The Heritage Foundation

BACKGROUNDER

No. 3476 | MAY 20, 2020

DOUGLAS AND SARAH ALLISON CENTER FOR FOREIGN POLICY

Government Buildings in Africa Are a Likely Vector for Chinese Spying

Joshua Meservey

KEY TAKEAWAYS

Beijing likely has better surveillance access to Africa than anywhere else by having built or renovated at least 186 African government buildings.

Beijing likely uses surveillance to, among other things, advantage its companies competing for contracts, spy on U.S. officials, and influence African officials.

The U.S. should try to complicate Beijing's surveillance of an important continent as part of a strategic response to the CCP's effort to reshape the global order.

The Chinese Communist Party's (CCP's) two-decade-long blitz of engagement in Africa has likely given it extensive surveillance access to the continent. Chinese companies, all of which are legally obliged to help the CCP gather intelligence, have built at least 186 government buildings in Africa and at least 14 sensitive intra-governmental telecommunication networks. Beijing has also donated computers to at least 35 African governments.

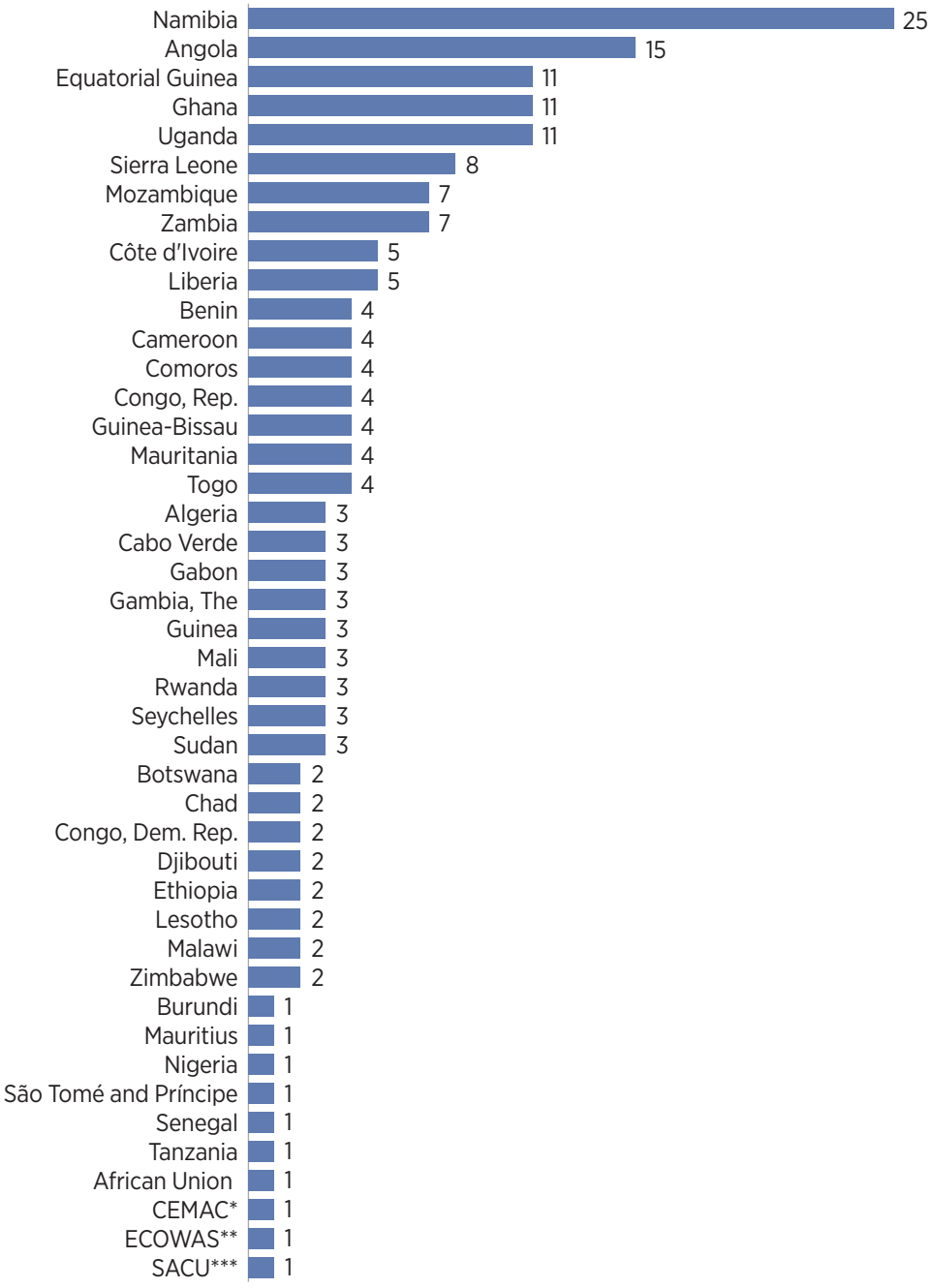
The wealth of information the CCP probably gathers in Africa presents four primary dangers for the U.S., as that information could be used to:

1. Facilitate Beijing's influence operations on the continent;

2. Recruit intelligence assets at senior levels of African governments;

CHART 1

Chinese-Constructed Government Buildings Across Africa

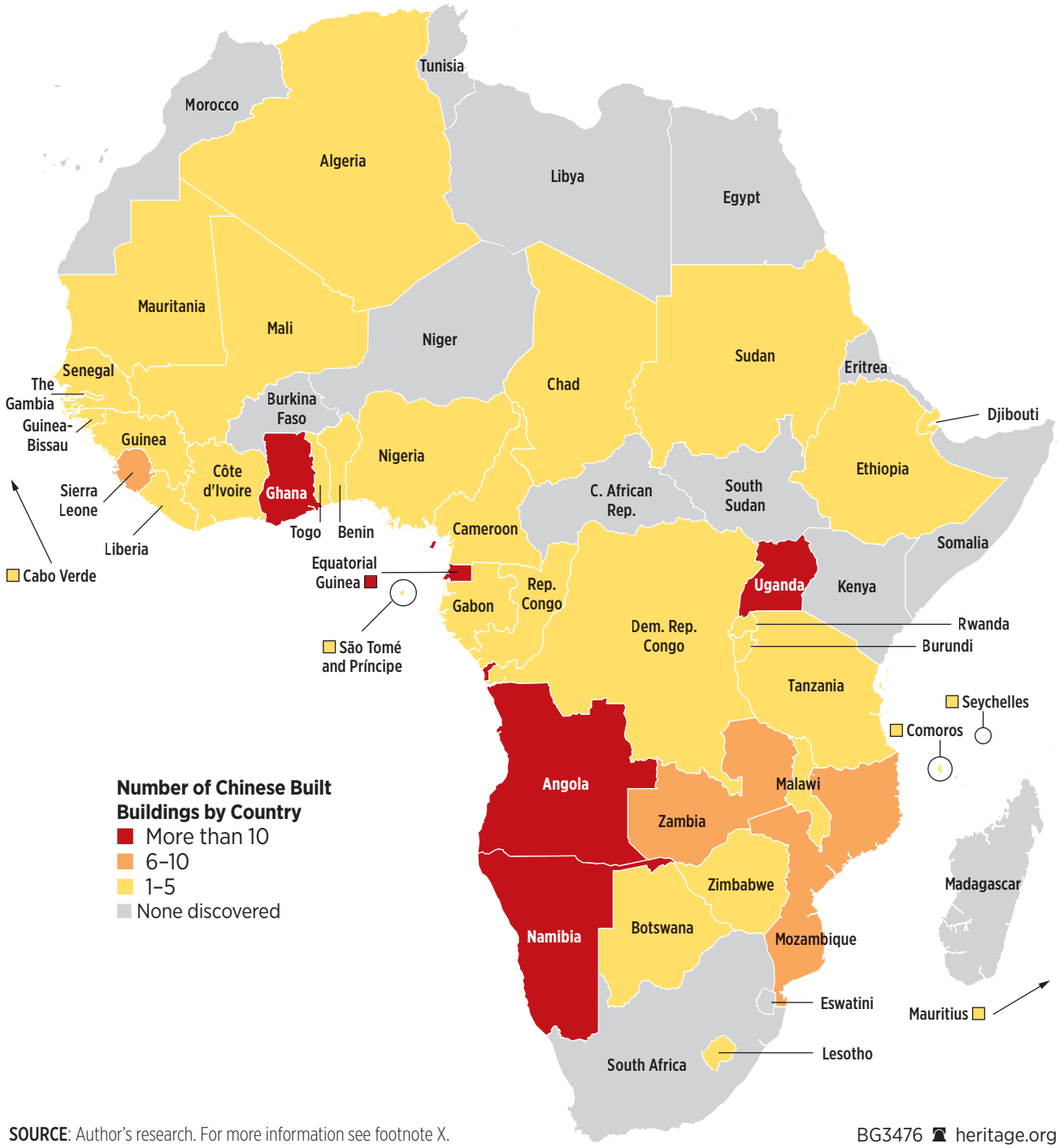


* Central African Economic and Monetary Community
** Economic Community of West African States
*** Southern African Customs Union
SOURCE: Author's reaserch. For more information, see footnote 3.

BG3476 heritage.org

MAP 1

Chinese-Constructed Government Buildings Across Africa



SOURCE: Author's research. For more information see footnote X.

BG3476 heritage.org

3. Gain insight into U.S. diplomatic strategies, military counterterrorism operations, or joint military exercises; and

4. Disadvantage U.S. companies competing against Chinese firms for Africa's growing economic opportunities.

While the longer-term challenge of Beijing's extensive influence in Africa can only be addressed by a comprehensive U.S. strategy, Washington can take a number of immediate steps to complicate Chinese surveillance access to Africa. Those steps should include working to understand the nature of Chinese surveillance and how it contributes to Beijing's influence operations on the continent, educating U.S. companies on the risks, and training its officials on techniques to protect themselves from Beijing's eavesdropping.

At Least 186 Buildings

In January 2018, the French newspaper *Le Monde* reported that servers installed by the Chinese telecommunications giant Huawei in the African Union (AU) headquarters were daily uploading their content to servers based in Shanghai, China. An inspection of the building—built by the state-owned China State Construction Engineering Corporation—also uncovered listening devices hidden throughout the building.[1] Three days later, the *Financial Times* newspaper confirmed *Le Monde*'s story.[2]

Beijing's eavesdropping on African government buildings likely extends well beyond the AU headquarters. Since 1966, Chinese companies have constructed or renovated (or both) at least 186 such buildings.[3] In fact, at least 40 of Africa's 54 countries have a government building constructed by a Chinese company. Given the difficulty of gathering comprehensive data on independent China's nearly seven decades of engagement with Africa, these numbers are almost certainly an undercount.[4]

A Tempting Opportunity for the CCP

There are compelling reasons to believe—beyond the fact that it has already done so with the AU headquarters—that the CCP is using the opportunity afforded it by Chinese companies constructing government buildings to gather intelligence.[5] Doing so would be in keeping with Beijing's extensive use of espionage and other malpractice to gain an economic advantage. A 2017 report branded China "the world's principal IP infringer,"[6] while a

TEXT BOX 1

"Private" Chinese Companies Do Beijing's Bidding

Chinese law requires that Internet companies cooperate with the Chinese government to reduce users' anonymity. Chinese government documents reveal that data collected from smart city technology is sent back to China for analysis that helps the CCP in its public diplomacy efforts.[1]

According to a U.S. Department of Defense report, Huawei and another Chinese firm, Boyusec, were constructing products that would assist Chinese intelligence gathering.[2] A Chinese SOE, China Telecom, allegedly equipped a Chinese government hacking unit with fiber optic infrastructure that could facilitate the unit's activities.[3] In 2017, the U.S. Army banned the use of drones manufactured by Chinese company DJI, one of the world's largest producers of drones. The Army charged that DJI was sharing information its drones collected with the Chinese government, something the company admitted to doing with data it collected in China and Hong Kong. A separate assessment by U.S. Immigration and Customs Enforcement made a similar claim, as did the U.S. Department of Homeland Security in 2019.[4]

A pattern has also emerged of widespread backdoors in Chinese technology companies' products that they are slow or refuse to fix. A cybersecurity firm's June 2019 analysis revealed that more than half the Huawei devices it tested had at least one possible backdoor that could allow unauthorized users access to the devices—a far higher rate of vulnerability than devices from other companies.[5] Similarly, devices manufactured by Chinese company Hikvision, a company in which the Chinese government has a controlling stake[6] and that is one of the world's leading producers of CCTV cameras, had frequent, critical security vulnerabilities the company was slow, if not completely unwilling, to fix.[7] A Chinese industry insider alleged in a 2018 report that the Chinese government could at any time access the information from any video surveillance company in the Chinese market.[8]

Furthermore, the University of Toronto found "surveillance mechanisms" in Chinese social media platforms, while in 2017 the Indian government forbade its armed forces from using a variety of

1. "Episode 38: Beyond South China Sea Tensions, Part Two; The CCP Vision and the Future of Chinese History," Defense One Radio, February 19, 2019, https://www.defenseone.com/ideas/2019/02/ep-38-beyond-south-china-sea-tensions-part-two-ccp-vision-and-future-chinese-history/154946/ (accessed February 20, 2020).
2. Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service," *Washington Free Beacon*, November 29, 2016, https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/ (accessed February 20, 2020).
3. "A Transactional Risk Profile of Huawei," RWR Advisory Group, February 13, 2018, https://www.rwradvisory.com/wp-content/uploads/2018/04/RWR-Huawei-Risk-Report-2-13-2018.pdf (accessed February 20, 2020).
4. David Shortell, "DHS Warns of 'Strong Concerns' That Chinese-Made Drones Are Stealing Data," CNN, May 20, 2019, https://www.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html (accessed February 20, 2020), and Paul Mozur, "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say," *New York Times*, November 29, 2017, https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html (accessed February 20, 2020).
5. *Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.*, Finite State, https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf (accessed February 20, 2020).
6. Heidi Swart, "Video Surveillance and Cybersecurity (Part Two): Chinese Cyber Espionage Is a Real Threat," *Daily Maverick*, June 26, 2019, https://www.dailymaverick.co.za/article/2019-06-26-video-surveillance-and-cybersecurity-part-two-chinese-cyber-espionage-is-a-real-threat/ (accessed February 20, 2020).
7. Heidi Swart, "Visual Surveillance and Weak Cyber Security, Part One: When Cameras Get Dangerous," June 13, 2019, https://www.dailymaverick.co.za/article/2019-06-13-visual-surveillance-and-weak-cyber-security-part-one-when-cameras-get-dangerous/ (accessed February 20, 2020).
8. Matthew Robertson, "The Danger of AI Collaboration With China," China Change, October 11, 2018, https://chinachange.org/2018/10/11/the-danger-of-ai-collaboration-with-china/ (accessed February 20, 2020).

Chinese-developed apps because of those apps' potential security vulnerabilities. Included in the ban was WeChat,[9] the messaging app giant from which the CCP has admitted to retrieving deleted messages.[10]

These companies enjoy close ties to the Chinese government that has constructed the world's most comprehensive surveillance state,[11] and they are *compelled by law* to help Beijing collect intelligence. It is reasonable to assume the Chinese government is aware of the vulnerabilities in some of China's largest "private" companies' products and is willing to use them, if it has not already done so.

9. Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy*, Vol. 30, Number 1 (January 2019), https://muse.jhu.edu/article/713722?_cldee=am9zaHVhLm1lc2VydmV5QGhlcml0YWdlLm9yZw%3d%3d&recipientid=contact-721553162a85e81180f3005056a456ce-0958f93837f647beaa934047a7e670ea&esid=4f0fde16-2915-e911-80fa-005056a456ce (accessed February 20, 2020).
10. Aleksandra W. Gadzala, "Global Reach: Information Is a Weapon," *Democracy: A Journal of Ideas*, No. 52 (Spring 2019), https://democracyjournal.org/magazine/52/global-reach-information-is-a-weapon/ (accessed February 20, 2020).
11. Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers," *New York Times*, December 17, 2019, https://www.nytimes.com/2019/12/17/technology/china-surveillance.html (accessed February 20, 2020).

recent U.S. Trade Representative investigation found that the U.S. loses at least $50 billion every year to unscrupulous Chinese activity.[7] The FBI found that China committed 95 percent of the cases of economic espionage reported by 165 American firms,[8] while a German firm estimated that around 20 percent of Germany's $61 billion in annual losses to espionage were due to Chinese attacks.[9]

There is also the attractiveness of the opportunity: Chinese companies have built, expanded, or renovated at least 24 presidential or prime minister residences or offices; at least 26 parliaments or parliamentary offices; at least 32 military or police installations; and at least 19 ministries of foreign affairs buildings. Having surveillance access to these buildings is an extraordinary opportunity for the CCP to gather intelligence directly from the highest levels of African governments. The opportunity is so enticing, in fact, that Beijing may have financed and constructed some of the buildings to improve its surveillance of certain governments.

Furthermore, most of the Chinese companies that built these structures are probably state-owned enterprises (SOEs), given that SOEs undertake a large majority of China's foreign construction projects.[10] SOEs, as implements of the CCP, must obey its orders,[11] though in practice it does not matter whether an SOE or private Chinese company was involved. Chinese law compels both to assist the Chinese government in collecting intelligence,[12] and there are many examples—in addition to Huawei's role in the AU bugging—of ostensibly private Chinese companies engaging in surveillance and espionage on behalf of the Chinese government.

Finally, Beijing's engagement blitz in Africa for the past two decades demonstrates how important the CCP considers Africa, which presumably makes the continent worth surveilling. Every year, the Chinese Foreign Minister includes Africa in his first overseas trip; from 2008 to 2018, in fact, senior Chinese leadership visited the continent 79 times.[13] In two decades, China–Africa trade increased fortyfold,[14] and China has dramatically increased its military cooperation, investment, and public diplomacy efforts on the continent as well.[15]

The Chinese state also likely has the capacity to parse the high volume of data they would collect in such a surveillance operation. China is one of the world leaders in artificial intelligence technology that is well suited to sifting immense amounts of data. In places like Xinjiang, Beijing already uses artificial intelligence and other technologies to maintain virtually constant surveillance of the approximately 11 million Uighurs living there. There are reports of Chinese hacking groups utilizing tools that filter short message service (instant messaging) traffic—a staggering amount of data—to track individuals and keywords for later scrutiny.[16]

The Problem for the U.S.

CCP surveillance of Africa poses a number of problems for the U.S. First, if Beijing's surveillance blankets the most sensitive offices of some African governments, the CCP can gain insights into leaders' personalities, habits, and preferences that would help Beijing tailor its influence campaigns directed at senior leaders.

Building such influence is important to achieving the CCP's goal of becoming an unassailable global power. If it succeeds, the U.S.'s own global power would diminish, given the incompatibility of the American and Chinese political systems. CCP leadership believes political warfare is—as Chairman Mao put it—a "magic weapon,"[17] and the People's Liberation Army may have the world's only intelligence agency dedicated to running overseas influence operations.[18] Chinese President Xi Jinping has intensified China's use of the "magic weapon" to influence and intimidate countries around the world,[19] including developed, democratic nations.[20]

The effort is paying dividends in Africa. The governments there are usually reliable Chinese allies in international forums. In 1971, African states provided more than one-third of the votes that transferred the U.N. Security Council seat from Taiwan to China.[21] In 1989, Africa helped Beijing weather a period of international isolation after the Chinese military massacred unarmed protesters

in Tiananmen Square.[22] Today, African governments are helping whitewash Beijing's large-scale human rights abuses in Xinjiang[23] and have helped Chinese nationals win leadership of influential international organizations.[24]

A second, and related, problem for the U.S. is that Chinese surveillance could enable Beijing to recruit highly placed assets within African governments. If the CCP collected embarrassing or harmful information on an African official, it could blackmail cooperation from him or her. Or surveillance could gather other information, such as a recruitment target's financial situation, which could facilitate recruitment. Having Chinese assets peppered throughout governments on an increasingly strategic continent is an obvious problem for the United States.[25]

Third, Beijing's spying could pick up sensitive conversations between senior American officials and their African counterparts. That would include U.S. military officers who frequently meet with senior African officials to discuss joint military exercises, counterterrorism operations, and other activities it would be best not to divulge to a competitor like China. A September 2019 report detailed how the Chinese government conducted just that sort of surveillance operation against foreign officials by hacking telecommunications companies in Asia.[26]

Fourth, American businesses competing for the continent's lucrative opportunities may suffer harm. U.S. companies would be at a disadvantage if any negotiating strategies, bids, or business processes they might discuss with an African leader were known by a Chinese competitor. This includes U.S. tech companies—long a prized target of Chinese commercial espionage—that are increasingly active in Africa. The Chinese government's practice of supporting its companies—particularly its "national champions" such as Huawei—through anticompetitive means, including economic espionage, suggests it would pass any commercially useful information it gleaned to a Chinese company.[27]

The risk to U.S. companies is perhaps higher than it has ever been. A significant part of China's technological progress is built from technology and intellectual property stolen or coerced from the West, especially the United States.[28] In recent years, the CCP has escalated its theft of U.S. commercial secrets[29] as President Xi Jinping seeks to achieve the ambitious goals laid out in his Made in China 2025 strategy, lessen Chinese dependence on Western technologies, and gain leverage against Washington in the ongoing trade war. The existential nature of the task suggests Xi will use every means at his disposal, including whatever surveillance capabilities China has in Africa.

The Problem for Africa

African countries have yet to develop the sort of cutting-edge technologies the Chinese government and its companies target, and so cannot suffer the same losses that the U.S. and many other countries have from Chinese theft. Yet there is a dynamic, emerging technology industry in Africa. If it produces technology the Chinese government or one of its companies covet, that technology would be at great risk of being poached. Chinese companies have already done this in West Africa, enabling them to dominate the region's wax-print fabric industry and force out indigenous competitors.[30]

The bigger economic risk for African governments is that they frequently negotiate with the Chinese government, its banks, and its companies, as China is by far the largest bilateral lender to the continent,[31] and Chinese companies dominate Africa's lucrative infrastructure construction sector.[32] Chinese eavesdropping could gain valuable information on African governments' negotiating strategies, competitors' bids, and other relevant information: There are reports of Chinese hackers stealing just that sort of information in other parts of the world.[33]

As noted earlier, it is also possible Chinese surveillance of such buildings could collect damaging or embarrassing information about a country's senior leadership. That material could be used as leverage to ensure African leaders' pliability, to the harm of the countries they represent.

It Is Not Just Buildings

There are other elements of the counterintelligence problem the U.S. faces in Africa. Huawei has built more than 70 percent of the 4G telecom networks in Africa[34] and is proceeding with plans to deploy 5G networks on the continent.[35] Huawei, ZTE (another Chinese telecommunications giant), and other Chinese telecoms have built and/or equipped at least 14 government networks, including dedicated military and police telecoms systems.[36]

Furthermore, the Chinese government has donated office equipment, including computers, to at least 35 African governments over the years.[37] It is difficult to believe the Chinese government did not take the opportunity to make those computers vulnerable to Chinese spying before gifting them.

African leaders are likely aware of at least some of the vulnerabilities such Chinese gifts bring—and are either too far under the influence of Beijing to resist, believe that Beijing's surveillance does not matter,[38] or that they can manage the challenge. A Zambian government official said that his government had "changed the locks" after Huawei finished constructing

Zambia's national data center that processes and stores all government data.[39] Yet intelligence officials from some of the world's most sophisticated cyber powers such as the U.S., the U.K., Japan, and Germany do not believe their countries can adequately protect against the intelligence threat posed by Huawei-built systems.[40] If those countries, with their extensive budgets and advanced capabilities cannot, it is unlikely African countries with far fewer resources can.

Steps for Addressing a Serious Problem

Protecting U.S. interests requires an American response as determined and holistic as the CCP's efforts to reshape the global order and should include, whenever possible, pushing back against damaging Chinese activity *everywhere* it occurs.

In Africa, that means not simply acquiescing to broad Chinese surveillance access to the continent. For the foreseeable future, it will be impossible to fully protect against Chinese spying in Africa, as Beijing's access there is enabled by its successful, long-running influence-building campaign on the continent. The problem that reality poses for American interests can only be addressed by a comprehensive U.S. strategy.[41]

Yet Washington can take a number of immediate steps to complicate Chinese surveillance in Africa, including the following:

- **Assume that all communication with African government counterparts is vulnerable to Chinese exploitation.** This should be the baseline assumption for all American officials operating in Africa.

- **Develop government-wide counterintelligence protocols and training for operating in Africa.** Every U.S. official visiting or posted to Africa should receive a standardized training on techniques for combatting Chinese surveillance. Such training should be supplemented with country-specific information on the unique risks different countries pose. It will be impossible to always fully defeat Chinese surveillance in Africa, but the U.S. can and should make it harder.

- **Task all U.S. embassies in Africa with developing a digital hygiene outreach program as a key part of their host-country engagement.** Embassies should offer assistance to host-country governments with protecting their vital digital networks and

infrastructure. This could include best-practices training or technical support for sweeping networks or buildings. If a government is interested in assistance beyond the embassy's capabilities, the embassy could solicit help from other U.S. agencies with the requisite expertise.

- **Map potential vectors of Chinese surveillance and influence.** U.S. embassies and other U.S. agencies active on the continent should document potential entry points for Chinese surveillance, such as Chinese-built government buildings and telecommunications networks. That information should be compiled and made accessible to policymakers to better understand the contours of Chinese engagement in a particular country or region, the risks it poses, and possible countermeasures.

- **Educate U.S. companies on the surveillance risks in specific countries.** A standard part of any briefing a U.S. embassy gives to American companies interested in or already operating in a particular African country should include best practices for protecting themselves as much as possible from Chinese surveillance. The embassy should share any unclassified, relevant data with American companies operating in the country.

- **Expect little help—and perhaps even resistance—from some African states.** Given how adroitly the CCP has built influence in Africa and the many examples of African countries fearing to defy Beijing, the U.S. should not expect these governments to offer much assistance in ameliorating America's counterintelligence problem in Africa. Some, if asked, or in an attempt to curry CCP favor, may even actively collaborate with Beijing to hinder American efforts to protect its interests on the continent.

A Broader Challenge

Africa may be the most permissive region on earth for Chinese spying and espionage. Beijing and its companies have enormous sway over many African governments, whether because of personal inducements to African leaders[42] or because of African countries' economic enmeshment with China—something Beijing increasingly uses as a weapon.[43] This suggests some African governments might hesitate to be appropriately skeptical of Chinese intentions.

African countries also have limited cyber-defense capabilities. All of this is in addition to the extraordinary potential for surveillance access the CCP has from the computers it donates to African governments and the Chinese companies building government buildings and sensitive (including intra-governmental) communications networks.

The CCP's surveillance of Africa is only one part of the much larger challenge an increasingly globally assertive China poses for the U.S. Yet it contributes to the problem, and Washington should respond. It can start by working to understand the nature of Chinese surveillance and how it contributes to Beijing's influence operations on the continent, educating U.S. companies on the risks, and training its officials on techniques to complicate Beijing's information gathering on the continent.

Joshua Meservey is Senior Policy Analyst for Africa and the Middle East in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

APPENDIX TABLE 1

Chinese-Constructed Government Buildings Across Africa (Page 1 of 7)

Building Name	City	Date Completed/Delivered
Algeria		
Constitutional Court	Algiers	—
Ministry of Foreign Affairs	Algiers	July 3, 2005
Republican Guard barracks	Lido	—
Angola		
Academy of Social Sciences and Technology	Luanda	May 21, 2019
Cabinda Provincial Government Building	Cabinda	—
Construction Ministry	Luanda	—
Funda Residential Zone	Luanda	—
Higher Institute of Foreign Affairs complex	Kilamba	January 31, 2019
Luanda Provincial headquarters	Luanda	—
Ministry of Education	Luanda	—
Ministry of Finance	Luanda	June 27, 2005
Ministry of Foreign Affairs	Luanda	—
Palace of Justice	Luanda	July 2012
Presidential Palace	Luanda	—
Public Water Company headquarters	Luanda	April 3, 2017
Quisseque Communal Administration	Quisseque	—
Regional Geological Institute of Angola headquarters	Lubango	January 2016
Televisão Pública de Angola (TPA) Production and Transmission Centre	Luanda	—
Benin		
Cotonou Administrative Towers	Cotonou	July 31, 2013
Cotonou Congress Center	Cotonou	July 31, 2003
Ministry of Foreign Affairs and African Integration	Cotonou	—
Ministry of Industry Trade and Promotion of Employment	Cotonou	—
Botswana		
Botswana High Court and Court of Appeals	Gaborone	—
Botswana Police Service Forensic Science Laboratory	Gaborone	July 2019, Probable
Burundi		
Government Complex	Mutimbuzi	February 14, 2019
Cabo Verde		
Government Palace	Praia	—
National Assembly	Praia	October 30, 1985
Presidential Palace	Praia	—

APPENDIX TABLE 1

Chinese-Constructed Government Buildings Across Africa (Page 2 of 7)

Building Name	City	Date Completed/Delivered
Cameroon		
National Congress Hall/Palais des Congrès/ Yaounde Conference Center	Yaounde	May 12, 1982
Original National Assembly	Yaounde	—
New National Assembly	Yaounde	Ongoing
Presidential Palace/Unity Palace/Palais de l'Unité	Yaounde	August 1982
Chad		
Original National Assembly	N'Djamena	—
New National Assembly	N'Djamena	November 2013
Comoros		
People's Palace (National Assembly)	Moroni	June 7, 2005
Presidential Office in Anjouan	Anjouan	July 5, 2005
Presidential Office in Moheli	Moheli	July 5, 2005
The Comoros Radio and Television Service (Office de Radio et Télévision des Comores)	Moroni	September 26, 2002
Congo, Dem. Rep.		
Foreign Ministry Conference Room	Kinshasa	January 8, 2004
People's Palace/Palais du Peuple/ National Assembly/Parliament	Kinshasa	1979
Congo, Rep.		
Constitutional Court building	Location Uncertain	2009
New Ministry of Foreign Affairs	Brazzaville	—
National Petroleum Company of Congo (SNPC) office building	Brazzaville	November 2007
Parliament building	Brazzaville	Ongoing
Côte d'Ivoire		
Hôtel des Parlementaires	Yamoussoukro	2007
Ministry of Foreign Affairs Conference Hall	Yamoussoukro	2007 or 2008, probable
Ministry of Foreign Affairs office building	Yamoussoukro	November 2017
Parliamentary Complex	Yamoussoukro	May 2006
Presidential Palace	Yamoussoukro	—
Djibouti		
Foreign Ministry headquarters	Djibouti	2003, Probable
People's Palace Conference Center	Djibouti	1983
Equatorial Guinea		
Bata Ministry of Foreign Affairs building	Bata	July 2009
Equatoguinean Television	Malabo	January 2, 2007

APPENDIX TABLE 1

Chinese-Constructed Government Buildings Across Africa (Page 3 of 7)

Building Name	City	Date Completed/Delivered
Equatorial Guinea *(cont.)*		
Equatorial Guinea de Petróleos (GEPETROL)	Malabo	—
Malabo Ministry of Foreign Affairs building	Malabo	January 14, 2015
Ministry of Energy, Industry, and Mines	Malabo	—
Ministry of Finance	Malabo	October 10, 2013
Ministry of Labour	Malabo	—
National Treasury office building	Malabo	—
Parliament	Location Uncertain	—
Presidency Building	Location Uncertain	—
Sociedad Nacional de Gas de Guinea Ecuatorial (SONAGAS, G.E.) headquarters	Malabo	—
Ethiopia		
Commercial Bank of Ethiopia	Addis Ababa	November 2020, Probable
National Oil Company	Addis Ababa	Near completion
Gabon		
National Assembly	Libreville	2001 or 2002, probable
Radio Télévision Gabonaise/Cité des Informations	Libreville	2008, Probable
Senate Building	Libreville	2005
Gambia, The		
Government Office Building	Location Uncertain	—
Police headquarters	Banjul	—
Supreme Court	Banjul	—
Ghana		
Burma Camp Military-Police Barracks	Accra	March 11, 2004
Burma Hall Complex	Accra	April 2006
Court Complex	Accra	—
Military housing - Takoradi	Takoradi	—
Military housing - Tamale	Tamale	—
Military housing - Teshie Military Academy and Training School	Accra	—
Military housing - Sunyani	Sunyani	—
Ministry of Defense	Accra	April 2008
Ministry of Foreign Affairs	Accra	March 18, 2013
Parliament offices/Job 600 building	Accra	—
Peduase Presidential Lodge	Accra	—
Guinea		
People's Palace/Palais du Peuple	Conakry	September 1967
Radio Télévision Guinéenne (RTG)	Conakry	—
Sekhoutereya Palace/Presidential Palace	Conakry	1998

APPENDIX TABLE 1

Chinese-Constructed Government Buildings Across Africa (Page 4 of 7)

Building Name	City	Date Completed/Delivered
Guinea-Bissau		
Government Palace of Guinea-Bissau	Bissau	November, 2010
National Assembly of Guinea-Bissau	Bissau	March 23, 2005
Presidential Palace/Palace of the Republic	Bissau	July 6, 2013
Palace of Justice	Bissau	January 26, 2016
Lesotho		
Parliament	Maseru	June 27, 2012
State House	Maseru	February 14, 2018
Liberia		
Camp Tubman Military Barracks	Gbarnga	April 28, 2009
Capitol Building annexes	Monrovia	—
Ministry of Foreign Affairs	Monrovia	March 2007
Ministry of Health	Congo Town	January 26, 2012
Ministerial Complex	Monrovia	July 25, 2019
Malawi		
Parliament/National Assembly	Lilongwe	June 2010
Presidential Villas	Lilongwe	June 27, 2012
Mali		
National Assembly headquarters	Bamako	—
Presidential Office complex	Bamako	December 2007
Secretariat General of the Presidency	Bamako	—
Mauritania		
Ministry of Foreign Affairs	Nouakchott	—
Parliament/National Assembly	Nouakchott	—
Presidential Palace	Nouakchott	—
Prime Minister's Office	Nouakchott	—
Mauritius		
Mauritius Broadcasting Corporation headquarters	Réduit	—
Mozambique		
Anti-Corruption Bureau/Centre	Matola	—
Auditor-General office	Maputo	—
Military Housing	Location Uncertain	—
Ministry of Foreign Affairs	Maputo	—
Palace of Justice/Justice Tribunal	Maputo	March 2012
Parliament	Maputo	1999
Presidential Palace/Presidential office	Maputo	January 24, 2014

APPENDIX TABLE 1

Chinese-Constructed Government Buildings Across Africa (Page 5 of 7)

Building Name	City	Date Completed/Delivered
Namibia		
Anti-Corruption Commission head office	Windhoek	—
Auditor General head office	Windhoek	—
Command and Staff College	Okahandja	October 17, 2019
Council of Traditional Leaders head office	Windhoek	—
Directorate of Civil Aviation	Windhoek	—
Government Hangar Complex	Windhoek	—
Helao Nafidi Town Council building	Helao Nafidi	—
Katima Mulilo Magistrates Court	Windhoek	—
Katutura Magistrates Court	Katutura	1999
Ministry of Home Affairs and Immigration (MoHAI)	Windhoek	—
Ministry of Lands and Resettlement office	Windhoek	—
National Police headquarters	Windhoek	October 11, 2019
Omuthiya Police Station	Omuthiya	June 5, 2018
Oshakati High Court	Oshakati	September 2009
Oshikoto Police Regional headquarters	Omuthiya	June 5, 2018
Otjinene Magistrate's Court	Otjinene	—
Otjomuise Police Station	Otjomuise	March 31, 2017
Police and Prison Training College	Windhoek	1997
Presidential Office	Auasblick	2017, Probable
Presidential Residence	Auasblick	July 2010
Regional Council building in Outapi	Outapi	—
Regional Council building in Rundu	Rundu	—
Regional Council building in Zambezi	Zambezi	2016, Probable
Supreme Court	Windhoek	1997
South West African People's Organisation (SWAPO) Party headquarters	Katutura	Likely Ongoing
Nigeria		
Nigerian Communications Commission	Abuja	August 2005
Rwanda		
Ministry of Foreign Affairs and Cooperation	Kigali	January 14, 2009
Government Administrative Office complex	Kigali	April 22, 2019
Rwanda Utilities Regulatory Authority	Kigali	Under construction as of July 2018
São Tomé and Príncipe		
Palace of Conventions /Palácio dos Congressos	Sao Tome	—
Senegal		
Ministry of Foreign Affairs	Dakar	—

APPENDIX TABLE 1

Chinese-Constructed Government Buildings Across Africa (Page 6 of 7)

Building Name	City	Date Completed/Delivered
Seychelles		
National Assembly	Victoria	April 2009
Palais de Justice	Victoria	June 17, 2013
Seychelles Broadcasting Corporation	Victoria	—
Sierra Leone		
All People's Congress office	Freetown	—
Army headquarters	Freetown	—
China Bio-Safety Fixed Laboratory	Jui	February 11, 2015
Ministry of Foreign Affairs	Freetown	January 16, 2014
Parliament	Freetown	April 28, 2011
Police headquarters	Freetown	—
Sierra Leone Tropical Infectious Disease Prevention & Control Center	Freetown	July 5, 2018
Youyi (Friendship) Ministerial complex	Freetown	—
Sudan		
Friendship Hall	Khartoum	—
Presidential Palace	Khartoum	January 26, 2015
Sudan National Petroleum Corporation headquarters	Khartoum	—
Tanzania		
Ministry of Foreign Affairs	Dar es Salaam	2018
Togo		
Administrative Services Center	Lomé	April 24, 2019
Presidential Palace	Lomé	—
National Assembly building	Lomé	June 14, 2018
Togolese Television (TVT) and Radio Lomé	Lomé	—
Uganda		
Bureau of Statistics	Kampala	—
Defence Ministry headquarters	Bombo	—
Ministry of Foreign Affairs	Kampala	—
State House Entebbe	Entebbe	—
President and Prime Minister offices	Kampala	January 12, 2012
Senior Command and Staff College	Jinja	—
Treasury building	Kampala	—
Uganda People's Defence Forces barracks at Kakiri	Kakiri	—
Uganda People's Defence Forces barracks at Lunyo	Lunyo	April 11, 2010
Uganda People's Defence Forces headquarters	Bombo	—
Uganda People's Defence Forces National Referral Hospital	Kampala	—

APPENDIX TABLE 1

Chinese-Constructed Government Buildings Across Africa (Page 7 of 7)

Building Name	City	Date Completed/Delivered
Zambia		
Military Housing - Twin Palm Base	Lusaka	December 20, 2013
Military Housing - Makeni, Zambian National Service	Lusaka	—
Military Housing - Waterfalls Lusaka East, Office of the President	Lusaka	—
Military Housing - Chindwin Barracks Kabwe, Zambia Army	Kabwe	—
Military Housing - Tung Up Barracks Mufulira, Zambia Army	Mufulira	—
Government Complex	Lusaka	—
United National Independence Party headquarters	Lusaka	—
Zimbabwe		
National Defence College	Harare	September 2013
Parliament	Harare	Ongoing as of January 24, 2020
African Union		
African Union (AU) headquarters	Addis Ababa	January 28, 2012
Central African Economic and Monetary Community		
Central African Economic and Monetary Community (CEMAC) Parliament	Malabo	—
Economic Community of West African States		
Economic Community of West African States (ECOWAS) headquarters*	Abuja	—
Southern African Customs Union		
Southern African Customs Union (SACU) headquarters	Windhoek	November 3, 2014

* Construction was due to begin in January 2020, but it is unclear if it has.

SOURCE: Author's research. For more information see footnote X.

Endnotes

1. Joan Tilouine and Ghalia Kadiri, "A Addis-Abeba, le Siège de l'Union Africaine Espionné par Pékin," (In Addis Ababa, the Seat of the African Union Spied on by Beijing) *Le Monde*, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html (accessed February 20, 2020).
2. John Aglionby, Emily Feng, and Yuan Yang, "African Union Accuses China of Hacking Headquarters," *Financial Times*, January 29, 2018, https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5 (accessed February 20, 2020).

ii. Wide variety of sources compiled by the author. Particularly helpful were AidData Research and Evaluation Unit, "Geocoding Methodology, Version 2.0.2," June 1, 2017, https://www.aiddata.org/publications/geocoding-methodology-version-2-0 (accessed February 20, 2020), and David H. Shinn and Joshua Eisenman, *China and Africa: A Century of Engagement* (Philadelphia: University of Pennsylvania Press, 2012). The 186 number includes three regional and one pan-African building: the Central African Economic and Monetary Community (CEMAC) Parliament, the Economic Community of West African States (ECOWAS) headquarters, the Southern African Customs Union (SACU) headquarters, and the African Union (AU) headquarters, respectively. Construction of the ECOWAS headquarters was slated to begin in January 2020, but it is unclear if construction has started. Nine other buildings appear to still be under construction.

4. The author did not include in the final number 60 government buildings he found mention of Chinese companies constructing but for which he did not find the source sufficiently reliable and could not obtain other confirmation. The numbers also understate the true extent of Chinese access to African government buildings because some buildings documented here house multiple ministries or sensitive offices. Guinea-Bissau's Palace of Justice, for instance, houses not only the Supreme Court, but also administrative courts and the Attorney General's office. Liberia's recently completed Ministerial Complex is expected to host *five* ministries and one agency once it is fully staffed. Also, the author only counted once an original Chinese-built structure that was later renovated by a Chinese company, under the reasoning that if the CCP was going to install surveillance access, it would have done so in the initial building. However, if the building was renovated and expanded, then the author included this data. The author also assumed that a Chinese company built any structure financed by China, as the great majority of Chinese financing is conditioned on a Chinese company executing the contract. The author used his best judgment in determining whether to include conference centers. If media reports recounted high-level government meetings at the conference centers, he included them in the count. If there was no indication that the center is used for such meetings, he did not include them. This likely leads to an undercount. Similarly, despite the attractive surveillance opportunities Chinese-built hotels offer, the author included only two of them, the Hôtel des Parlementaires in Cote d'Ivoire and the Presidential Villas within the President Walmont Hotel grounds in Malawi. The former was designed specifically to house members of Parliament, though it was later opened to the general public, and the latter for "discerning international government delegations, long-stay guests and royalty." For instance, Niamey, Niger, has only one five-star hotel—the Soluxe—and at least some high-ranking delegations visiting Niger would likely stay at the Soluxe. Several author assumptions may have led to a few instances of over-counting the number of Chinese-built buildings, but the net effect of the author's approach is almost certainly an undercount. See Irene Costa, "Peermon Welcomes Malawi to Its Group," *Business Events Africa*, May 4, 2015, https://www.businesseventsafrica.com/2015/05/04/peermont-welcomes-malawi-to-its-group-2/ (accessed February 20, 2020). For a description of Niamey's Soluxe, see Armin Rosen, "Inside the Amazing Chinese-built Luxury Hotel in the Capital of One of the World's Poorest Countries," *Business Insider*, October 12, 2015, https://www.businessinsider.com/chinese-built-luxury-hotel-in-niger-2015-10 (accessed February 20, 2020).
5. A year and a half before the *Le Monde* expose, a 2016 report mentioned rumors that the Chinese had bugged the AU headquarters. Mathieu Duchâtel, Richard Gowan, and Manuel Lafont Rapnouil, "Into Africa; China's Global Security Shift," European Council on Foreign Relations *Policy Brief*, June 2016, https://www.ecfr.eu/page/-/Into_Africa_China%e2%80%99s_global_security_shift_PDF_1135.pdf (accessed February 20, 2020).
6. The Commission on the Theft of American Intellectual Property, "Update to the IP Commission Report," The National Bureau of Asian Research, 2017, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf (accessed February 26, 2019),
7. "Section 301 Investigation Factsheet," Office of the United States Trade Representative, June 28, 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/june/section-301-investigation-fact-sheet (accessed February 26, 2019).
8. Matt Dean, "FBI: China the Most Predominant Economic Espionage Threat to US," Fox News, July 25, 2015, https://www.foxnews.com/politics/fbi-china-the-most-predominant-economic-espionage-threat-to-us (accessed February 20, 2020).
9. Didi Kirsten Tatlow, "The Chinese Influence Effort Hiding in Plain Sight," *The Atlantic*, July 12, 2019, https://www.theatlantic.com/international/archive/2019/07/chinas-influence-efforts-germany-students/593689/ (accessed February 20, 2020).
10. Derek Scissors, "Record Chinese Outward Investment in 2016: Don't Overreact," American Enterprise Institute, January 2017, https://www.aei.org/wp-content/uploads/2017/01/China-Tracker-January-2017.pdf (accessed February 20, 2020).
11. In 2005, the U.S. embassy in Djibouti reported an incident that may have been an attempt by the employee of a state-owned Chinese construction company to gather intelligence on the embassy and the U.S. military base in the area. See "Djibouti: Possible CI Incident," Wikileaks, March 1, 2005, https://search.wikileaks.org/plusd/cables/05DJIBOUTI208_a.html (accessed February 20, 2020).
12. Elsa Kania, "Much Ado About Huawei (Part 2)," Australian Strategic Policy Institute, March 28, 2018, https://www.aspistrategist.org.au/much-ado-huawei-part-2/ (accessed February 20, 2020).

13. "Senior leadership" means the president, premier, and foreign minister. Kemi Lijadu, "Chinese Leaders Visit Africa More Often Than You Think and Not Always the Places You Expect," Quartz Africa, July 26, 2018, https://qz.com/africa/1335418/chinese-leaders-visit-africa-more-often-than-you-think-and-not-always-the-places-you-expect/ (accessed February 20, 2020).
14. Brook Larmer, "Is China the World's New Colonial Power?" *New York Times*, May 2, 2017, https://www.nytimes.com/2017/05/02/magazine/is-china-the-worlds-new-colonial-power.html (accessed February 20, 2020).
15. Joshua Meservey, "China in Africa: The New Colonialism?" testimony before the Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations, Committee on Foreign Affairs, U.S. House of Representatives, March 7, 2018, https://docs.house.gov/meetings/FA/FA16/20180307/106963/HHRG-115-FA16-Wstate-MeserveyJ-20180307.pdf (accessed February 20, 2020).
16. Raymond Leong, Dan Perez, and Tyler Dean, "MESSAGETAP: Who's Reading Your Text Messages?" FireEye, October 31, 2019, https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html (accessed February 20, 2020).
17. Aaron L. Friedberg, "Competing with China," *Survival: Global Politics and Strategy*, Vol. 60, No. 3 (June–July 2018), pp. 7–64, https://www.iiss.org/publications/survival/2018/survival-global-politics-and-strategy-junejuly-2018/603-02-friedberg (accessed February 21, 2020).
18. John Garnaut, "Australia's China Reset," *The Monthly*, August 2018, https://www.themonthly.com.au/issue/2018/august/1533045600/john-garnaut/australia-s-china-reset (accessed February 20, 2020).
19. Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities Under Xi Jinping," paper presented at The Corrosion of Democracy Under China's Global Influence conference, September 16–17, 2017, https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping (accessed February 20, 2020).
20. As just one example, in November 2019, the former head of the Australian Security Intelligence Organisation accused the Chinese government of a sweeping interference campaign designed to "take over" Australian politics, a day before news broke that a Chinese spy in Australia defected and offered details of the Chinese government's infiltration of universities, media houses, and politics in Australia, Taiwan, and Hong Kong. Peter Hartcher, "'Insidious': Former ASIO Boss Warns on Chinese Interference in Australia," *The Age*, November 22, 2019, https://www.theage.com.au/politics/federal/insidious-former-asio-boss-warns-on-chinese-interference-in-australia-20191121-p53cv2.html (accessed February 20, 2020), and Nick McKenzie, Paul Sakkal, and Grace Tobin, "Defecting Chinese Spy Offers Information Trove to Australian Government," *The Age*, November 23, 2019, https://www.theage.com.au/national/defecting-chinese-spy-offers-information-trove-to-australian-government-20191122-p53d1l.html (accessed February 20, 2020).
21. Irene Yuan Sun, Kartik Jayaram, and Omid Kassiri, *Dance of the Lions and Dragons: How Are Africa and China Engaging, and How Will the Partnership Evolve*? McKinsey & Company, https://www.africa-newsroom.com/files/download/aa9f2979a3dc18e (accessed February 20, 2020).
22. Centre for Chinese Studies, *China's Engagement of Africa: Preliminary Scoping of African Case Studies*, University of Stellenbosch, November 2007, http://www0.sun.ac.za/ccs/wp-content/uploads/2009/04/rf_paper_final.pdf (accessed February 20, 2020).
23. Eric Olander, "Most African States Quietly Take China's Side in Xinjiang Battle at the United Nations," China–Africa Project, October 31, 2019, https://chinaafricaproject.com/analysis/most-african-states-quietly-take-chinas-side-in-xinjiang-battle-at-the-united-nations/ (accessed February 20, 2020).
24. Ministry of Foreign Affairs of the People's Republic of China, "Wang Yi: Thank African Countries for Supporting the Chinese Candidate's Election as Director-General of the World Food and Agriculture Organization (FAO)," June 25, 2019, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1676251.shtml (accessed February 20, 2020).
25. For discussion of why Africa is increasingly important to the United States' strategic interests, see Joshua Meservey, "Implications of China's Presence and Investment in Africa," testimony before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate, December 12, 2018, https://www.armed-services.senate.gov/imo/media/doc/Meservey_12-12-181.pdf (accessed February 20, 2020).
26. Jack Stubbs, "China Hacked Asian Telcos to Spy on Uighur Travelers: Sources," Reuters, https://www.reuters.com/article/us-china-cyber-uighurs/china-hacked-asian-telcos-to-spy-on-uighur-travelers-sources-idUSKCN1VQ1A5 (accessed February 20, 2020).
27. Matthew Brazil, co-author of the recent book *Chinese Communist Espionage: An Intelligence Primer*, makes the point explicitly: "Other countries focus on stealing classified information…. The CCP pursues this standard espionage but also focuses on tech theft to benefit not only its military but also its state-owned enterprises." There are many examples. For instance, in 2014, a U.S. grand jury indicted members of the Chinese military for stealing information from a variety of U.S. companies. Also, British intelligence reportedly believed that a hack of the British mining giant Rio Tinto that cost the company more than $1 billion was also launched by the Chinese military. Robert Mclean, "U.S. Steel Accuses China of Stealing Trade Secrets," CNN, April 27, 2016, http://money.cnn.com/2016/04/27/news/companies/us-steel-china-investigation-trade/ (accessed February 20, 2020), and Kit Chellel, Franz Wild, and David Stringer, "When Rio Tinto Met China's Iron Hand," Bloomberg, July 13, 2018, https://www.bloomberg.com/news/features/2018-07-13/did-china-hack-rio-tinto-to-gain-a-billion-dollar-advantage (accessed February 20, 2020). For Brazil's quote, see Bethany Allen-Ebrahimian, "New Book Unveils China's Formidable Spy Agencies," Axios, February 5, 2020, https://www.axios.com/china-spy-agencies-66e43830-e60c-458d-b9dc-053a6152f9fd.html (accessed February 20, 2020).
28. The Federal Reserve Bank of Minneapolis in 2015 estimated that over 50 percent of all Chinese companies' technology was taken from foreign companies. Thomas J. Holmes, Ellen R. McGrattan, and Edward C. Prescott, "The Costs of Quid Pro Quo," Federal Reserve Bank of Minneapolis, January 29, 2015, https://www.minneapolisfed.org/research/economic-policy-papers/the-costs-of-quid-pro-quo (accessed February 20, 2020).

29. Del Quentin Wilber, "China 'Has Taken the Gloves Off' in Its Thefts of U.S. Technology Secrets," *Los Angeles Times*, November 16, 2018, https://www.latimes.com/politics/la-na-pol-china-economic-espionage-20181116-story.html (accessed February 20, 2020), and Junhua Zhang, "The Trade War, Huawei, and Chinese Strategy," Geopolitical Intelligence Services, June 12, 2019, https://www.gisreportsonline.com/the-trade-war-huawei-and-chinese-strategy,economy,2899.html (accessed February 20, 2020).
30. Chinese companies used "design espionage, business espionage and stealing of techniques and machinery ideas and patterns" to dominate the industry. Chidinma Irene Nwoye, "Your Favorite Wax Print Wasn't Really African and a Chinese Takeover Means it Never Will Be," Quartz Africa, November 25, 2018, https://qz.com/africa/1474039/wax-print-african-fashion-and-chinese-importers/ (accessed February 20, 2020).
31. Wenjie Chen and Roger Nord, "China and Africa: Crouching Lion, Retreating Dragon?" in Brahima S. Coulibaly, ed., *Foresight Africa: Top Priorities for the Continent in 2018*, https://www.brookings.edu/wp-content/uploads/2018/01/foresight-2018_full_web_final2.pdf (accessed February 20, 2020).
32. Sun, Jayaram, and Kassiri, *Dance of the Lions and Dragons*.
33. It is possible this danger is not as pronounced as it might be. African rulers can personally benefit from Chinese engagement, whether it be through accepting bribes, using China's "no-strings-attached" aid to fuel patronage, or receiving glitzy infrastructure projects to present as evidence to voting constituents of how effective they are. Some African rulers may not negotiate as good terms for their countries with Chinese banks and companies as they might absent such personal inducements. For the reports of the Chinese hackers, see "Report: Chinese Hackers Resume Attacks on U.S. Targets," CBS News, August 7, 2013, https://www.cbsnews.com/news/report-chinese-hackers-resume-attacks-on-us-targets/ (accessed February 20, 2020); Chellel, Wild, and Stringer, "When Rio Tinto Met China's Iron Hand"; and Laurie Chen, "'Chinese' Cyber Spy Ring Accused of Targeting Key Players in Belt and Road Initiative," *South China Morning Post*, June 13, 2019, https://www.scmp.com/news/china/society/article/3014421/chinese-cyber-spy-ring-accused-targeting-key-players-belt-and (accessed February 20, 2020).
34. "Huawei Looks to Africa to Cut Network Deals," African Business Central, March 25, 2016, https://www.africanbusinesscentral.com/2016/03/25/huawei-looks-to-africa-to-cut-network-deals/ (accessed February 20, 2020).
35. Among many other warnings about the security risks posed by Chinese-built 5G networks, a group of former senior U.S. military officers penned an open letter cautioning that "Chinese-designed 5G networks will provide near-persistent data transfer back to China that the Chinese government could capture at will." See "Former U.S. Military Leaders Warn of Risks to Future Combat Operations Posed by Chinese-Built 5G Networks," *The Washington Post*, April 2, 2019, https://www.washingtonpost.com/context/former-u-s-military-leaders-warn-of-risks-to-future-combat-operations-posed-by-chinese-built-5g-networks/?noteId=75d276c8-8ac5-4dc7-98c7-981ec0a5da72&questionId=b41ae8c1-2697-4dd7-9a16-a56318713b37 (accessed February 20, 2020). For a report on Huawei's 5G activities in Africa, see Chris Kelly, "Huawei and MTN Group Take First Steps towards 5G in Africa," Total Telecom, November 13, 2019, https://www.totaltele.com/504243/Huawei-and-MTN-Group-take-first-steps-towards-5G-in-Africa (accessed February 20, 2020).
36. Tracking these networks was not the focus of the author's research, so this number almost certainly understates Chinese companies' involvement in creating or upgrading government communications systems that are supposed to be secure. The author's count also only reflects the number of countries in which there are such Chinese-built systems, not the total number of Chinese-built systems. That is a significant distinction, as Chinese companies have built multiple telecommunications systems in many countries. Many are e-governance networks designed to expand, harmonize, and streamline government communications and online services. Other examples include Uganda's Tetra Communications System, implemented by Huawei, used by the military, police, and intelligence agencies; or Kenya's ZTE-built e-government system based in the National Intelligence Service's headquarters. A U.S. government report said that the "project involved a secure network for Kenyan e-Government activities, including software and computer-based security, and a two-story complex that would house the entire Kenyan governments' network files." In Ghana, parliament recently approved a loan from Huawei and state-owned China Machinery Engineering Corporation to construct the country's "National Security Communication Enhancement Network." For mention of Uganda's system, see AidData Research and Evaluation Unit, "Geocoding Methodology, Version 2.0.2." For the U.S. report on Kenya, see "Chinese Engagement in Kenya," WikiLeaks, February 17, 2010, https://search.wikileaks.org/plusd/cables/10NAIROBI181_a.html (accessed February 20, 2020). For the Ghana report, see Lawrence Markwei, "Ghana: Parliament Ratifies 2 Loan Agreements," All Africa, November 29, 2019, https://allafrica.com/stories/201911290488.html (accessed February 20, 2020).
37. Variety of sources compiled by author. Given the incomplete nature of the data on such donations, this is almost certainly an undercount of how frequently this occurs.
38. Some African leaders' reactions to the AU bugging report demonstrates this mentality. The head of the AU, Moussa Faki, and Rwandan President Paul Kagame said in separate interviews that the AU headquarters does not have any secret defense dossiers, implying the Chinese have no reason to spy on the AU. Burundian President Pierre Nkurunziza told Chinese state media he did not believe the report of the AU bugging, and that it was a Western plot to sow division between China and Africa. Ben Blanchard, "African Union Says Has No Secret Dossiers After China Spying Report," Reuters, February 8, 2018, https://www.reuters.com/article/us-china-africanunion/african-union-says-has-no-secret-dossiers-after-china-spying-report-idUSKBN1FS19W (accessed February 20, 2020); Aaron Masho, "China Denies Report it Hacked African Union Headquarters," Reuters, January 29, 2018, https://www.reuters.com/article/us-africanunion-summit-china/china-denies-report-it-hacked-african-union-headquarters-idUSKBN1FI2I5 (accessed February 20, 2020); and "Burundian President Refutes Reports Accusing China of Spying on AU," Xinhua, February 7, 2018, http://www.xinhuanet.com/english/2018-02/07/c_136955756.htm (accessed February 20, 2020).
39. Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain," Bloomberg, January 10, 2019, https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain (accessed February 20, 2020).

40. Andy Keiser and Bryan Smith, "Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat," The National Security Institute *Policy Paper*, January 24, 2019, https://nationalsecurity.gmu.edu/chinese-telecommunications/ (accessed February 20, 2020), and Noah Barkin, Tweet, October 29, 2019, 7:02 a.m., https://twitter.com/noahbarkin/status/1189135507906846723?s=11. (accessed February 20, 2020). Barkin is a journalist and visiting academic fellow at the Mercator Institute for China Studies. ("The head of Germany's foreign intelligence agency has just made crystal clear at a public Bundestag hearing that he does not believe Chinese firms should be allowed to participate in #5G infrastructure. If they are allowed in, then Merkel is ignoring advice of her intel agencies.")
41. For ideas for what the U.S. approach to China in Africa should be, see Joshua Meservey, "Looking Forward: U.S.–Africa Relations," testimony before the Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations, Committee on Foreign Affairs, U.S. House of Representatives, March 26, 2019, https://foreignaffairs.house.gov/2019/3/looking-forward-u-s-africa-relations (accessed February 20, 2020).
42. Joshua Meservey, "Chinese Corruption in Africa Undermines Beijing's Rhetoric About Friendship With the Continent," Heritage Foundation *Issue Brief* No. 4895, August 8, 2018, https://www.heritage.org/global-politics/report/chinese-corruption-africa-undermines-beijings-rhetoric-about-friendship-the (accessed February 20, 2020).
43. There are numerous incidents of China retaliating economically against countries that displease it. In 2006, Zambia's ambassador to China publicly warned that Chinese investors had paused further investment in the country as they were concerned about the possible election to the presidency of a pro-Taiwan candidate. In 2017, the former President of Botswana, Ian Khama, revealed that China threatened to use its influence with African states to isolate Botswana if the Dalai Lama were allowed to visit the country. After Chinese dissident Liu Xiaobo won the Nobel Peace Prize in 2010, China partially closed itself to imports of Norwegian salmon. Beijing similarly restricted exports of rare earth minerals to Japan in 2010 during a maritime dispute, and in 2012 curtailed Filipino banana imports during a row with Manila. Australia, Canada, Mongolia, New Zealand, South Korea, and Taiwan have at various times suffered similar fates for opposing the CCP's wishes. John Reed, "China Intervenes in Zambian Election," *Financial Times*, September 5, 2006, https://www.ft.com/content/d6d5d176-3d0a-11db-8239-0000779e2340 (accessed February 20, 2020); Dikarabo Ramadubu, "'We Are Not a Colony of China'—Khama," *Botswana Guardian*, August 21, 2017, www.botswanaguardian.co.bw/news/item/2790-we-are-not-a-colony-of-china-khama.html (accessed February 20, 2020); Tone Sutterud and Elisabeth Ulven, "Norway Criticised Over Snub to Dalai Lama During Nobel Committee Visit," *The Guardian*, May 6, 2014, https://www.theguardian.com/world/2014/may/06/norway-snub-dalai-lama-nobel-visit (accessed February 20, 2020); Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, *China's Use of Coercive Economic Measures*, Center for a New American Security, June 2018, https://s3.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf?mtime=20180604161240 (accessed February 20, 2020); and Matt Schrader, "Huawei's PR Campaign Comes Straight From the Party's Playbook," *Foreign Policy*, June 6, 2019, https://foreignpolicy.com/2019/06/06/huaweis-pr-campaign-comes-straight-from-the-partys-playbook/ (accessed February 20, 2020).