CYBER STATECRAFT
INITIATIVE

#ACcyber

DFRLab

ISSUE BRIEF

OCTOBER 2022

China's Surveillance Ecosystem & The Global Spread Of Its Tools

BULELANI JILI

EXECUTIVE SUMMARY

This paper seeks to offer insights into how China's domestic surveillance market and cyber capability ecosystem operate, especially given the limited number of systematic studies that have analyzed its industry objectives. For the Chinese government, investment in surveillance technologies advances both its ambitions of becoming a global technology leader as well as its means of domestic social control. These developments also foster further collaboration between state security actors and private tech firms. Accordingly, the tech firms that support state cyber capabilities range from small cyber research start-ups to leading global tech enterprises. The state promotes surveillance technology and practices abroad through diplomatic exchanges, law enforcement cooperation, and training programs. These efforts encourage the dissemination of surveillance devices, but also support the government's goals concerning international norm-making in multilateral and regional institutions.

The proliferation of Chinese surveillance technology and cyber tools and the associated linkages between both state and private Chinese entities with those in other states, especially in the Global South, is a valuable component of Chinese state efforts to expand and strengthen their political and economic influence worldwide. Although individual governments purchasing Chinese digital tools have their local ambitions in mind, Beijing's export and promotion of domestic surveillance technologies shape the adoption of these tools in the Global South. As such, investigating how Chinese actors leverage demand factors for their own aims, does not undercut the ability of other countries to detect and determine outcomes. Rather it demonstrates an interplay between Chinese state strategy and local political environments. This paper specifically focuses on key features in China's surveillance ecosystem, while the companion to this report will focus on the key 'pull factors' from African countries and their significance for US interests.

INTRODUCTION

Chinese tech companies are among the largest firms in the world. Initially focused on the domestic market, they now sell various surveillance technologies to a global customer base. Increased collaboration between the party-state and private Chinese actors in the sale of surveillance products inspires trepidations about the proliferation of China's surveillance tools, ergo the rise of unwarranted surveillance. Namely, researchers scrutinize China's diplomatic activities, raising questions about the degree to which the government enables surveillance practices abroad. Large Chinese firms and state amplify debate and concerns by pushing to change the norms and mechanisms in the use of public security technology.

This paper seeks to offer insights into how China's domestic surveillance market and cyber capability ecosystem operate, especially given the limited number of systematic studies on the industry and its growing influence in the Global South. This issue brief focuses on the development of the Chinese surveillance industry and the firms that make it possible, including those firms that sell surveillance tools within the international surveillance market. The brief has four parts. The first discusses the development of China's surveillance ecosystem. It specifically explores the establishment of the Golden Shield Project (GSP), a national Closed-Circuit Television (CCTV) network intended to digitize the public security sector, and its consequences for surveillance practices in China. The second section investigates China's conception of "cyber sovereignty," or *wangluo zhuquan,* which seeks to influence the governance of cyberspace. This idea and policy prerogative helps Beijing's promotion of a controlled cyberspace and, therefore, the development of surveillance practices that rely on the use of artificial intelligence, big data, and biometric collection, among other means, to monitor citizens. The third and fourth sections carefully look at how private-public partnerships have empowered China's cyberpower, while at the same time creating a more restrictive legal and political environment in China. What appears to make the party-state distinct from other exporters is the legal and political system from which these surveillance tools emerge—crucially, how China promotes their use in the Global South.[1] The brief concludes by taking a close look at how the spread of Chinese surveillance tools is both a consequence of China's supply capacity and local demand factors.

CHINA'S DOMESTIC TECH ENVIRONMENT

In 2014, President Xi Jinping declared that there was "no national security without cybersecurity."[2] For the Chinese Communist Party (CCP), surveillance technology research and development support the party's intention to be a global technology leader while also augmenting its means of domestic social control. Promoting social stability has been the chief policy goal of the party, and therefore the state, for years.[3] As early as 1990, the State Council approved a proposal to establish a national information system.[4] This includes the Golden Shield (GSP), or *jindun gongcheng* program. GSP is a surveillance initiative launched by the state in 1998. Promoted by public security authorities, the primary aim of the initiative is to create a fully digitized public security sector using a national surveillance network to bolster the means of data management and state security capabilities. Walton's seminal report, "China's Golden Shield Corporations and the Development of Surveillance Technology in The People's Republic of China," examines the early developments of GSP.[5] Walton's work examines how the initiative relied on American and Canadian made technology. Recent government bidding documents show further evidence that American companies supply some of the parts necessary for the GSP project.[6]

The first phase of the GSP involved the digitization of the ministry, province, and city, while the second phase's intent has been to integrate all three levels of public security networks by establishing the means to foster information sharing between the three levels.[7] The project relies on information and communication technology (ICT) systems to enhance the ability of a unified command, rapid response, and coordinated effort to address supposedly the challenges of crime. In its early stages, it was characterized mostly by

1 Bulelani Jili, *The Rise of Chinese Surveillance Technology in Africa.*

2 President Xi Jinping, "China Must Evolve from a Large Internet Nation to a Powerful Internet Nation," 习近平:把我国从网络大国建设成 为网络强国, Xinhuanet, February 27, 2014, http://news.xinhuanet.com/politics/2014- 02/27/c_119538788.htm.
Also see, William Wan, "Chinese President Xi Jinping takes charge of new cyber effort," Washington Post, February 27, 2014, https://www.washingtonpost.com/world/chinese-president-takes-charge-of-new-cyber-effort/2014/02/27/a4bffaac-9fc9-11e3-b8d8-94577ff66b28_story.html.

3 Samantha Hoffman, *Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion*, *Australian Strategic Policy Institute*, October 14, 2019, https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

4 See, for example: Peter Mattis, "China's Adaptive Approach to the Information Counter-Revolution," *Jamestown Foundation China Brief*, 11 No.10 (June 3, 2011), https://jamestown.org/program/chinas-adaptive-approach-to-the-information-counter-revolution/; Yu Xu and Hongren Zhou, "Analysis and Forecast on China's Informatization," 中国信息化形势分析和预测, Beijing: Social Sciences Academic Press, 2010; and Qin Liang, "Public Security Information Industry Overview." 公安信息化行业概况, *Sealand Securities*, 2019, https://web.archive.org/web/20201119002413/pg.jrj.com.cn/acc/Res/CN_RES/INDUS/2016/1/26/3d0f5812-fd68-4045-8dd7-c7a2b04862c6.pdf.

5 Greg Walton, *China's Golden Shield Corporations and the Development of Surveillance Technology in The People's Republic of China*, *International Centre for Human Rights and Democratic Development*, Montreal, 2001, https://ora.ox.ac.uk/objects/uuid:084840ac-b192-407b-ab6c-f8f810310369/download_file?file_format=pdf&safe_filename=CGS_ENG.pdf&type_of_work=Book.

6 Walton, *China's Golden Shield*.

7 Yu Xu and Hongren Zhou, Analysis and Forecast on China's Informatization, 中国信息化形势分析和预测, Beijing: Social Sciences Academic Press, 2010.

surveillance cameras paired with more efficient ways of sharing data within state bureaus. The GSP has grown significantly in size and sophistication since its founding. It now includes 416 million surveillance cameras around the country that utilize artificial intelligence (AI) facial recognition technology.[8] These developments also include many ostensibly benign technologies like geolocation and storage servers that support social control. The Police Geographic, for example, is a geolocation platform made by Tianjin Troila Technology that offers the police real-time spatial visualization data.[9] This project enables the representation of space into grids for surveillance and knowledge building to serve security objectives. Valentin Weber and Vasilis Ververis bolster this argument in research published in August 2021. Their report examines various technologies, including geolocation, which form part of a layered assemblage of surveillance systems that support the tracking of vehicles and people.[10]

The "safe city model," or *Ping an chengshi*, evolved from the GSP.[11] Simply put, it is "a computational model of urban planning that promises to optimize operational efficacy and promote economic growth by leveraging ICT systems."[12] It is a commodity sold by Huawei at home, but also offered across the Global South. Currently, the safe city relies on integrating data from multiple sources that include utility companies, retail stores, and formal banks. This biometric data then feeds databases run by public security bureaus, which utilize facial recognition tools. The centralized information systems are known as city brains, or *Chengshi danao*.[13] These efforts in part bring together civil-commercial actors with the state for the sake of data-driven governance. Underlying the turn towards data-driven governance is Beijing's belief in a scientific outlook on development, or *kexue fazhan guan*, a notion that assumes that technical interventions can numerically capture and abate social challenges, like crime.[14]

CYBER SOVEREIGNTY

In 2016, President Xi maintained that legal and political constraints must be accompanied by the development of technology at home and abroad.[15] A goal of its lobbying on multilateral institutions like the UN is the adoption of its conception of cyber sovereignty. Simply put, cyber sovereignty refers to respecting a nation's right to choose the trajectory of its internet development and management.[16] These lobbying efforts do not merely focus on technical norms and standards aimed at advancing network security, but also speak to the state's right to control the flow of information within its borders. As it stands, Beijing's notion of cyber sovereignty seeks to advocate for a country's sovereign right to delimit and control data flows based on its domestic security interests. From this vantage point, states should discourage interference in the internal affairs of others. This privileging of the state offers legitimacy and cover to Beijing's predilection towards delimiting and controlling online activity, but is also in contrast to Western commitments to cyber governance. While the United States and its allies "advocate for a more open, free, and multistakeholder approach, which provides open platforms for private actors and civil society organizations, China wishes to promote a complete counterapproach that asserts the interests of the government over non-state actors."[17]

China's domestic environment has nurtured a tech industry that supports the state's aims to monitor, censor, and condition public opinion. The Golden Shield Project, which is popularly referred to as the "Great Firewall of China," is the best illustration of this project. An initiative managed by the Ministry of Public Security, which crucially relies on filtering and censorship technologies that operate alongside domestic law that limits and seeks to curate online discourse. Margaret Roberts, in her work titled "Censored: Distraction and Diversion Inside China's Great Firewall," offers a systematic analy-

8 Valentin Weber and Vasilis Ververis. "China's Surveillance State: A Global Project," Top10VPN, August 2021, https://www.top10vpn.com/assets/2021/07/Chinas-Surveillance-State.pdf.

9 Troila Technology, 2022. "警用地理信息服务平台." (Police geographic information service platform). Available at: https://www.troila.com/jiejuefangan?id=159.

10 Weber and Ververis, "China's Surveillance State: A Global Project."

11 Samantha Hoffman, "China's Tech-Enhanced Authoritarianism." (Written Testimony before the House Permanent Select Committee on Intelligence), US Congress, May 16, 2019, https://www.congress.gov/116/meeting/house/109462/witnesses/HHRG-116-IG00-Wstate-HoffmanS-20190516.pdf.

12 Bulelani Jili, "Chinese ICT and Smart City Initiatives in Kenya," Asia Policy, 17, no. 3 (July 2022): 44, https://www.nbr.org/wp-content/uploads/pdfs/publications/asiapolicy17.3_africa-china_relations_rt_july2022.pdf; Shannon Mattern, "A City Is Not a Computer: Other Urban Intelligences," Princeton: Princeton University Press, 2021, DOI: 10.2307/j.ctv1h9dgtj.

13 See, for example: Sohu, "Shanghai's 'Public Security Brain' Is Upgraded to 'City Brain'," 上海"公安大脑"将升级为"城市大脑, 2019, https://www.sohu.com/a/338738299_649849.

14 The concept *kexue fazhan guan* or scientific outlook on development was initially discussed in CCP circles as early as 2003. However, it was only introduced to the public by Hu Jintao in January 2004. It was later adopted by the National People's Congress as a new guideline for social and economic development in March 2004.

15 President Xi Jinping, "Speech at the Symposium on Network Security and Informatization," 习近平在网信工作座谈会上的讲话全文发表, *Xinhuanet*, April 19, 2016, http://www.xinhuanet.com//politics/2016-04/25/c_1118731175.htm.

16 See, for further elaboration of the concept: President Xi Jinping, "Speech at the Opening Ceremony of the Second World Internet Conference," 习近平在第二届世界互联网大会开幕式上的讲话, *Xinhuanet*, December 16, 2015, http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm; Rogier Creemers "China's Conception of Cyber Sovereignty: Rhetoric and Realization," in *Governing Cyberspace: Behavior, Power, and Diplomacy*, SSRN (February 5, 2020) 1-34, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=353242.

17 Bulelani Jili, *The Rise of Chinese Surveillance Technology in Africa.*; Tian Shaohui, ed., "International Strategy of Cooperation on Cyberspace," *Xinhuanet*, March 1, 2017, http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm.

sis that demonstrates how state agencies have created social media accounts that flood the internet with approved state media content that seeks to influence public opinion.[18] The state's attempt to control discourses also includes a desire to influence international opinion about China. Adam Segal's in-depth 2020 essay describes how Beijing promotes cyber sovereignty, or *wangluo zhuquan,* as an organizing principle to prevent the flow of online information that threatens domestic political stability, foster technological supremacy and independence from the United States, and counter US global influence.[19]

China increasingly acts in accordance with its policy of cyber sovereignty. In 2017, the government told companies like Tencent, a giant internet-based platform and company, to shut down websites that host content deemed as socially and politically threatening.[20] Weibo, a Chinese social media platform, made changes to its platform in 2018 to allow government censors to tag posts as unsubstantiated rumors.[21] This corporate complicity has made and scaled up surveillance. Likewise, mass surveillance practices in Xinjiang—a matter that Beijing has claimed to be a domestic affair that is beyond international critique—has several corporate actors involved. For instance, H3C has also developed an internet protocol (IP) telephone network for the Xinjiang Public Security authorities.[22] State agencies employ a multisource and layered surveillance system that uses mobile apps, biometric collection, artificial intelligence, and big data, among other means, to monitor and control thirteen million Turkic Muslims.

PUBLIC-PRIVATE PARTNERSHIPS

State procurement of public security technology and innovation policy is driving China's surveillance ecosystem. Surveillance tools scale the party-state's means to conduct surveillance operations on targeted populations that are presumed to be threats to social stability, which result in legal and extralegal means to address the supposed challenge to security. Chinese tech start-ups are seeking to meet the demands of the country's security services. Many cybersecurity firms in China focus on vulnerability research, threat detection, and security intelligence products, which they sell to the state.[23] While these firms mostly rely on Chinese venture capital, they have grown to service clients globally. For example, Pangu Lab is a cybersecurity research team under Pwnzen Infotech that focuses on advanced security research in offensive and defensive cyber capabilities. Pwnzen Infotech has the backing of Qihoo 360, the largest provider of internet and mobile security products in China.[24] Pangu Lab aims to be at the forefront of vulnerability research and to offer insights into the offensive and defensive techniques necessary to combat potential infiltration and exploitation. Pangu Lab founder, Han Zhengguang, is well-known in the Chinese cybersecurity industry for cracking the iPhone.[25] According to Han, Pangu Lab conducts security research on iOS. Moreover, they have discovered hundreds of zero-day security vulnerabilities in mainstream operating systems and popular applications, including Android and other leading mobile operating systems.[26] Pangu Lab, like many new Chinese cybersecurity research firms, has connections to more established tech firms, but also forms

18 Margaret Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*, Princeton: Princeton University Press, 2018.

19 Adam Segal, "China's Vision for Cyber Sovereignty," National Bureau of Asian Research (NBR) Special Report *87* (2020): 85-117, https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/.

20 *Reuters*, "China shuts 128,000 'harmful' websites in 2017 – Xinhua," January 8, 2018, https://www.reuters.com/article/china-internet/china-shuts-128000-harmful-websites-in-2017-xinhua-idINKBN1EX2GO; *People's Daily*, "Last Year's Top Ten 'anti-pornography and Illegal' Cases Announced," January 9, 2018, 2018. 去年"扫黄打非"十大案件公布, http://politics.people.com.cn/n1/2018/0109/c1001-29752891.html; Cyberspace Administration of China, "Opinions on Further Intensifying Website Platforms' Entity Responsibility for Information Content," China Law Translate, September 15, 2021, https://www.chinalawtranslate.com/en/content-responsibility/.

21 See, for example: Yuan Yang, "Beijing Now Able to Flag Weibo Posts as Rumor," *Financial Times,* 2018, https://www.ft.com/content/e21369fe-e0db-11e8-8e70-5e22a430c1ad; and Yang Ziyu, "Weibo Gives Media, Government Power to Quash 'Rumors'," *Sixth Tone*, November 3, 2018, https://www.sixthtone.com/news/1003152/weibo-gives-media%2C-government-power-to-quash-rumors.

22 See, for example: H3C, "Xinjiang Public Security Dedicated Line IP Telephone System Project," 新疆公安专线IP电话系统项目, 2007, https://web.archive.org/web/20210514091329/http:/www.h3c.com/cn/Products___Technology/Products/Router/IP_Voice/Home/Success_Stories/200712/322755_30003_0.htm; Government Procurement of Xinjiang, "Announcement of the Winning Bid for the Upgrade Project of Yili Prefecture Public Security Bureau," 伊犁州公安局党政军链路升级工程项目中标(成交)结果公告, April 1, 2021, https://web.archive.org/web/20210514094226/http:/www.ccgp-xinjiang.gov.cn/ZcyAnnouncement/ZcyAnnouncement4/ZcyAnnouncement3004/KG3KrdvMzw/o/pLznRbnoQ==.html.

23 Margin Research, "The Chinese Private Sector Cyber Landscape," April 25, 2022, https://margin.re/media/the-private-sector-chinese-offensive-cyber-landscape.aspx.

24 Pei Li and Cate Cadell, "At Beijing Security Fair, an Arms Race for Surveillance Tech," *Reuters,* May 30, 2018, https://www.reuters.com/article/ctech-us-china-monitoring-tech-insight-idCAKCN1IV0OY-OCATC.

25 Qi Anxin Group, "Interview| Qian Pangu, the Strongest Guardian of Mobile Security," 专访|奇安盘古，做移动安全的最强守护者, https://www.qianxin.com/news/detail?news_id=2664.

26 Qi Anxin Group, "Interview | Qian Pangu."

part of an ecosystem of smaller firms and start-ups increasingly used by security services to conduct defensive and offensive cyber operations.[27]

Drawing attention to the development of China's cybersecurity industry also means uncovering China's national cyber ambitions, which are partly contingent on the rapidly advancing sector. Companies operating in this space are increasingly at the forefront of their respective fields, and their insights and products are sold to public security services in China.[28] Party-state cyber capacities depend on private-public cooperation, where the state procures interception and intrusion technologies. Unlike the Israeli NSO Group, which claims to only sell products to state actors, Chinese start-ups like Pangu offer products to state and non-state actors. They justify their business model by pointing to the need for cybersecurity, but also how their vulnerability research allows for better software.[29]

Many tech firms tailor their services to meet the demands of China's security services. For example, Chinese companies like Haimeng, Jin Ruan, Ruitec, and Goldeweb have developed products to support the police in predictive policing and the management of targeted populations perceived to be threats to social stability.[30] Arcvideo, like Megvii, also helps equip public security services and has established relationships with the Beijing Criminal Investigation Corps, the Wuhan Public Security Bureau, and six other local security organs.[31] Megvii offers a range of digital solutions, which includes portable video equipment, covert video tracking capabilities, and AI-based analytics software. Western companies like IBM, Intel, Cisco, and Oracle have also provided hardware and software used in China's surveillance network. Oracle sold the software to Liaoning police, which has enhanced their tracking of key objects, events, and people to better identify potential suspects.[32] Scholars have also noted that other Chinese security services—including the Xinjiang police force—use Oracle's data security service.[33]

Chinese leaders have criticized Chinese cyber researchers for doing work outside of China. Indeed, they have implored them to stay in China in order for the government to realize the strategic value of software vulnerabilities.[34] As a result, Zhou Hongyi, the chairman and CEO of Qihoo 360, delisted the company from the New York Stock Exchange in 2016. Qihoo 360 then relisted in Shanghai in 2018 in part to qualify for Chinese government and military contracts.[35] Likewise, Chen Xie, the CEO of Tophant, has claimed that Chinese firms dealing with cloud security, data security, zero trust, and privacy, are more likely to receive contracts and funding from Beijing.[36] Megvii, a partner of Chinese public security authorities, garnered sixty percent of its revenues from smart city contracts in 2020.[37] Additionally, such access to mass population data enables firms like Megvii to better train their algorithms to identify human faces.[38] As such, given the financial incentives to work with the CCP, companies have little interest or limited reasons not to develop and supply technologies for public security officials. Private firms within the technology sector, particularly in the cybersecurity space, are increasingly offering their insights and services to the Chinese government, even as they assert ignorance about their collaborative ventures with the state.[39]

While encouraging the private-public partnerships that have capacitated its cyber power, the Chinese government has also created a more restrictive environment for researchers. Chinese cyber researchers are now effectively banned from participating in international hacking events and competi-

27 Margin Research, "The Chinese Private Sector Cyber Landscape."

28 Winnona DeSombre, Lars Gjesvik, and Johann Ole Willers, *Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets*, *Atlantic Council*, November 8, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/.

29 Pangu Lab, "Pangu Research Lab," https://pangukaitian.github.io/pangu/?lg=en.

30 Jin Ruan Science and Technology, "System Solution for the Construction of the Social Security Prevention and Control System," 社会治安防控体系建设系统解决方案, March 1, 2022, https://archive.ph/Yzlez#selection-381.0-381.16.

31 Arcvideo Tech, "Business Scenario of Security+ AI commercial landing practice," 安防+AI 业务场景驱动的商业化落地实践, https://web.archive.org/web/20220316140031/http://cpsforum.com.cn/15th/Public/Home/images/dh.pdf.

32 Mara Hvistendahl, "How Oracle Sells Repression in China," *The Intercept*, February 18, 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.

33 Weber and Ververis. "China's Surveillance State: A Global Project."

34 See, for example: Cyberspace Administration of China, "Regulations on the Management of Network Product Security Vulnerabilities," 工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知, December 7, 2021, https://archive.ph/9cL8j#selection-713.0-713.41;
Sina Technology, Zhou Hongyi interview, 周鸿祎接受采访, September 12, 2017, https://tech.sina.cn/i/gn/2017-09-12/detail-ifykusey8931658.d.html?vt=4 ;
Patrick Howell O' Neill, "How China Built a One-of-a-Kind Cyber-Espionage Behemoth to Last," *MIT Technology Review*, February 28, 2022, https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/#:~:text=Computing-,How%20China%20built%20a%20one%2Dof%2Da%2Dkind%20cyber,is%20paying%20off%20for%20China.&text=The%20%E2%80%9Cmost%20advanced%20piece%20of,to%20use%20was%20revealed%20today.

35 See, for example: Laura He, "Chinese Internet Security Firm Coming Home from US Valued at US$62bn, Drops 10pc on Shanghai Debut," *South China Morning Post*, February 28, 2018, https://www.scmp.com/business/companies/article/2135098/chinese-internet-security-firm-coming-home-us-valued-us62bn-drops; Elsa Kania and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*, *Center for New American Security*, January 28, 2021, https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

36 Margin Research, 2022. "The Chinese Private Sector Cyber Landscape."

37 Megvii Technology Limited, "IPO prospectus of Megvii Technology Limited," 2020, https://static.sse.com.cn/stock/information/c/202103/bab29f856dc5431d931548cd27304d80.pdf.

38 Bulelani Jili, *The Rise of Chinese Surveillance Technology in Africa*, *Electric Privacy Information Center* (EPIC), May 31, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/.

39 Minghe Hu, "Coronavirus: WeChat, Alipay Deny Helping Government Identify 350,000 Users Who Visited Beijing Food Market," *South China Morning Post*, June 15, 2020, https://www.scmp.com/tech/apps-social/article/3089068/coronavirus-wechat-alipay-deny-helping-government-identify-350000.

tions, which they once dominated.[40] If researchers wish to participate in an international competition, they must ask for permission, which the state rarely grants.[41] Additionally, they must submit their knowledge of software vulnerabilities to security services before attending any international event, giving Chinese security officials a comparative advantage over the United States concerning defensive or offensive hacking operations.

CHINA'S POLITICAL & LEGAL ENVIRONMENT

While direct engagement with the private and public sectors varies between firms, Chinese technology firms operate under a more restrictive legal environment. The 2016 cybersecurity law, 2021 data security law, and 2017 national intelligence law form a series of laws that obligate firms to cooperate with state security organs when requested.[42] Lucero contends that this environment of increasing rigidity has exacerbated a bureaucratic architecture that prioritizes political stability over economic efficiency.[43] Such a move has reportedly resulted "increased centralization and ideological control with fear and paralysis."[44] Accordingly, these rules establish obligations for firms to cooperate with party-state organs by sharing data that is believed to threaten or promote national security interests. Certainly, it appears that these changes in recent years to the Chinese system occur without any legal recourse or administrative means to decline requests made by state security officials.[45]

Pointedly, the shift towards public stability and security as the primary objective of the party-state has led to a more strict environment for corporations. For example, the new intelligence law requires companies to contribute to government intelligence work by sharing their data when requested by security officials. Simultaneously, this change is unfolding alongside progress being made in personal consumer rights in China. Two recent legal statements challenge this view of a more restrictive legal environment.[46] The first is by the Beijing-based Zhong Lun law firm, their statement was submitted to the Federal Communications Commission during its proceedings regarding concerns around Huawei. At this time, Huawei representatives were sending documents to state officials and organs around the world in support of company as a safe and reliable vendor. The "Zhong Lun declaration" discusses statutory laws passed by China's Standing Committee, and crucially contends that the current national cybersecurity law, national intelligence law, and anti-terrorism law do not necessarily require tech firms to cooperate with Beijing or obligate them to offer backdoor access to data. This position is further supported by the second statement made by the British law firm Clifford Chance, which was employed by Huawei to issue a legal opinion supposedly in concurrence with the Zhong Lun declaration. Despite these notable interventions, it is a misstep to simply focus on what Chinese law says about the party-state and what it can demand of firms. It is more salient, I argue, to know what the government can actually do, regardless of what the law says. These interventions on behalf of Huawei assume that Beijing is meaningfully constrained by law.

In this light, scholars, like Donald Clarke, contend these two legal statements offer a misleading conclusion. Indeed, the arguments do not ameliorate US national security concerns.[47] Because while discussing some key features of the intelligence law, the Zhong Lun declaration focuses on a limited subset of mandatory rules and crucially ignores a number of other rules that ask for cooperation. The declaration contends that companies can simply decline state security official requests, and even take action if their legal rights have been violated, companies can pursue remedy through administrative review and through the court system.[48] This view implies that there are judicial checks to state excesses. However, there is as yet no evidence of such a case resulting in an enterprise or citizen receiving this remedy as a result of such violations. These rights asserted in the Zhong Lun declaration—and supposedly respected—are not clearly defined and stated. For these reasons, it is unlikely that the CCP is meaningfully and substantially constrained by law.[49]

The party-state utilizes all-encompassing surveillance practices that mobilize the national CCTV network and cyber researchers to bolster its cyber power. This policy, in part, relies on a more rigid regulatory environment. Strategies, ranging from buying company shares to requiring the

40 Chris Bing, "China's Government Is Keeping Its Security Researchers from Attending Conferences," *Cyberscoop*, March 8, 2018, https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/.

41 See, for example: Cyberspace Administration of China, "Regulations on the Management of Network Product Security Vulnerabilities."

42 Standing Committee, National Intelligence Law, 中华人民共和国国家情报法, China Law Translate, June 27, 2017, https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/.

43 Karman Lucero, "In China, Planning Towards AI Policy Paralysis," New America, January 15, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/china-planning-towards-policy-paralysis/.

44 Karman Lucero, "In China, Planning Towards AI policy Paralysis."

45 Standing Committee, National Intelligence Law.

46 Chen Jihong and Jianwei Fang, "The Zhong Lun Declaration," 2018, https://perma.cc/L9BF-4JNY.

47 Donald Clarke, "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law," for George Washington University Law School, SSRN (March 17, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354211.

48 Chen and Jianwei, "The Zhong Lun Declaration."

49 See, for example: 2013. Susan Lawrence and Michael Martin, "Understanding China's Political System," *Congressional Research Service*, March 20, 2013, https://sgp.fas.org/crs/row/R41007.pdf.

establishment of party committees within firms, allow for state-overseen enterprises. Weber and Ververis contend that the procurement of Chinese surveillance tools may expose Western individuals to privacy risks, as the backdoors used for domestic surveillance in China are exported to foreign markets, unless the tech firms choose to sell a more secure version of public security technologies for international customers.[50] Researchers like Honovich have unearthed and forewarned the various cybersecurity vulnerabilities in Hikvision cameras.[51] Currently, there is no empirical evidence from the ground that demonstrates the systematic coordination between Beijing and Hikvision in the purposeful theft of personal data. This concern, however, remains an escalating vulnerability. For example, African Union's (AU) staffers discovered that China-based hackers, Bronze President, had "rigged a cluster of servers in the basement of an administrative annex to steal surveillance videos from across the AU's sprawling campus in Addis Ababa, Ethiopia's capital."[52] As such, it is paramount to promote and advance supply chain integrity given the real risk for designed backdoors in hardware or software.

THE GLOBAL PUSH FACTORS OF CHINA'S SURVEILLANCE TOOLS

In addition to aiming to realize cyber power ambitions at home, China's drive for tech and cybersecurity leadership extends globally. Research from Steven Feldstein found that Chinese companies supply AI surveillance technology in sixty-three countries, thirty-six of which have signed onto China's Belt and Road Initiative.[53] Accordingly, these technologies, developed for the sake of the GSP program, are now exported across the globe. Much of the establishment of surveillance programs is through third parties and subsidiaries of Chinese companies.[54] To be clear, the selling of digital monitoring tools and cyber capability technologies is not unique to Chinese vendors. Many non-Chinese enterprises, including Western firms, are involved in the sale of cyber capabilities and surveillance tools.[55] This focus on Chinese technology does not aim to obfuscate the broader transnational market of digital surveillance tools, which indubitably includes American actors. Rather, the paper illustrates how the procurement of Chinese technology appears to be a result of both Chinese supply and local demand factors. What is unique about Beijing is how it goes about promoting public security systems in the Global South.

The party-state utilizes multilateral institutions like the BRICS (Brazil, Russia, India, China, and South Africa), an emerging markets group, the Belt and Road Initiative, and the Forum on China-Africa Cooperation (FOCAC) to promote its surveillance platforms across the Global South.[56] Particularly, through FOCAC and the China-Africa Defense Forum, China has signed resolutions to increase cooperation in areas like counterterrorism, safe city projects, and cybersecurity.[57] China also supplements this promise with commitments to offer finance, technical assistance, and training to African governments on topics ranging from digital forensic techniques to cybersecurity.[58] These efforts reflect Beijing's aims to influence international norms through multilateral institutions, which further normalize and seek to legitimize its surveillance practices at home.

These trends are particularly prevalent in a handful of African countries. The China-Africa Internet Development and Cooperation Forum held in August 2021 offers an example of China's aims to implement a joint China-Africa partnership to advance digitization and promote its notion of cyber sovereignty.[59] Additionally, Beijing's efforts to shape cybersecurity standards and regulations in part garner legitimacy from its digital development aid and projects in Africa.

The proliferation of surveillance technology has, unsurprisingly, had clear effects on law enforcement practices. For example, the use of Chinese surveillance technologies in South Africa has risen largely in tandem with police-to-police training and cooperation—like the 2018 South African delegation tour of Shanghai's Public Security Bureaus to learn how to improve policing techniques.[60] Similarly, the Botswana Police Services enlisted Huawei to install 500

50 Weber and Ververis. "China's Surveillance State: A Global Project."

51 John Honovich, "Hikvision Has 'Highest Level of Critical Vulnerability,' Impacting 100+ Million Devices," IPVM, September 20, 2021, https://ipvm.com/reports/hikvision-36260.

52 Raphael Satter, "Exclusive-Suspected Chinese Hackers Stole Camera Footage from African Union – Memo," *Reuters*, December 16, 2020, https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idINKBN28Q1DB.

53 Steven Feldstein, *The Global Expansion of AI Surveillance*, *Carnegie Endowment for International Peace*, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

54 Weber and Ververis. "China's Surveillance State: A Global Project."

55 See, for example: Feldstein, *The Global Expansion of AI Surveillance"*; and Walton, *China's Golden Shield*; Bulelani Jili, *The Rise of Chinese Surveillance Technology in Africa.*

56 Bulelani Jili, *The Rise of Chinese Surveillance Technology in Africa.*

57 Michael Kovrig, *China Expands its Peace and Security Footprint in Africa, International Crisis Group*, October 24, https://www.crisisgroup.org/asia/north-east-asia/china/china-expands-its-peace-and-security-footprint-africa; Yao Jianing, ed., "China to Host First China-Africa Defense Forum," China Daily, June 1, 2018, http://eng.mod.gov.cn/news/2018-06/01/content_4815796.htm; Yin Hang, "Wei Fenghe Meets with Representatives of the First China-Africa Defense and Security Forum," 魏凤和会见首届中非防务安全论坛代表, Ministry of National Defense People's Republic of China, press release, July 10, 2018, http://www.mod.gov.cn/topnews/2018-07/10/content_4818896.htm.

58 Heidi Swart, "Joburg's New Hi-Tech Surveillance Cameras: A Threat to Minorities That Could See the Law Targeting Thousands of Innocents," *Daily Maverick*, September 28, 2018, https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/.

59 State Council Information Office, "China and Africa in the New Era: A Partnership of Equals," White Paper, November 26, 2021, http://english.scio.gov.cn/whitepapers/2021-11/26/content_77894768_4.htm; Li Zhengwei, "The China-Africa Internet Development and Cooperation Forum Held," 中非互联网发展与合作论坛举办, Guangming, August 24, 2021, https://m.gmw.cn/baijia/2021-08/24/35106965.html.

60 Li Wanyi, "Delegation of South African Parliament Police Committee Visits Shanghai." 南非议会警察委员会代表团访问上海, *Jiefang Daily*, October 4, 2107, http://shzw.eastday.com/shzw/G/20171014/u1a13342865.html.

surveillance cameras in Gaborone and Francistown, including inside commercial buildings, as part of a two-year deal with the company's Safe City Project.[61]

Utilizing ICT systems and services, the Kenyan government aims to foster a safe city project where digital surveillance systems are incorporated into Nairobi's city infrastructure to optimize development and security ambitions. Working with Huawei and Safaricom, the government established the first African safe city in Nairobi, which connected 200 high-definition traffic surveillance cameras and 1800 high-definition cameras.[62] What is more, these integrated platforms include a high-speed private broadband network and command center for the National Police Service, which supports over 9000 police officers in 195 police stations. Through these digital surveillance systems, the safe city platform aims to meet several service delivery demands, including real-time surveillance, evidence collection, and video browsing that purportedly support accelerated police response, recovery missions, and crime prevention.

Namely, Huawei's safe city platforms are promoted as solutions for crime and rising terroristic threats. Governments in the Global South are procuring their services on the grounds to expand their surveillance capacities to address growing trepidations around crime and terrorism. Yet, in part, due to the dearth of publically available data, the benefits of the safe city platforms are difficult to verify and appear grossly overstated by Huawei.[63] According to them, crime rates decreased by 46 percent in areas supported by their platform in 2014 to 2015.[64] However, the Eastern African nation's police services report lower reduction rates in crime during those years.[65] Unfortunately, Nairobi and Mombasa, the two cities supported by Huawei's safe city platforms have seen an increase in reported crime between 2017 and 2018.

While China's surveillance system is confined to its national borders, the companies that make its surveillance state possible are now actively selling their tools abroad. Given the growing influence of these firms and the spread of digital surveillance tools, scholars like Feldstein contend that the party-state is not only supporting the proliferation of digital public security technologies, but also enabling the rise of authoritarianism. This kind of argument, I contend presumes a coordinated effort between the party-state and technology firms as a way to export Chinese norms and repressive practices overseas. Indeed, while this argument draws attention to Chinese push factors, it ignores local demand features. Moreover, it lacks robust empirical evidence from the ground to establish the consequences of Beijing's promotional efforts.[66] For instance, the use of surveillance tools in Kenya, and across Africa, is supposedly a means to improve service delivery and law enforcement. Accordingly, technologies are adopted in order to address such structural and political challenges.[67] The extent of technology and regulation diffusion, and indeed whether it undercuts civil liberties, is greatly contingent on the political and legal environment of the recipient African country.

We are yet to observe party-state solutions for public instability being promoted in the Global South by Beijing. Currently, Huawei's safe city technologies are marketed as solutions to local concerns around crime and terror. Indeed, China's active "push" of domestic surveillance technologies is a critical force in shaping African surveillance ecosystems. As such, highlighting how Beijing leverages local demand factors to advance its own geopolitical interests should not be viewed as an attempt to downplay African state agency in determining the application of public security technologies. For these reasons, Africa, and other regions, must be carefully studied both on their terms and as well as places enmeshed in wider relations. The companion report to this issue brief will focus on the key "pull factors" from African countries and their significance for US interests. More to the point, we must engender even-handed studies that demonstrate the degree to which local agency is shaping relations between Africa-China while also underscoring the interplay between local political commitments and Chinese state ambitions.[68] This more proportional analysis seeks to expand our understanding and offers insights into the perennial consequences of Beijing's growing cyber power on the global stage.

61 Frank Hersey, "Digital ID in Africa This Week: Biometrics for Tea Workers, Financial Inclusion with a Thumbprint," *Biometric Update*, August 23, 2019, https://www.biometricupdate.com/201908/digital-id-in-africa-this-week-biometrics-for-tea-workers-financial-inclusion-with-a-thumbprint.

62 See, for example: Bulelani Jili, "Chinese Surveillance Tools in Africa," *China, Law, and Development,* No. 8, June 30, 2020, https://cld.web.ox.ac.uk/files/finaljilipdf; Huawei, "Video Surveillance as the Foundation of 'Safe City' in Kenya," *Huawei Industry Insights*, 2019, https://www.huawei.com/us/industry-insights/technology/digital-transformation/video/video- surveillance-as-the-foundation-of-safe-city-in-kenya; Steven Feldstein, "Testimony Before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa," *US-China Economic and Security Review Commission*, May 8, 2020, https://www.uscc.gov/sites/default/files/2020-06/May_8_2020_Hearing_Transcript.pdf.

63 Rachel Bernstein et al, "Expanding Engagement: Perspectives on the Africa-China Relationship," 46.

64 See, for example: Huawei, "Huawei Hosts Safe City Summit in Africa to Showcase Industry Best Practices," news release, October 17, 2016, https://www.huawei.com/us/news/2016/10/safe-city-summit-africa; Integrated Solutions, "Safe City Summit in a Safe City," Hi-Tech Security Solutions, February 2017, http://www.securitysa.com/56445n.

65 National Police Service, Annual Crime Report 2018, National Police Service of the Republic of Kenya, accessed April 25, 2022, http://www.nationalpolice.go.ke/crime-statistics.html.

66 Bulelani Jili, "Chinese Surveillance Tools in Africa."

67 Bulelani Jili, "Africa: Regulate Surveillance Technologies and Personal Data," Nature, 607, No. 7919 (2022), 445–448.

68 Bulelani Jili, *The Rise of Chinese Surveillance Technology in Africa.*

AUTHOR

Bulelani Jili is a non-resident fellow at the Atlantic Council's Cyber Statecraft Initiative. His research interests include information and communications technology development, Africa-China relations, algorithmic decision-making, cybersecurity, internet governance, and privacy law. He is also a Visiting Fellow at Yale Law School, a Cybersecurity Fellow at the Harvard Kennedy School, Scholar-in-residence at the Electronic Privacy Information Center, Research Associate at Oxford University, and Meta Research PhD Fellow at Harvard University. He can be reached at bulelanijili@g.harvard.edu.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
*Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Jarosław Grzesiak
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Umer Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Gil Tenzer
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of September 12, 2022