Working Paper for the Penn Project on the Future of U.S.-China Relations

China's Surveillance State at Home & Abroad: Challenges for U.S. Policy

Sheena Chestnut Greitens
Associate Professor, University of Texas at Austin

This memo examines the challenges of China's surveillance state, and of the export of Chinese surveillance technologies and tools beyond the borders of the People's Republic of China. Under Xi Jinping, China has pursued a surveillance state of immense scale and ambition, focused on "prevention and control" of risks to social stability and CCP rule, with technology as the key tool by which the regime's preventive aims are to be achieved. The rise of this surveillance state has also had significant global consequences: over the course of the past decade, Chinese surveillance and policing technologies have been adopted in more than 80 countries worldwide, both democratic and autocratic, on every continent except Australia and Antarctica. China is therefore an 'index case' for a set of technological and informational conditions that have spread widely around the world. This memo briefly describes the challenges posed by these twin developments, and then outlines a set of recommendations for U.S. policy, beginning with the need for a comprehensive strategy to understand, track, and where necessary counter the spread of Chinese surveillance technology.

Media and policy discussions have been full of discussions about the use of Chinese surveillance and policing technology, and the rise of a surveillance state in China itself as well as the impact of Chinese surveillance technology well beyond China's borders. Reports by policy analysts warn of the dangers of high-tech surveillance and artificial-intelligence (AI)-based approaches to policing in autocrats' hands,[1] and journalists document the rise of a "dystopian surveillance state" inside China—especially in the far western region of Xinjiang, where Turkic Muslim minorities, particularly Uyghurs, have been subject to mass detention and involuntary ideological reeducation in the name of 'counterterrorism.'[2] Globally, China's export of these

[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; 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.

[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

surveillance and policing technologies has also received increasing media and policy scrutiny.[3] News organizations have provided detailed accounts of the spread and use of surveillance technology from China to places like Venezuela, Ecuador, Zimbabwe, and Uganda, and Huawei, the largest supplier of these kinds of platforms, has been at the center of debate over U.S.-China trade and technological competition.[4] At a U.S. House of Representatives hearing in May 2019 on "China's Digital Authoritarianism," both the chairman and the ranking member warned that the export of these technologies would give "countries the technological tools they need to emulate Beijing's model of social and political control."[5]

Dreams," *The New York Times,* July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html; Chris Buckley, Paul Mozur, and Austin Ramzy, "How China Turned a City Into a Prison," *New York Times,* April 4, 2019, https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillanceprison; Eva Dou, "Chinese Surveillance Expands to Muslims Making Mecca Pilgrimage," *Wall Street Journal,* July 31, 2018, https://www.wsj.com/articles/chinese-surveillance-expands-to-muslimsmaking- mecca-pilgrimage-1533045703; 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.

[3] 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; 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; 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] "U.S. Unlikely to Extend Waiver for U.S. Firms to Supply China's Huawei," *Reuters*, September 26, 2019.

[5] "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.

This project examines the internal development of Chinese surveillance and policing technologies, and explores the international consequences of the rise of China's surveillance state. Chinese surveillance technologies are now in use for policing and domestic security purposes in at least 80 countries, both democratic and autocratic, on every continent except Australia and Antarctica. China, therefore, should be thought of as the 'primary' or 'index case' from which a new set of informational and technological conditions is spreading across the world, impacting political life in a wide range of political systems and geographic contexts.[6] China's growing major power role, and its leadership role in a number of international institutions, make it more likely that these technologies and tools will spread into use globally, even if China is not explicitly exporting its authoritarian model.[7] The United States needs a comprehensive and strategic approach to this issue.

China's Surveillance State at Home

Xi Jinping has made redefining the philosophy and management of domestic security a hallmark of his tenure, a redirection that was signaled early by his speeches about the importance of "comprehensive" or "holistic" national security.[8] In doing so, he has emphasized "prevention and control" (防控, *fangkong*) rather than the regime's previous catchphrase, "stability

[6] In epidemiology, an "index case" is the first documented case. In political science, Finkel refers to the Holocaust as an index case for the study of genocide and repression: Evgeny Finkel, "The Phoenix Effect of State Repression: Jewish Resistance During the Holocaust," *American Political Science Review* 109, no. 2 (2015): 339-353; see also Charles King, "Can There Be a Political Science of the Holocaust?" *Perspectives on Politics* 10, no. 2 (2012): 323-41.

[7] For a systematic examination of the factors that make diffusion of Chinese technology more likely, and those that are likely to limit the transferability of Chinese models of surveillance, see Sheena Chestnut Greitens, "Surveillance, Security, and Liberal Democracy in a Post-COVID World," *International Organization,* special issue on the pandemic and global politics (Fall 2020).

[8] Xi Jinping. "Xi Jinping jiu zhengfa gongzuo zuochu zhongyao zhishi" [Xi Jinping issues important instructions on political-legal work], *Xinhua*, January 20, 2015, at http://www.xinhuanet.com/politics/2015-01/20/c_1114065786.htm; http://www.court.gov.cn/fabu-xiangqing-13840.html; Xi Jinping, *On the Holistic Approach to National Security* (Central Party Literature Press, 2018); see also *Xinhua*, "Book of Xi's discourses on national security published," April 15, 2018, http://www.xinhuanet.com/english/2018-04/15/c_137112987.htm.

maintenance," and has emphasized the use of technology and surveillance to collect information on citizens for preventive public security purposes.[9] In 2015, Secretary of the Politics and Law Commission (中共中央政法委员会，or *Zhongyang Zhengfawei*) Meng Jianzhu emphasized *fangkong* as the "correct direction" for political-legal work in a six-point address that invoked the term "foresight" (不断增强工作预见性*, buduan zengqiang gongzuo yujianxing*).[10] In early 2019, at a national meeting of Public Security Bureau (PSB) directors, Minister of Public Security Zhao Kezhi urged his audience to "Always insist on putting *prevention* of political risks as the first priority."[11]

The use of information technology in this effort is paramount: in mid-April 2015, the CCP Central Committee and PRC State Council called for the creation of a "three-dimensional information-based prevention and control system for public-social security" (创新立体化信息化社会治安防控体系，*chuangzin litihua xinxihua shehui zhi'an fangkong tixi*) – another term that appears repeatedly in CCP directives on "social governance" (社会治理, *shehui zhili*) – in order to "comprehensively promote the construction of a peaceful China."[12] The directive calls for the expansion of networked video surveillance and grid management, enhancement of predictive and early warning capabilities in public security, and reorganization of local party and government

[9] See for example, Xi Jinping, "习近平：提高防控能力，着力防范化解重大风险 保持经济持续健康发展社会大局稳定 [Xi Jinping: Improve Prevention and Control Capabilities; Try to Prevent and Resolve Major Risks; Maintain Sustainable and Healthy Economic Development and Overall Social Stability]," January 21, 2019, http://www.qstheory.cn/yaowen/2019-01/21/c_1124021825.htm; for a summary of Xi's changes to domestic security, see Sheena Chestnut Greitens, "Domestic Security in China under Xi Jinping," *China Leadership Monitor*, March 1, 2019, https://www.prcleader.org/greitens

[10] "Meng Jianzhu: Qieshi tigao zhengfa jiguan fuwu daju de nengli he shuiping" [Effectively improve the ability and level of political and legal organs to serve the overall situation], *Renmin fayuan bao*, March 18, 2015, at http://www.court.gov.cn/fabu-xiangqing-13840.html; see also Susan Trevaskes, Susan, "Rationalizing Stability Preservation Through Mao's Not-So-Invisible Hand," *Journal of Current Chinese Affairs* 42, no. 2 (2013): 51-77.

[11] Emphasis added. His statement was "始终坚持把防范政治风险置于首位." Li Yukun, "赵克志：防范抵御" 颜色革命"，打好政治安全保卫仗 [Zhao Kezhi: Prevent Color Revolutions and Defend Political Security," *Beijing News,* January 18, 2019, http://www.bjnews.com.cn/news/2019/01/18/540767.html.

[12] CCP Central Committee/PRC State Council, "关于加强社会治安防控体系建设的意见 [Opinion Regarding Strengthening the Construction of a Societal Security Prevention and Control System]," April 13, 2015, http://www.gov.cn/xinwen/2015-04/13/content_2846013.htm

work in this area to limit information gaps and achieve smoother coordination of information and public security intelligence.[13] The CCP has also explored a number of ways to more directly connect information-gathering with the infrastructure and management of public security at the ground level, including major organizational and legal reforms throughout China's political-legal apparatus (政法系统, *zhengfa xitong*).[14]

By 2015, at least 168 of China's 332 prefectural-level cities were using an approach known as "community grid management," in which high-tech data collection and integration platforms manage a system of local "grids," closely monitoring developments that emerge from the data and using it for social control.[15] Under initiatives such as Skynet (天网, *Tianwang*) or the "Bright Snow Project" (雪亮工程, *Xueliang Gongcheng*, also called "Sharp Eyes"), video surveillance and facial recognition are being integrated into grid management platforms, and officials are learning to use the data-integration platforms to identify threats via predictive analytics.[16] The *Xueliang Gongcheng* is now operating in all provinces, and China's 13th Five Year Plan calls for implementation to be completed by 2020.[17] In March 2018, a graduate student working on surveillance in Hunan province tested the system run by his local PSB; it took the police four minutes and fifteen seconds to locate him, and just over five minutes to take

[13] This emphasis on informatization and technology also parallels the emphasis on networked intelligence and decision-making observable in China's military strategy. See Taylor Fravel, *Active Defense: China's Military Strategy since 2919* (Princeton, 2019).

[14] For more detail on these reforms, see Sheena Chestnut Greitens, "Domestic Security in China under Xi Jinping," *China Leadership Monitor*, 1 March 2019, https://www.prcleader.org/greitens

[15] Lin, Xuefei. 2015. "Zhengfujian zuzhi xuexi yu zhengce zaishengchan [Organizational Learning among Governments and Policy Reproduction]", *Gonggong guanli xuebao* [*Journal of Public Management*] 12 (1): 11-23; National Development and Reform Commission [NDRC], "Guanyu jiaqiang gonggong anquan shipin jiankong jianshe lianwang [Strengthening Public Security Video Surveillance Network Construction]," 2015, http://www.ndrc.gov.cn/zcfb/zcfbtz/201505/t20150513_691578.html

[16] *Tianwang* comes from a saying "*Tianwang huihui, shu er bulou* (Heaven's net has large mesh, but it lets nothing through)"; while *Xueliang* comes from the saying, "*Renmin qunzhong de yanjing shi xueliang de* (the eyes of the people and the masses are as bright as snow)."

[17] "National Economic and Social Development of the People's Republic of China: Outline of the 13th Five-Year Plan," *Xinhua*, March 17, 2016, http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm

him into custody.[18] A similar experiment by BBC reporter John Sudworth in Guiyang in December 2017 lasted seven minutes.[19]

The outbreak of the novel coronavirus in Wuhan in early 2020 has accelerated the consolidation and enhancement of these systems.[20] CGM and its related surveillance capabilities were heavily relied on to enforce community lockdowns: Hubei's Politics & Law Committee, for example, mobilized 170,000 grid workers (for a provincial population of 59 million) to conduct health surveillance and enforce lockdown policies, home checks, and travel restrictions.[21] The 2008 Beijing Olympics acted as a demonstration point helping to diffuse China's surveillance technology for purposes of public safety and urban security; it is yet to be seen whether the 2020 outbreak will serve as a similar demonstration point for the marketing and export of Chinese health surveillance technologies.

China's Export of Surveillance and Policing Technology

The development of China's surveillance and policing technologies has already had global consequences. China has exported surveillance platforms for use in policing and internal

[18] "天网工程智能人脸监控系统再迎挑战者5分22秒被抓获," *Security knowledge network* [安防知识网], March 19, 2018, http://security.asmag.com.cn/news/201803/93606.html

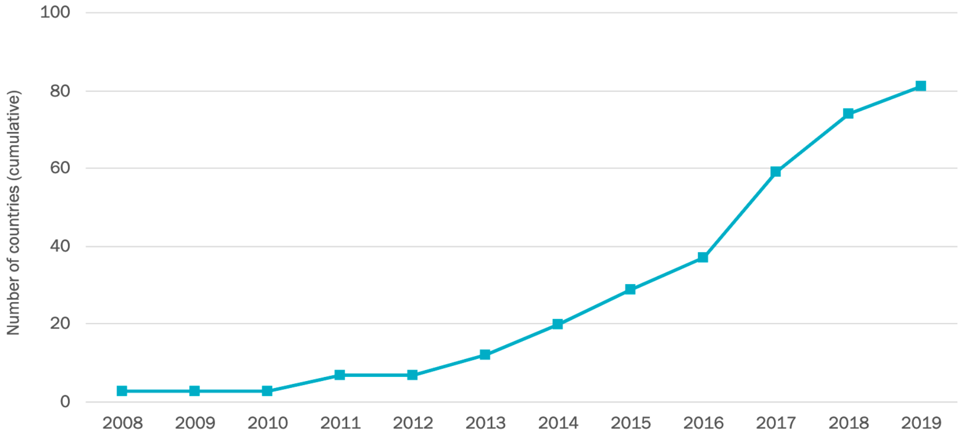
[19] "In Your Face: China's All-Seeing State," *BBC*, 10 December 2017, https://www.bbc.com/news/av/world-asia-china-42248056

[20] Sheena Chestnut Greitens and Julian Gewirtz, "China's Troubling Vision for the Future of Public Health," *Foreign Affairs* (July 2020), https://www.foreignaffairs.com/articles/china/2020-07-10/chinas-troubling-vision-future-public-health. See also 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.

[21] Raymond Zhong and Paul Mozur, "To Tame Coronavirus, Mao-Style Social Controls Blanket China," *New York Times,* February 15, 2020, https://www.nytimes.com/2020/02/15/business/china-coronavirus-lockdown.html; "On the frontline of epidemic prevention and control, nearly 170,000 Hubei grid members act," February 7, 2020, https://www.chahuxz.com/news/50626.html; Liza Lin, "China's Plan to Make Permanent Tracking on Smartphones Stirs Concern," *Wall Street Journal,* May 25, 2020, https://www.wsj.com/articles/chinas-plan-to-make-permanent-health-tracking-on-smartphones-stirs-concern-11590422497

security to at least 80 countries worldwide, with a timeline and geographic distribution shown in Figures 1-2 below: [22]

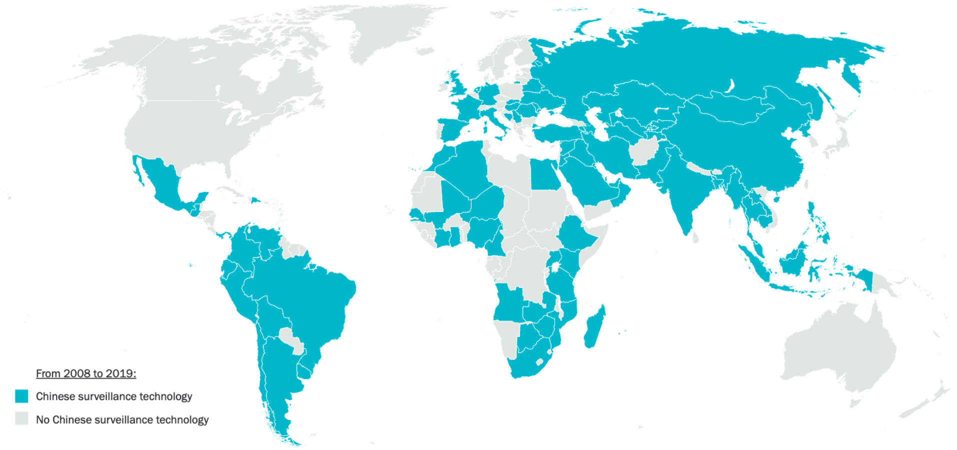
FIGURE 1: ADOPTION OF CHINESE SURVEILLANCE & PUBLIC SECURITY TECHNOLOGY PLATFORMS (2008-2019)



Source: Author's dataset

[22] Some of this section, including Figures 1-2, draws on Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports," *Brookings Global China Project*, April 2020. A prototypical example of surveillance for public safety and domestic security purposes is Huawei's "Safe City" (安全城市) solutions; Huawei remains the largest global supplier of these types of platforms at the time this memo was written, but China National Electronics Import and Export Corporation (CEIEC), ZTE, and other Chinese companies are also commonly involved in these types of projects. Huawei's 2018 annual report stated that its Safe City Solutions "now serve over 700 cities across more than 100 countries and regions," triple the figure cited in the 2015 report. "2015 Annual Report," (Shenzhen: Huawei, 2016), 28, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annualreport2015_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.

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

These data help to shed light on an important debate over the drivers of the spread of these technologies: is it driven by Beijing's desire to export (a supply-side explanation), or by demand from recipient countries—and demand for what exactly? Policymakers and scholars in the U.S. tend to focus on supply-side explanations, fearing that China is exporting these technologies to "make the world safe for autocracy,"[23] and doing so especially in places that China seeks to gain strategic leverage.[24] Chinese tech companies and officials speaking for adopter jurisdictions, however, tend to emphasize the demand or need to deal with crime, and the importance of public safety for attracting tourism and investment.[25]

[23] 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/; Jessica Chen Weiss, "A World Safe for Autocracy? China's Rise and the Future of Global Politics," *Foreign Affairs*, July/August 2019.

[24] 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.

[25] 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-

The data illustrated above suggest that both factors are at work: whether or not a country has a strategic partnership with the PRC (as defined by the Ministry of Foreign Affairs) is positively correlated with adoption of Chinese surveillance and public security technology, but so is violent crime. This suggests that demand and supply-side explanations are not mutually exclusive, but currently reinforce each other. Levels of political stability and levels of democracy in recipient countries are not strongly associated with adoption of these technologies, however, indicating that current and future policy debates should focus more on the potential impact of these technologies on global authoritarianism and democracy, rather than the other way around.

Implications for Policy

The widespread export and international adoption of Chinese surveillance technologies raises important issues for U.S. policy. Chief among these are:

a) concerns about data security and data privacy;
b) concerns over whether or not these technologies will be used to violate human rights or corrode democracy in the places they are exported to; and
c) concerns about the overall role that technology will play in U.S.-China strategic and security competition.[26]

In warning of the dangers of Chinese surveillance technology, current American policy discourse has a tendency to mix these issues without clearly specifying which ones are at risk with specific policy decisions, and why.

This report makes eight principal recommendations to enhance the clarity and strategic coherence of U.S. policy.[27] For brevity, it focuses on recommendations that are not already major

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.

[26] These three issues are outlined in more detail in Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports," *Brookings Global China Project*, April 2020.

components of American policy (such as export controls and sanctions designations). This should not be interpreted as a judgment that existing policies or policy tools are ineffective or unnecessary, but simply as an effort to focus on areas where current policy is lacking or where gaps exist.

The first recommendation is that the United States establish a coordinated, interagency strategy for addressing the challenges posed by the development and export of Chinese surveillance technology. Despite the administration's rhetorical emphasis on Chinese technology, and its actions on Huawei, WeChat, TikTok, and the like, the White House's actual strategy document on China, released in May 2020, contains only a brief reference to the export of surveillance technology from the PRC.[28] It does not provide a clear framework for understanding exactly what threats the global use of Chinese surveillance technologies pose to American national security, or how the United States should analyze and counter their global impact.[29] In the future, China's development and export of surveillance technology should be an area of explicit discussion and strategy development, either as a stand-alone piece or as a clear subcomponent of a larger strategy document, such as the one on China. Developing such a framework could be something that the next administration chooses to do on its own initiative, or could be mandated via a Congressional reporting requirement to ensure that the process will

[27] Some of these recommendations appear in less developed form in Greitens, "Dealing With Demand," as well as in Sheena Chestnut Greitens, "Testimony at the U.S. Commission on International Religious Freedom on Technological Surveillance of Religion in China," Summer 2020.

[28] "United States' Strategic Approach to the People's Republic of China," May 26, 2020, https://www.whitehouse.gov/articles/united-states-strategic-approach-to-the-peoples-republic-of-china/.

[29] On previous gaps between policy on paper and policy as it's been implemented by the administration, see Zack Cooper, "A Tale of Two Asia Policies," *War on the Rocks,* September 2018; Zack Cooper, "Five Critiques of the Administration's China Policy," War on the Rocks, June 29, 2020, https://warontherocks.com/2020/06/five-critiques-of-the-trump-administrations-china-strategy/.

carry over to future administrations. Either way, given the various equities and breadth of policy tools involved, the effort should be led and overseen by the National Security Council.[30]

A coordinated strategy would help because it would provide both a baseline reference point and shared lexicon for explaining specific policy decisions. For example, the identity of some of the companies involved in the export of surveillance technologies has helped to elevate concern about their activities in the U.S. national security and foreign policy community. At least some of these 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.[31] 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.[32] Other technology companies, such as WeChat and TikTok, have been targeted under Executive Orders because of how they treat U.S. citizens' data, or for their role in surveillance and potential coercion.[33] Outlining ahead of time the

[30] This effort should include the Department of Commerce, the State Department's International Communications and Information Policy Team ,and the U.S. Department of Education, among others. It should also seek out and incorporate input from the technology sector, civil society, and stakeholders outside the United States.

[31] "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.

[32] "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.

[33] White House, "Executive Order on Addressing the Threat Posed by WeChat," August 6, 2020; https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/; U.S. Department of Commerce, "Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States," September 18, 2020, https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect; see also Bobby Chesney, "Commerce Department Reveals Scope of TikTok and WeChat Sanctions," *Lawfare*, September 18, 2020, https://www.lawfareblog.com/commerce-department-reveals-scope-tiktok-and-wechat-sanctions.

framework and standards by which specific companies will be identified as concerning will help bring coherence to these measures. It will also highlight areas where U.S. objectives may be better served by creating structural solutions and principles for market access rather than, for example, one-off Executive Orders that target specific companies but leave open the larger problems and security risks associated with data exfiltration from the United States to China.[34]

The second recommendation is that the United States develop a method for regularly tracking and assessing the impact of Chinese surveillance technology on global democracy, civil liberties, and human rights, either inside the United States government or in partnership with academic research institutions and civil society advocacy groups. Right now, there is a major gap in our understanding of whether or not these technologies actually work for the purposes they are marketed for—crime reduction and public safety—as well as whether they systematically undermine democracy, freedom, and human rights in the countries in which these tools are employed, and under what circumstances. (We know, for example, that the use of surveillance to manage the COVID-19 pandemic has resulted in much worse rights violations in autocracies and hybrid regimes than in consolidated democracies; it is possible that Chinese surveillance technology would have similarly disaggregated effects.[35]) It may be that these tools affect one outcome but not the other, or that they affect both outcomes simultaneously, or the effects may differ across different political contexts. Clearer evidence on this front will enhance the credibility of American arguments in the global discussion on tradeoffs and policy solutions. In terms of policy process, this data could be collected and incorporated into the U.S. Department

[34] Aynne Kokas, "China Already Has Your Data. Trump's TikTok and WeChat Bans Can't Stop That," *Washington Post*, August 11, 2020, https://www.washingtonpost.com/outlook/2020/08/11/tiktok-wechat-bans-ineffective/

[35] Amanda B. Edgell, Sandra Grahn, Jean Lachapelle, Anna Lührmann, and Seraphine F. Maerz, "An Update on Pandemic Backsliding: Democracy Four Months After the Beginning of the Covid-19 Pandemic," *V-Dem Policy Brief* #24 (June 30, 2020), https://www.v-dem.net/en/our-work/research-projects/pandemic-backsliding/; see also Greitens, "Surveillance, Security, and Liberal Democracy in a Post-COVID World."

of State's annual reports on global human rights, as suggested by legislation proposed in the 116th Congress, or it could take another form.[36]

The third recommendation is that the United States understand its audience in messaging about the risks of Chinese surveillance technology. One piece of this is that the U.S. should develop country- or at least region-specific language to express its concerns about Chinese surveillance technology. Huawei's marketing materials differentiate its appeal by region, emphasizing extremism in the Middle East, crime in Latin America, and data management and sustainability in Europe.[37] By contrast, current U.S. rhetoric is relatively one-size-fits-all, in keeping with American focus on this as a supply-side China problem, but (as noted above) this rhetoric often weaves together concerns about geostrategic rivalry, democracy and human rights, and data security without clearly stating which one is at issue—and to what extent where. In reality, these three issues are unlikely to be equally present in all potential recipient or adopter countries; recent survey data shows that the level of concern and preferred approach toward Huawei and other tech companies differs globally.[38] Effective diplomatic messaging, therefore, should take these overarching concerns and adapt them to address the context and conditions in particular recipient countries to maximize the effectiveness of U.S. public (and private) communications with potential adopters and stakeholders.

The other way in which the United States must understand its audience is to realize that many of the officials making adoption decisions are subnational authorities—mayors or

[36] See for example, the proposed HR 7307: Foreign Advanced Technology Surveillance Act, https://www.congress.gov/bill/116th-congress/house-bill/7307/text.

[37] "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.

[38] Center for Strategic and International Studies, Mapping the Future of U.S. China Policy (Washington: CSIS, 2020), https://chinasurvey.csis.org/about/.

provincial governors or their public safety leadership—rather than national-level experts in foreign policy and national security. Subnational officials are likely to have different priorities from foreign policy experts; they are often more directly accountable to voters and operate on specific electoral timetables; and they may have more widely varying levels of knowledge and expertise about China and technology from a national security perspective. Moreover, depending on a country's political institutions and culture, subnational officials may have more or less contact with the foreign policy and national security expertise in their own governments. Any effective communication strategy on the part of the United States will have to take all of these differences into account in deciding what messages to deliver, in what format, at what point in time, and to whom.

In keeping with the idea of understanding one's audience is the fourth recommendation: the United States must more concretely grapple with the notion that demand for Chinese technology often exists because it can solve real governance problems for recipients, and work to address the problems that Chinese surveillance technology is being deployed to solve. In Latin America, for example, American officials should realize that listeners may perceive that advocacy to slow or stop the spread of Chinese surveillance technology competes with other American priorities in the region—such as decreasing crime and drug-related activity in order to lower migration pressure on the United States' southern border. Each region of the world will need to think through how region-specific messaging on Chinese surveillance technology may generate competing policy priorities, and how these can be resolved. Similarly the United Nations has announced a partnership with China on several data-integration and big-data analysis projects intended to support the UN's 2030 sustainable development goals, meaning that China-based researchers will have firsthand access to sources of data provided by member governments from all over the world.[39] If the United States is concerned about this kind of development, it must clearly articulate why this is a concern. (Data security? The privacy of the data provided? Some kind of strategic advantage that this could generate to China? The potential for China to use the data to refine its own algorithms of repression? Any of these are plausible, but the logic remains relatively unspecified.) And beyond more precisely articulating the United States' concerns and the causal logic that underpins them, American officials then also need to assess what governance problems China is offering to solve with its use of technology, and identify what alternatives—especially democracy-compatible ones—might exist that the U.S. can reasonably advocate for instead.

The fifth recommendation is that the United States government think about how to maintain and/or increase the United States' edge in innovation, and work with democratic partners to ensure that democracy-compatible alternatives to Chinese technology exist and are competitive in the global marketplace. The United States will only be successful at convincing the world to use "Clean Networks" if the technologies involved in these networks are as good and as affordable as the ones offered by Chinese technology companies;[40] evidence indicates that at present, this is not always the case. Without question, maintaining the United States' capacity for technological innovation is a complex challenge, and will involve thorny questions about how to protect intellectual property and protect illicit technology transfer while also recognizing that a large part of the U.S. current data and tech talent originates from individuals born in the PRC who have come to the U.S. for undergraduate and graduate study.[41] This is yet another reason why a comprehensive interagency strategy—in this case incorporating the Department of

[39] Claudia Rosett, "China Uses the UN to Expand its Surveillance Reach," *Wall Street Journal,* October 7, 2020.

[40] U.S. Department of State, "The Clean Network," https://www.state.gov/the-clean-network/.

[41] MacroPolo, "The Global AI Talent Tracker," https://macropolo.org/digital-projects/the-global-ai-talent-tracker/; Paul Mozur and Cade Metz, "A U.S. Secret Weapon in AI: Chinese Tech Talent," *New York Times,* June 9, 2020, https://www.nytimes.com/2020/06/09/technology/china-ai-research-education.html.

Education and immigration authorities at the Department of Homeland Security—is critical to the effectiveness of American strategy.

The sixth recommendation is that the United States consider a two-layered strategy around the use of Chinese surveillance technology. U.S. strategy to date has involved major campaigns to convince allies and partners not to use technologies made by Chinese companies such as Huawei.[42] While there is some evidence of success in recent decisions to curtail or decline to use Huawei technology in countries like the UK and India, the record on surveillance technology for policing purposes is less positive in terms of the administration's objectives: we were unable to locate a single case of complete de-adoption of a Chinese surveillance and policing platform as of the end of 2019. Instead, countries were more likely to put legal restrictions on the use of these platforms or on specific features. These kinds of adaptation were also more likely in democratic countries (such as the Philippines, Malta, etc.) where civil society and media freedom contributed to scrutiny of the introduction of Chinese technology, and led to specific safeguards being created and elite commitments made about the protection of both data privacy and civil liberties.

This suggests that the United States may want to think about an additional layer of policy, in which it works with countries unwilling to completely de-adopt Chinese surveillance technology to nevertheless create safeguards and firewalls around their use. Rather than trying (belatedly) to prevent adoption altogether or push for costly de-adoption and replacement in all cases, the U.S. may be better served by focusing on creating strong norms of legal constraint

[42] Justin Sherman, "Is the U.S. Winning its Campaign Against Huawei?" *Lawfare*, August 12, 2020, https://www.lawfareblog.com/us-winning-its-campaign-against-huawei; for a more skeptical perspective, see Thomas Lairson, David Skidmore, and Wu Xinbo, "Why the US Campaign Against Huawei Backfired," *The Diplomat,* May 13, 2020, https://thediplomat.com/2020/05/why-the-us-campaign-against-huawei-backfired/; Eric Olander, "Why the US Campaign Against Huawei Will Fail in Africa," *Africa Report,* July 20, 2020, https://www.theafricareport.com/34171/why-the-us-campaign-against-huawei-will-fail-in-africa/.

around these technologies' use in places where de-adoption is not feasible at least in the short-term. Such protective measures could be both technical and legal (either legislative or regulatory/administrative), and would provide some fallback or intermediate measures that would nevertheless contribute to global democracy protection and data security in the countries in question. U.S. democracy promotion attention and funding, as well as partnerships with organizations that focus on capacity-building, such as the American Bar Association and the National Democratic Institute (among others), could be deployed toward this goal, and allies and partners could also contribute to this as a democracy and capacity-building effort.[43]

Seventh, the comprehensive strategy outlined above must include a clear plan for American engagement with global standards-setting and regulation of surveillance technologies. The use and export of surveillance technology is subject to very few global regulations,[44] and where international standards exist, they have been written largely by Chinese tech companies. This is an area where China's growing willingness to lead in global governance has been particularly important; the International Telecommunications Union, for example, which has been headed by PRC national Zhao Houlin since 2014, has received almost all its suggestions on standards for facial recognition technology from Chinese technology companies, and has adopted over half of them.[45] In September 2020, PRC Foreign Minister Wang Yi proposed a Global Data Security Initiative, outlining a Chinese framework that he hoped would serve as "a blueprint for

[43] In the event that the COVID-19 pandemic prompts an upsurge in the adoption of Chinese health-surveillance technology, for example, the United States could work with partners like South Korea, who have written legislation to protect civil liberties during infectious disease outbreaks, who can provide a review of lessons learned to other countries based on their own valuable experiences.

[44] "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; Tom Miles, "UN Surveillance Expert Urges Global Moratorium on Sale of Surveillance Tech," *Reuters*, June 18, 2019, https://www.reuters.com/article/us-socialmedia-un-spyware/u-n-surveillance-expert-urges-global-moratorium-on-sale-of-spyware-idUSKCN1TJ2DV.

[45] Anna Gross, Madhumita Murgia, and Yuan Yang, "Chinese Tech Groups Shaping UN Facial Recognition Standards," *Financial Times*, December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67; see also "Office of the Secretary General of ITU," https://www.itu.int/en/osg/Pages/default.aspx.

the formulation of international principles," inviting other countries and international organizations to participate, and implicitly seeking to position this framework as an alternative to the "free and open internet" approach long advocated by the United States.[46] This multipronged effort is characteristic of a larger and longer-term Chinese project to assume leadership of global governance and international organizations and rewrite rules and norms within the international system such that they are more to China's liking.[47]

Efforts to lead in shaping the global regulatory environment are notable because if China is successful at setting standards that favor Chinese companies, it will tilt the global marketplace in their favor and provide governments worldwide additional reasons to use these technologies. This, in turn, is likely to seed support for these systems across the international system, making it harder for the United States and like-minded partners to promote democracy-compatible technological alternatives. Conversely, however, it is probably unrealistic and counterproductive for the United States to try to deny China a say in global data and tech governance altogether. The United States' overall strategy, therefore, needs to address questions such as: which global forums should set standards for which technologies; what those standards and safeguards should be; how interagency efforts within the United States should be organized; and how the U.S. should work with allies, partners, and international organizations to collaboratively but assertively shape a global environment compatible with liberal democracy.

[46] Graham Webster and Paul Triolo, "Translation: China Proposes Global Data Security Initiative," New America/DigiChina Project, September 7, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative/; for the Chinese-language text, see https://www.fmprc.gov.cn/web/wjbzhd/t1812947.shtml

[47] See for example, Anne Applebaum, "How China Outsmarted the Trump Administration," *The Atlantic* (November 2020), https://www.theatlantic.com/magazine/archive/2020/11/trump-who-withdrawal-china/616475/; "How China is Taking Over UN Agencies, One Vote at a Time," *Wall Street Journal,* September 29, 2020, https://www.wsj.com/articles/how-china-is-taking-over-international-organizations-one-vote-at-a-time-11601397208; Sarah Zheng, "UN Intellectual Property Agency Latest Battleground as China and US Vie For Influence," *South China Morning Post,* March 1, 2020; Kristine Lee, "It's Not Just the WHO: How China is Moving on the Whole UN," *Politico*, April 15, 2020, https://www.politico.com/news/magazine/2020/04/15/its-not-just-the-who-how-china-is-moving-on-the-whole-un-189029.

Eighth, and finally, the strategy adopted by the United States with respect to surveillance technology should carefully consider the role of the Chinese diaspora in the United States, both those who now hold American citizenship and those who do not. As noted above, much of the United States' tech talent involves people who have come from China to study in the United States and choose to remain longer-term.[48] Administration officials and law enforcement personnel must ensure that counterintelligence investigations related to illicit tech transfer and academic espionage do not unfairly target legitimate study and research. Unnecessarily convincing Chinese students and researchers who would otherwise seek to stay in the United States that their only option is returning to China will damage the human capital base required for future technological innovation.[49] Indiscriminate targeting of legitimate activity may also make it more difficult to counter pernicious foreign influence by alienating the very communities and diaspora members who are critical to successful counterintelligence work. Any successful strategy must therefore recognize and deal with a thorny conundrum: while the United States seeks to avoid profiling and discrimination based on ethnic background, the Chinese Communist Party tends to regard members of the diaspora as a monolithic national asset and part of the body politic even when they are located abroad, and has not shied away from placing members of the diaspora under pressure or using relational repression against them.[50] Technologies such as WeChat have sometimes played a role in that coercive pressure, but getting rid of the technology

[48] MacroPolo, "The Global AI Talent Tracker"; Mozur and Metz, "A U.S. Secret Weapon in AI"; Remco Zwetsloot, "US-China STEM Talent Decoupling: Background, Policy, and Impact," *National Security Report,* Johns Hopkins Applied Physics Laboratory, October 2020, https://www.jhuapl.edu/assessing-us-china-technology-connections/publications.

[49] While a full discussion of this point is beyond the scope of the paper, several of the papers in the "Research, Education, and Academic Freedom" section of the Penn Project on the Future of U.S.-China Relations address this dilemma and offer further constructive policy recommendations. These can be found at https://web.sas.upenn.edu/future-of-us-china-relations/research-education-and-academic-freedom/.

[50] Miles Kenyon, "WeChat Surveillance Explained," CitizenLab, May 2020, https://citizenlab.ca/2020/05/wechat-surveillance-explained/; Sheena Chestnut Greitens and Rory Truex, "Repressive Experiences Among China Scholars: New Evidence from Survey Data," *China Quarterly* 242 (2019): 349-375.

will not solve the fundamental dilemma, which is political rather than technological. The Chinese diaspora is increasingly the site of political contention, action, and repression, especially as other avenues of contention within China become ever more limited.[51] The U.S. must begin to think systematically about this issue, define the problem and the stakes, and articulate the principles and interests that will guide its choices, as a first step toward generating constructive policy solutions.

Conclusion

This memo has examined the challenges that emanate from China's domestic development of a high-tech surveillance state, and of the export of Chinese surveillance technologies and tools beyond the borders of the People's Republic of China. Under Xi Jinping, China has pursued a surveillance state of immense scale and ambition, focused on "prevention and control" of risks to social stability and CCP rule, with technology as the key tool by which the regime's preventive aims are to be achieved. Over the course of the past decade, Chinese surveillance and policing technologies have also "gone global," and are now in operation in more than 80 countries worldwide, both democratic and autocratic, on every continent except Australia and Antarctica.

In order to address this challenge, the United States needs a comprehensive strategy that tracks the spread and effects of these technologies; understands and tailors rhetoric to the key audiences it needs to bring on board; identifies and works on democracy-compatible solutions to the governance challenges that Chinese technology is being used to address; and clearly outlines the role of U.S. engagement with international organizations and standard-setting bodies that

[51] This is not a unique dynamic among diasporas whose homelands are under authoritarian rule. See for example, Will Jones and Alexander Betts, *Mobilizing the Diaspora: How Refugees Challenge Authoritarianism* (Cambridge, 2016).

regulate surveillance technology use and export. Additionally, the United States must maintain its own technological capacity for innovation to ensure that democracy-compatible solutions are widely available and cost-competitive, and should consider incorporating an additional layer into its strategies aimed not just at complete de-adoption of Chinese technologies, but of installing protective technical and legal safeguards where such technologies are already in use. Finally, the United States must carefully consider the role of the Chinese diaspora in the United States, and consider how best to address the practical and ethical contradictions that result from the CCP's approach to members of this community. These measures are only a start, but collectively they represent an important first step toward dealing with a major global development and urgent American foreign policy and national security challenge.