personal communication with the author, June 2019). “2015 Annual Report,” (Shenzhen: Huawei, 2016), 28, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annualreport2015_en.pdf; “2016 Annual Report,” (Shenzhen: Huawei, 2017), 4, https://www-file.huawei.com/-/media/CORPORATE/PDF/annual-report/AnnualReport2016_en.pdf?la=en; “2017 Annual Report,” (Shenzhen: Huawei, 2018), 31, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2017_en.pdf; “2018 Annual Report,” (Shenzhen: Huawei, 2019), 30, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en_v2.pdf?la=zh.

[7] The dataset was developed as part of a broader research project; several articles and a book manuscript using this data are currently in development or under peer review. More detail is available from the author, who can be contacted via her Brookings expert page: https://www.brookings.edu/experts/sheena-chestnut-greitens/.

[8] For example, a recent Carnegie report that covers AI surveillance has two key differences from this approach: a) it discusses hardware usage that does not necessarily involve the use of a full "platform" (such as facial-recognition enabled cameras only); and b) it examines countries other than China and non-Chinese as well as Chinese companies. Steven Feldstein, "The Global Expansion of AI Surveillance."

[9] Note that although C4ISR typically is used to denote "Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance," Huawei materials substitute "Cloud" instead of "Computers." See for example, "2017 Annual Report," Huawei, 31. Safe City platforms are a subcomponent of "Smart City" projects, which Huawei describes as providing a "nervous system" for the city; Safe City platforms are specifically focused on public safety. "Huawei Creates a Smart City Nervous System for More Than 100 Cities with Leading New ICT," Huawei, November 14, 2017, https://www.huawei.com/en/press-events/news/2017/11/Huawei-Smart-City-Nervous-System-SCEWC2017.

[10] "Iran, North Korea, and Syria Nonproliferation Act: Imposed Sanctions," U.S. Department of State, May 23, 2013, https://2009-2017.state.gov/t/isn/inksna/c28836.htm. On CEIEC's work in Latin America, see Fan Feifei, "Transforming Public Security," *China Daily*, January 9, 2017, https://www.chinadaily.com.cn/business/2017-01/09/content_27896419.htm.

[11] "Addition of Certain Entities to the Entity List," Federal Register, October 9, 2019, https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.

[12] Due to lags in reporting, it is likely that not all 2019 adoptions are reflected on this map.

[13] This way of viewing today's developments is also consistent with how historians understand past cases of public security training and technology transfer, wherein national security considerations played a major role. The U.S., the Soviet Union, and East Germany all provided significant amounts of internal security assistance to affiliated states during the Cold War. See for example, Jeremy Kuzmarov, *Modernizing Repression: Police Training and Nation-Building in the American Century* (Amherst and Boston: University of Massachusetts Press, 2012).

[14] Steven Feldstein, "The Global Expansion of AI Surveillance," 1.

[15] Steven Feldstein, "The Global Expansion of AI Surveillance"; see also Steven Feldstein, "How Artificial Intelligence is Reshaping Repression," *Journal of Democracy* 30, no. 1 (January 2019), https://carnegieendowment.org/2019/01/09/how-artificial-intelligence-is-reshaping-repression-pub-78093; Steven Feldstein, "Artificial Intelligence and Digital Repression: Challenges to Global Governance," SSRN, May 9, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3374575.

[16] Alina Polyakova and Chris Meserole, "Exporting digital authoritarianism: The Russian and Chinese models," (Washington, DC: The Brookings Institution, August 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.

[17] "Safe Cities: a Revolution Driven by New ICT," Huawei, https://e.huawei.com/us/publications/global/ict_insights/201608271037/ecosystem/201608271557; Koh Hong-Eng, "How video cameras can make cities safer and contribute to economic growth," *South China Morning Post*, June 3, 2018, https://www.scmp.com/comment/insight-opinion/article/2148860/big-brother-surveillance-how-video-cameras-can-make-cities.

[18] Myat Pyae Pho, “Huawei to Supply Mandalay’s Safe City Project with Security Cameras, Equipment,” The Irrawaddy, May 9, 2019, https://www.irrawaddy.com/news/burma/huawei-supply-mandalays-safe-city-project-cameras-security-equipment.html; Cassandra Garrison, “Safe Like China: in Argentina, ZTE finds eager buyer for surveillance tech,” Reuters, July 5, 2019, https://www.reuters.com/article/us-argentina-china-zte-insight-idUSKCN1U00ZG; “Chinese technology brings falling crime rate to Ecuador,” Xinhua, January 19, 2018, http://www.xinhuanet.com/english/2018-01/19/c_136908255.htm.

[19] “Transforming Bonifacio Global City into a Safe City with Huawei,” Huawei, https://e.huawei.com/topic/leading-new-ict-en/safe-city-case.html.

[20] Ben O’Rourke and Gigi Choy, “Big Brother Huawei Kitted Out this Philippine City,” *South China Morning Post*, January 28, 2019, https://www.scmp.com/week-asia/economics/article/2183540/big-brother-huawei-watches-philippine-city-does-china-too.

[21] Loreben Tuquero, “Año says China-funded Safe Philippines project will be ‘all-Filipino’,” Rappler, November 22, 2019, https://www.rappler.com/nation/245529-ano-china-funded-safe-philippines-project-all-filipino; Camille Elemia, “Senators Sound Alarm over China-funded DILG surveillance project,” Rappler, December 13, 2018, https://www.rappler.com/nation/218831-dilg-china-telecom-affiliate-partnership-video-surveillance-system-philippines.

[22] Jacob Borg, “Huawei Project Similar to That Considered in Malta Had Security Issues,” *Times of Malta*, April 19, 2019, https://timesofmalta.com/articles/view/security-vulnerabilities-found-in-huawei-project-considered-in-malta.707260; Yannick Pace, “Huawei Not Operating Safe City Equipment, as concerns mount over Chinese tech giant,” *Malta Today*, January 30, 2019, https://www.maltatoday.com.mt/news/national/92556/huawei_not_operating_safe_city_equipment_as_concerns_mount_over_chinese_tech_giant#.XpouNOu1vOQ; Matthew Vella, “Huawei Link to China Carries Risk in Safe City Malta Project, Says US Official,” *Malta Today*, May 13, 2019, https://www.maltatoday.com.mt/news/national/94927/huawei_link_in_safe_city_carries_risk#.Xposwuu1vOQ.

[23] Bojan Stojkovski, “Huawei’s Surveillance System in Serbia Threatens Citizens’ Rights, Watchdog Warns,” ZDNet, April 10, 2019, https://www.zdnet.com/article/huaweis-surveillance-system-in-serbia-threatens-citizens-rights-watchdog-warns/; “New surveillance cameras in Belgrade: location and human rights impact analysis – ‘withheld,’” SHARE Foundation, March 29, 2019, https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/.

[24] A systematic quantitative exploration of these associations is available from the author, as part of a book manuscript-in-progress.

[25] Jonathan E. Hillman and Maesea McCalpin use Freedom House ratings; similar variation exists across Polity scores — see “The Polity Project,” Center for Systemic Peace,” https://www.systemicpeace.org/polityproject.html.

[26] Bojan Pancevski, “U.S. Officials Say Huawei Can Covertly Access Telecom Networks,” *The Wall Street Journal*, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[27] The National Intelligence Law (中华人民共和国国家情报法) is one of a series of legal reforms pursued by Xi Jinping as part of a larger overhaul of the domestic and internal security system in China. See Sheena Chestnut Greitens, “Domestic Security in China under Xi Jinping,” *China Leadership Monitor*, March 1, 2019, https://www.prcleader.org/greitens. See also Murray Scot Tanner, “Beijing’s new national intelligence law: from defense to offense,” Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; English translation at “National Intelligence Law of the P.R.C. (2017),” *China Law Translate*, June 27, 2017, https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/?lang=en.

28 Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs* 99, no. 2 (March/April 2020), https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

29 Ryan Hass and Mira Rapp-Hooper, "Responsible Competition and the Future of U.S.-China Relations: Seven Critical Questions for Strategy," The Brookings Institution, February 6, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/02/06/responsible-competition-and-the-future-of-u-s-china-relations/.

30 "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019," (Arlington, VA: U.S. Department of Defense, May 2, 2019), 101, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

31 For a range of perspectives on this phrase and its implications, see "Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy," (Washington, DC: U.S.-China Economic and Security Review Commission, June 7, 2019), https://www.uscc.gov/sites/default/files/2019-10/June%207,%202019%20Hearing%20Transcript.pdf.

32 Kelly A. Hammond, "Reconfiguring Geopolitics in the Era of the Surveillance State: Uyghurs, the Chinese Party-State, and the Reshaping of Middle Eastern Politics," Hoover Institution, June 27, 2019, https://www.hoover.org/research/reconfiguring-geopolitics-era-surveillance-state-uyghurs-chinese-party-state-and-reshaping.

33 Sokwoo Rhee, Associate Director of Cyber-Physical Systems Program at the National Institute of Standards and Technology (NIST), in remarks at "Cities of Tomorrow: Safety, Smarts, and Surveillance" (event at Center for Strategic and International Security, Washington, DC, January 23, 2020), https://reconnectingasia.csis.org/analysis/entries/cities-tomorrow-safety-smarts-and-surveillance/.

34 "Moratorium call on surveillance technology to end 'free-for-all' abuses: UN Expert," United Nations, June 25, 2019, https://news.un.org/en/story/2019/06/1041231.

35 Tarun Chhabra, "The China challenge, democracy, and US grand strategy," (Washington, DC: The Brookings Institution, February 2019), https://www.brookings.edu/research/the-china-challenge-democracy-and-u-s-grand-strategy/.

36 Elsa Kania, "China's play for global 5G dominance—standards and the 'Digital Silk Road,'" Australian Strategic Policy Institute, June 27, 2018, https://www.aspistrategist.org.au/chinas-play-for-global-5g-dominance-standards-and-the-digital-silk-road/.

37 Anna Gross and Madhumita Murgia, "China Shows its Dominance in Surveillance Technology," *Financial Times*, December 26, 2019, https://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96.

38 That the United States should think carefully, strategically, and creatively about available forums does not mean that it can unilaterally choose which forums to care about; given how far the discussion has evolved already, some forums – like the ITU – are not going to be discretionary. In that case, the United States needs a clear and active plan for robust multilateral engagement.

39 For a discussion of the EU's role, see Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020).

40 On Taiwan, see C. Jason Wang, Chun Y. Ng, and Robert H. Brook, "Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing," *Journal of the American Medical Association* 323, no. 14 (March 3, 2020): 1341-1342, https://jamanetwork.com/journals/jama/fullarticle/2762689. For an overview of the way surveillance and data tools have been used in South Korea, see this Twitter thread by Raphael Rashid (@koryodynasty), Twitter, April 17, 2020, https://twitter.com/koryodynasty/status/1251348652070592516.

[41] See “3 key areas innovative tech is helping during the COVID-19 pandemic,” International Telecommunications Union, April 17, 2020, https://news.itu.int/3-ways-innovative-tech-is-helping-during-the-covid-19-pandemic/.

[42] Recent examples of this debate are too numerous to exhaustively list, but see, for example, the cover story “Is China Winning?” *The Economist*, April 16, 2020, https://www.economist.com/leaders/2020/04/16/is-china-winning.

[43] More information on this is available from the author upon request, as part of a book manuscript-in-progress. On other ways in which domestic security tools are being used to enforce quarantines, etc. in China, see Paul Mozur, Raymond Zhong, and Aaron Krolik, “In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags,” *The New York Times*, March 1, 2020, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html; Raymond Zhong and Paul Mozur, “To Tame Coronavirus, Mao-Style Social Controls Blanket China,” *The New York Times*, February 15, 2020, https://www.nytimes.com/2020/02/15/business/china-coronavirus-lockdown.html.

[44] Carrie Cordero and Richard Fontaine, “Health Surveillance Is Here To Stay,” *The Wall Street Journal*, March 27, 2020, https://www.wsj.com/articles/health-surveillance-is-here-to-stay-11585339451; Nicholas Wright, “Coronavirus and the Future of Surveillance,” *Foreign Affairs*, April 6, 2020, https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance.

ABOUT THE AUTHOR

Sheena Chestnut Greitens is a nonresident senior fellow at the Center for East Asia Policy Studies at Brookings, and an assistant professor of political science at the University of Missouri. Her work focuses on East Asia, authoritarian politics, and American national security policy. In August 2020, she will become an associate professor at the Lyndon B. Johnson School of Public Affairs at the University of Texas at Austin.

ACKNOWLEDGEMENTS

The author thanks the National Asia Research Program for financial support and Adriana Boersner, Marc-Olivier Cantin, Edward Goldring, Yuan Yuan Hsu, Yu Bin Kim, and Emir Yazici for excellent research assistance. Thanks also for helpful feedback from audiences at National Bureau of Asian Research's 2019 Asia Policy Assembly, the American Political Science Association's 2019 conference, Princeton University, the University of Texas at Austin, the Center for a New American Security and Bridging the Gap's "Digital Authoritarianism" workshop, Duke University's "Getting China Right" workshop, and Yale University's "Repression in China and the World" conference, as well as Heather Ba, Benjamin Della Rocca, Bryce Reeder, Laron Williams, Joseph Wright, and the anonymous reviewers arranged by Brookings. Ted Reinert edited this paper, and Rachel Slattery provided layout. Any errors of fact or interpretation are the author's responsibility.

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.