Testimony before the U.S.-China Economic and Security Review Commission
Hearing on China's Strategic Aims in Africa
May 8, 2020

Steven Feldstein
Nonresident Fellow, Carnegie Endowment for International Peace
Frank and Bethine Church Chair of Public Affairs, Boise State University

Governments in many regions, including in Africa, are making use of Chinese technology to enhance their repressive capacities and actions. Major Chinese firms, such as Huawei, ZTE, Hikvision, Dahua, Meiya Pico, Sensetime, and others, are building surveillance networks, peddling hi-tech censorship tools, and supplying advanced social media monitoring capabilities to countries around the world.[1] Many of the recipient governments possess troubling human rights records. Cloudwalk's mass surveillance facial recognition project in Zimbabwe, or Huawei's safe city projects in Kenya, Zambia, and Uganda illustrate this trend. They raise concerning questions about the motives behind China's digital exports – in particular, is the dissemination of these technologies reinforcing, if not driving, the spread of digital repression?

I would highlight the following points related to patterns of digital repression and surveillance in Africa.

- Chinese companies are actively exporting digital tools with advanced surveillance capabilities to African governments. These capabilities flow towards a diverse array of countries – both autocracies and democracies – who use this technology in different ways. For countries with high internal coercive capacity, such as Egypt, Kenya, or Zimbabwe, these tools reinforce and enhance political repression. In lower capacity countries, their utility diminishes.

- Chinese firms do not have a monopoly on repressive technology. They frequently face stiff competition from companies based in liberal democracies. Moreover, the evidence is inconclusive as to whether surveillance technology provided by China is allowing them to access African data.

- One technology that has gained attention is China's promotion of "safe cities." These projects use tracking devices, video cameras, and other surveillance technology to enhance police and security force capabilities. Unsurprisingly, such systems lend themselves to improper use.

- Thirteen countries in Africa have acquired advanced surveillance capabilities – nine of which are implementing safe city systems: Botswana, Cote d'Ivoire, Ghana, Kenya, Mauritius, Morocco, South Africa, Uganda, and Zambia. Chinese firms, particularly Huawei, are responsible for developing safe cities in all nine countries.

- This raises a key question – does safe city technology matter as a major tool of digital repression in Africa? At present, the answer is most likely no. For now, safe cities are

boutique surveillance techniques that in certain circumstances provide powerful capabilities to governments, but generally are not employed as key instruments of control. Repression on the continent remains a human capital-intensive enterprise.

- The COVID-19 pandemic has caused governments around the world to turn to digital surveillance tools to fight the virus' spread. Compared to other regions, African countries have not yet carried out extensive digital surveillance or censorship measures in response. Consequently, China's role in supporting COVID-19 digital surveillance and censorship measures in Africa remains small, at present.

- Congressional action in three areas would have a beneficial impact in mitigating the repressive uses of Chinese-supplied digital technology in Africa and globally: 1) shape norms of responsible use for surveillance technology by establishing a high-level advisory panel to lay out recommendations, 2) increase support for digital rights organizations by establishing a standalone digital rights fund, and 3) provide targeted funding to level the commercial playing field vis-à-vis Chinese firms by establishing a digital technology infrastructure fund administered by the U.S. International Development Finance Corporation.

Diffusion of Chinese Technology in Africa

How extensive is China's proliferation of digital technology? Its exports encompass a range of products and services – telecom network cables, digital partnerships with universities, surveillance, cloud computing data centers, manufacturing facilities, R&D research labs, and trainings. My data shows that Chinese digital engagement across these different sectors occur in at least 47 of 54 countries in Africa.[2] Huawei and ZTE are the most active Chinese firms, but other key players include Dahua, Hikvision, China Telecom, Meiya Pico, China Mobile, CETC, and Uniview. China's large digital footprint on the continent is not surprising given how many African states are members of the Belt and Road Initiative (BRI) – at last count, approximately 41 countries in Africa have officially joined the BRI.[3]

Starting in 2015, Chinese officials began to trumpet the "Digital Silk Road" (DRS), an adjunct to BRI focused on internet connectivity, artificial intelligence, the digital economy, telecommunications, smart cities, and cloud computing.[4] The launch of the DRS has been murky, and tangible figures are hard to come by. Nonetheless, reports indicate that China has signed DRS cooperation agreements with at least 16 countries. In Africa, *Bloomberg* describes five countries – Angola, Ethiopia, Nigeria, Zambia, and Zimbabwe – which are direct beneficiaries of DSR investments totaling $8.43 billion.[5]

This likely significantly undercounts the scope of Chinese tech activities in Africa; it excludes numerous documented projects, from Kenya and South Africa to Cameroon, Cote d'Ivoire, and Ghana. In fact, according to researchers C. Raja Mohan and Chan Jia Hao, Chinese officials claim that as a result of the BRI, "over 6,000 of China's Internet enterprises alongside over 10,000 Chinese technological products have gained access to overseas markets."[6]

African governments are using much of this technology for benign purposes. They are enhancing connectivity and laying digital infrastructure necessary to modernize their economies. But there's a downside to China's increased involvement in Africa's ICT sector. Its exports are accompanied by an authoritarian mindset that implicitly encourages and directly enables repressive uses of its technology.

Insights Regarding Surveillance & Digital Repression in Africa

We can conclude several things regarding patterns of digital repression and the state of surveillance in Africa.

First, a diverse array of countries procure advanced surveillance instruments for a variety of reasons. For some leaders, sophisticated surveillance tools are a key part of their governing strategies. In these circumstances, not only are Chinese companies abetting non-democratic governments, but they are providing capabilities to states that would otherwise struggle to acquire such tools. In Zimbabwe, for example, which remains under targeted sanctions from the United States, there are reputational and legal risks for western companies to do business with the government (particularly for sensitive digital equipment). Chinese companies have eagerly stepped into the void. As a result, they are directly propping up an oppressive government that willingly and violently subdues its population.

While China can supply digital tools, whether governments will effectively deploy them is another matter. Does the government possess high internal coercive capacity? How strong are civil society and government oversight mechanisms? Depending on the answer, digital tools can potentially transform the state's ability to track political opponents, monitor dissent, quash protest movements, and consolidate political control. But in lower capacity countries which lack disciplined security forces, a coherent command and control structure, and highly-trained personnel able to analyze, interpret, and act on relevant information, the effectiveness of digital tools noticeably diminishes.

In democratic countries, such as Botswana, Ghana, Mauritius, or South Africa, which have stable political systems and governments that abide by the rule of law, their procurement of Chinese technology brings different implications. Their motivations for acquiring these tools have less to do with political repression and largely relate to other issues, such as enhancing law enforcement capacity (e.g., addressing elevated crime rates in South Africa's urban centers). For these countries, Chinese products offer two big advantages: 1) they are comparatively less expensive because of extensive subsidies provided by the Chinese state, and 2) Chinese firms aggressively market their products and are present in the African market in ways that many US and European firms are not. In my research, contacts emphasized to me that Chinese companies are willing to take the extra effort to fulfill immediate needs at competitive – oftentimes unbeatable prices. At the same time, they also share concerns about how Chinese technology may be used – to what extent is data being protected? Is data being shared with the Chinese government? What safeguards are Chinese companies building into their product design?

Second, Chinese firms do not have a monopoly on repressive technology. They frequently face stiff competition from companies based in liberal democracies. Ethiopia is a good example. In

February, I flew to Addis to conduct research for my upcoming book examining the global spread of digital repression. I wanted to hear directly from people on the ground about the impact of digital repression in a country that has generated significant attention for its innovative use of digital tools to enhance the government's political objectives. Ethiopian citizens have suffered from an array of abusive tactics – frequent internet shutdowns, targeted surveillance against journalists and opposition politicians, widespread censorship filtering, and persecutions of individuals for sharing online content. China has cultivated a close relationship with the ruling party, and its companies were responsible for developing much of Ethiopia's digital infrastructure. For example, Ethiopia's national telecom network was largely built by ZTE. As Zhang Yanmeng, ZTE's chief executive officer, crisply put it, "This is the world's only project in which a national telecom network is built by a sole equipment supplier."[7] Thus, China's critical role has allowed it to shape the government's choices, including providing digital capabilities that enable surveillance and censorship.

But it would be inaccurate to hold China responsible for Ethiopia's digital repression. Many other countries have contributed digital capabilities to the regime. Groups like The Citizen Lab have documented how Israeli, Italian, and German firms provided spyware to the Ethiopian government to assist its repression program. During my visit, I met with Tekleberhan Woldearegay, the former director of Ethiopia's Information Network Security Agency (INSA), which is responsible for most of the state's digital repression activities. I asked him about the level of Chinese influence during his tenure at INSA. He smiled and said, "always the Americans think we're working behind the door with the Chinese. Never. That's a completely false perception." He continued, "So we, for example, bought technology from Israel, from Italy, even from Germany, including from America. Also from China. Always to protect your country to create a secure environment. We were searching the best technologies from every part of the world."[8]

Finally, a common question that arises is whether advanced technology provided by China is facilitating access to African data. On this front, the evidence is inconclusive. There are several anecdotal examples that have emerged regarding partnerships between Chinese AI companies and African governments, where Chinese firms provide advanced surveillance capabilities in exchange for access to African data. Researchers from the Australian Strategic Policy Institute, for example, have written about "data colonialism in Zimbabwe" and described how an agreement between China's Cloudwalk Technology and the Zimbabwean government will facilitate sending biometric data on "millions of its [Zimbabwe's] citizens to China to assist in the development of facial recognition algorithms that work with different ethnicities and will therefore expand the export market for China's product." In return, the authors note that the Zimbabwean government "will get access to CloudWalk's technology and the opportunity to copy China's digitally enabled authoritarian system."[9] This may be true, but there are few other examples that have come to light. This remains an area to watch, but there is insufficient evidence that indicates a trend.

Unpacking the Safe City Model

A growing area of importance for China is the export of advanced surveillance tools powered by artificial intelligence and big data technology. In particular, its promotion of "safe cities" has

gained increasing attention. The safe city concept originated from development institutions like the World Bank, which promoted "smart cities" as a way for municipalities to improve service delivery. Smart cities feature an array of sensors which gather information in real time from "thousands of interconnected devices" helping city officials manage traffic congestion, direct emergency vehicles to needed locations, foster sustainable energy use, and streamline administrative processes.[10] Activities specifically oriented towards public safety objectives emerged out of the smart city concept. These projects use tracking devices, video cameras, and other surveillance technology to enhance police and security force capabilities.

Huawei has been a leader in trumpeting public safety technologies for smart cities. It popularized the term "safe cities" as a marketing tool for law enforcement communities that would help "predict, prevent, and reduce crime" and "address new and emerging threats."[11] Huawei explicitly links its safe city technology to confronting regional security challenges, noting that in the Middle East, its platforms can prevent "extremism"; in Latin America, safe cities enable governments to reduce crime; and that in North America, its technology will help the United States advance "counterextremism" programs.[12] Huawei's description of the Kenya Safe City project is illuminating:

> As part of this project, Huawei deployed 1,800 HD cameras and 200 HD traffic surveillance systems across the country's capital city, Nairobi. A national police command center supporting over 9,000 police officers and 195 police stations was established to achieve monitoring and case-solving. The system worked during Pope Francis' visit to Kenya in 2015, where more than eight million people welcomed his arrival. With Huawei's HD video surveillance and a visualized integrated command solution, the efficiency of policing efforts as well as detention rates rose significantly.[13]

Unsurprisingly, such systems lend themselves to improper use. An investigative report by the *Wall Street Journal* in 2019 provided an eye-opening illustration. The reporters discovered that Huawei technicians in both Uganda and Zambia had helped government officials spy on political opponents. This included "intercepting their encrypted communications and social media, and using cell data to track their whereabouts." Not only did Huawei employees play a "direct role in government efforts to intercept the private communications of opponents," but they also encouraged Ugandan security officials to travel to Algeria so they could study Huawei's "intelligent video surveillance system" operating in Algiers.[14] Uganda subsequently agreed to purchase a similar facial recognition surveillance system from Huawei costing $126 million.[15]

Safe Cities in Africa – Where Are They Located? Do They Matter?

Where do safe city surveillance systems operate in Africa and how extensive is their proliferation? Last year I published a report, "The Global Expansion of AI Surveillance" that established an index and methodology for evaluating the diffusion of advanced surveillance technology worldwide in four sectors: safe cities, public facial recognition systems, smart policing, and social media surveillance. Extrapolating and updating the data for Africa shows that thirteen countries in the region have acquired advanced surveillance capabilities, and that nine of these countries are implementing safe city systems: Botswana, Cote d'Ivoire, Ghana, Kenya, Mauritius, Morocco, South Africa, Uganda, and Zambia. Chinese firms are providing

advanced surveillance technology in twelve of the thirteen countries (Namibia is the lone exception). Huawei is the most frequently identified company. A map graphically showing the distribution of Chinese surveillance technology can be found in Figure 1.

What is noteworthy about this set of countries is that they represent a diversity of regime types with corresponding levels of digital repression. The list features liberal democracies (Ghana Botswana), closed autocracies (Morocco), and competitive authoritarian states (Algeria, Egypt, Zambia, Zimbabwe). Some of the countries heavily rely on digital repression with high levels of censorship (Egypt, Algeria) or social media surveillance (Zimbabwe, Zambia, Algeria). Others rank among the best performers on the continent and have virtually no internet constraints (Botswana, Ghana) or online surveillance (Botswana, South Africa). One connecting factor these countries share in common are relatively robust military expenditures. Several of the countries – Algeria, Egypt, South Africa – rank in the top 50 globally for their military budgets. However, two of the countries – Ghana and Mauritius – place outside the top 100. A detailed table showing specific technologies and rankings associated with each country is located in Figure 2.

While thirteen countries make for a reasonable sample, this still represents a minority of countries on the continent. This raises a key question – does safe city technology matter as a major tool of digital repression in Africa? At present, the answer is most likely no.

For now, safe cities are boutique surveillance techniques that in certain circumstances provide powerful capabilities to governments, but generally are not employed as key instruments of control. Repression on the continent remains a human capital-intensive enterprise. Most governments possess neither the institutional capacity nor sufficient resources to reliably use safe cities and related techniques to subdue their populations. Instead, they favor blunter tactics. Internet shutdowns, for example, are prevalent on the continent. They are simple to enact and lead to immediate results (although in the medium to long-term they are ineffective tools in suppressing dissent – as leaders in Sudan and Ethiopia can attest). Arrests and persecutions of journalists, opposition members, and civil society activists are another preferred tactic. They also require minimal technological capacity to undertake. What surveillance does occur largely encompasses targeted measures – such as implanting spyware to extract confidential information from specific individuals. Except for a handful of countries, mass surveillance in Africa is largely absent.

Even globally, the onset of artificial intelligence and big data surveillance has yet to reach critical mass – it remains aspirational for most countries. While China has shown the world how cutting-edge technology can reinforce a massive police presence to turn regions like Xinjiang into virtual police states, for now, China's actions are unique.[16]

That being said, it isn't a stretch to project that in the coming years, increasingly advanced surveillance networks supplied by Chinese firms will become more and more common in Africa – and around the world. In other words, while safe cities have yet to make a big impact in terms of their repressive outcomes, it is worth spending time understanding how they function and how authorities may exploit them for future repressive purposes.

Impact of the COVID-19 Pandemic and Impact on China-Africa Relations

The COVID-19 pandemic has caused governments around the world to turn to digital surveillance tools to fight the virus' spread. While there are many legitimate reasons for governments to deploy contact tracing apps and use location monitoring technology to monitor viral outbreaks, there are troubling reports of privacy violations and human rights abuses. Five trends are particularly salient – both in Africa and globally:

- **Acceleration of existing repression.** Governments already prone to using digital surveillance, censorship, or peddling disinformation, such as Egypt, China, Russia, and India, have aggressively moved ahead to deploy facial recognition surveillance, contact tracing apps, and social media monitoring, along with information controls. State authorities are using the pandemic as a pretext to advance their political agendas.

- **States have become central in gathering and providing information.** As analysts Nathan Brown, Intissar Fakir, and Yasmine Farouk write, "technology may facilitate daily lives under lockdown, but it also aids in the official control of information."[17] The enduring implications of this shift are yet unclear but they present flashing warning signs citizens living in autocracies.

- **The deployment of COVID-19 digital surveillance measures is not limited to authoritarian states.** All manner of governments, are relying on these tools, from autocracies (China, Russia, Thailand, Egypt, Morocco) to established democracies (Spain, Italy, Ghana, Belgium, South Africa).

- **Arrests for violating "fake news" laws linked to the pandemic.** Governments are arresting scores of individuals for spreading "fake news" about the coronavirus in countries such as Myanmar, Cambodia, Kenya, Uganda, China, and Morocco. Targets for arrest are often civil society activists and political opposition figures. In Niger, for example, authorities arrested prominent journalist Kaka Touda for his reporting on the virus.[18]

- **New surveillance techniques are coming online in an ad hoc manner amidst a policy vacuum.** Clear rules of the road regarding safeguards, privacy protections, let alone remedies for abuse, have not been clearly thought out (some governments are deliberately overlooking them). In South African, government officials substantially revised a controversial contact tracing proposal after a firestorm of criticism regarding lack of privacy protections.[19] This raises larger questions about whether new levels of intrusion are here to stay, particularly in non-democracies.

Compared to other regions, such as Asia or Europe, countries in Africa have not yet carried out extensive digital surveillance or censorship measures in response.[20] As of April 27, 2020, only Ghana had implemented contact tracing apps (mobile phone applications which use location data to track infected individuals). South Africa and Kenya have instituted digital tracking using aggregated mobile phone data and/or advanced phone monitoring technology. Tunisia is the lone country that has deployed physical surveillance measures to stem the coronavirus – its police are using remote-controlled robots to enforce the country's quarantine.[21] When it comes to

censorship controls (e.g., locking up individuals who spread "fake news" on social media regarding the coronavirus) African countries display troubling trends. At least seven countries – Algeria, Egypt, Kenya, Morocco, Niger, Tanzania, and Uganda – have imprisoned journalists and civil society activists on misinformation grounds. In Tanzania, for instance, its communications regulatory authority sanctioned three TV stations for spreading misinformation when they allegedly criticized President John Magufuli for declaring that churches should stay open because "coronavirus cannot survive in a church."[22] Finally, Ethiopia continues its internet shutdown in the Oromia region even as the country's coronavirus caseload rises (although there are reports that the government has restored access to parts of the region). Figure 3 shows a breakdown of digital measures implemented by African countries in response to the coronavirus.

China's role in supporting COVID-19 digital surveillance and censorship measures in Africa remains small. It is true that China's COVID-19 surveillance model has received widespread attention (the government is using a combination of facial recognition surveillance, QR codes linked to mobile phone contact tracing apps, as well as drones and robots deployed to hot spots). And there are reports that its government is exporting technology and surveillance practices – e.g., Huawei has donated network equipment and cloud computing access to Italian hospitals, and Iran's Ministry of Health has released a contact tracing app modeled after China's version. But there is little indication that these techniques have spread to Africa and has caused their governments to consider adopting similar measures. Of course, as caseloads rise in Africa, circumstances could change.

China's coronavirus response in Africa have focused predominantly on providing splashy deliveries of emergency medical equipment, such as a Boeing 777 cargo plane loaded with masks, testing kits, and related medical supplies (sponsored by Chinese billionaire Jack Ma) which landed in Ethiopia in March.[23] These actions have been accompanied by coordinated disinformation narratives from officials such as Foreign Ministry spokesperson Zhao Lijian and former ambassador to South Africa Lin Songtian, about the generosity of the Chinese people compared to the failed promises of the United States.[24]

Interestingly, a new twist has occurred in the past several weeks. Reports have emerged of widespread discrimination against African citizens in China, including evictions of citizens from Togo, Nigeria, and Benin from their homes in Guangzhou. There are also accounts that Chinese restaurants and shops are refusing service to African citizens. As reported by AFP, one Ugandan student disclosed, "I've been sleeping under the bridge for four days with no food to eat… I cannot buy food anywhere, no shops or restaurants will serve me."[25] In response, several African ambassadors in Beijing broke with established practice and sent a scathing note to Foreign Affairs Minister Wang Yi to express outrage over their citizens' treatment in China.[26] More broadly, this has generated public outrage against China and threatens to unravel its meticulous public diplomacy efforts. While it is possible that the backlash may diminish, particularly if China reverses its discriminatory policies, it signifies the fragile nature of China's relationship with Africa and the drawbacks to relying primarily on transactional diplomacy as a means to strengthen ties.

Recommendations for Congressional Action

Congressional action in three areas would have a beneficial impact in mitigating the repressive effect of Chinese-supplied digital technology in Africa and globally: 1) shape norms of responsible use for surveillance technology by establishing a high-level advisory panel to lay out recommendations, 2) increase support for digital rights organizations by establishing a standalone digital rights fund, and 3) provide targeted funding to level the commercial playing field vis-à-vis Chinese firms by creating a digital technology infrastructure fund.

First, norms of responsible use when it comes to advanced digital technologies, particularly surveillance tools, remain unsettled. In the absence of effective guidelines and standards of conduct, companies and countries are free to create their own rules. This gives authoritarian countries like China a continual opportunity to impart their own value-systems regarding privacy, sharing of data, and government control of information. It is incumbent that liberal democracies create shared understandings and common regulatory approaches to counter abusive trends. *One proposal would be for Congress to authorize the creation of a high-level commission or advisory body* made up leading policymakers, experts, and academics who would hold public hearings and generate a consensus set of recommendations to guide best practices on pressing digital surveillance issues – something particularly urgent in light of COVID-19. As Rob Berschinski and Benjamin Haas from Human Rights First recently wrote, such a body could also "advise on whether appropriate processes are in place to adjudicate licensing of U.S. intelligence capabilities and services to governments exhibiting a pattern of human rights abuses, and whether foreign governments meet their human rights obligations when undertaking surveillance and other forms of intelligence activities with the support of U.S. agencies or firms."[27]

Second, the rise of digital repression is enabling dictators and would-be autocrats to persecute political rivals, tamp down free expression, and suppress criticism.[28] *One of the best ways to push back on these techniques would be to provide a substantial infusion of resources to support digital rights groups – such as creating a standalone digital rights fund administered by the State Department's Democracy, Human Rights, and Labor Bureau.* Such a fund could focus in three areas: 1) support local groups that are directly pushing back against digital repression efforts, 2) fund international digital rights groups (e.g., Access Now, Privacy International, Netblocks, the Open Observatory of Network Interference, etc.), who are challenging China's "cyber sovereignty" agenda (which gives states implicit permission to restrict internet access and digital rights as they would like),[29] and 3) fund longer-term research to investigate critical questions – what strategies bring the most impact to counter governments' digital repression efforts? What tactics are states adopting in response? To what extent are Chinese and Russian companies facilitating global adoption of digital repression tools, and how effective are these technologies in muzzling advocacy, dissent, and political mobilization? Ensuring that liberal democracies can confront short-term issues and develop longer-term responses is crucial. Without sufficient funding, these efforts will lag.

Third, one of the big selling points of Chinese technology is its cost. Chinese financial institutions provide conditional loans to countries that restrict tech purchases to Chinese firms. Chinese companies are likewise subsidized at a heavy rate by the CCP – by one estimate, more than three percent of China's annual output goes towards direct and indirect business subsidies.[30]

This cash infusion gives Chinese firms significant advantages vis-à-vis foreign rivals. They can access discounted loans from state banks, obtain low-cost inputs (cheap land, electricity), and receive direct cash infusions from government investment funds. This enables firms like Huawei, ZTE, Hikvision, and others to consistently underbid rivals for digital technology contracts – from installing 5G networks and establishing data centers to building safe cities. When African countries with scant resources receive Chinese bids that or 40% lower than comparative tenders from American or European firms, it's not difficult to guess which company wins the contract. While it is not practical nor desirable for the US government to compete on subsidies, there are interim steps the US government could take to level the playing field for American companies. In digital technology areas of strategic importance, such as 5G networks or smart city systems, *Congress could establish a digital technology infrastructure fund, administered by the U.S. International Development Finance Corporation (DFC), that would provide financial resources in the form of matching grants and/or low-interest loans to make US bids more price competitive.* Such a fund could leverage equity financing currently offered by the DFC, but it would offer several enhancements: 1) upgrade the amount of resources available, 2) focus specifically on digital technology projects and reprioritize evaluation criteria so that strategic considerations become much more important factors for determining whether financing is provided, and 3) streamline the lengthy administrative process that companies currently must undergo to obtain support through the use of waivers.

Tables and Graphs

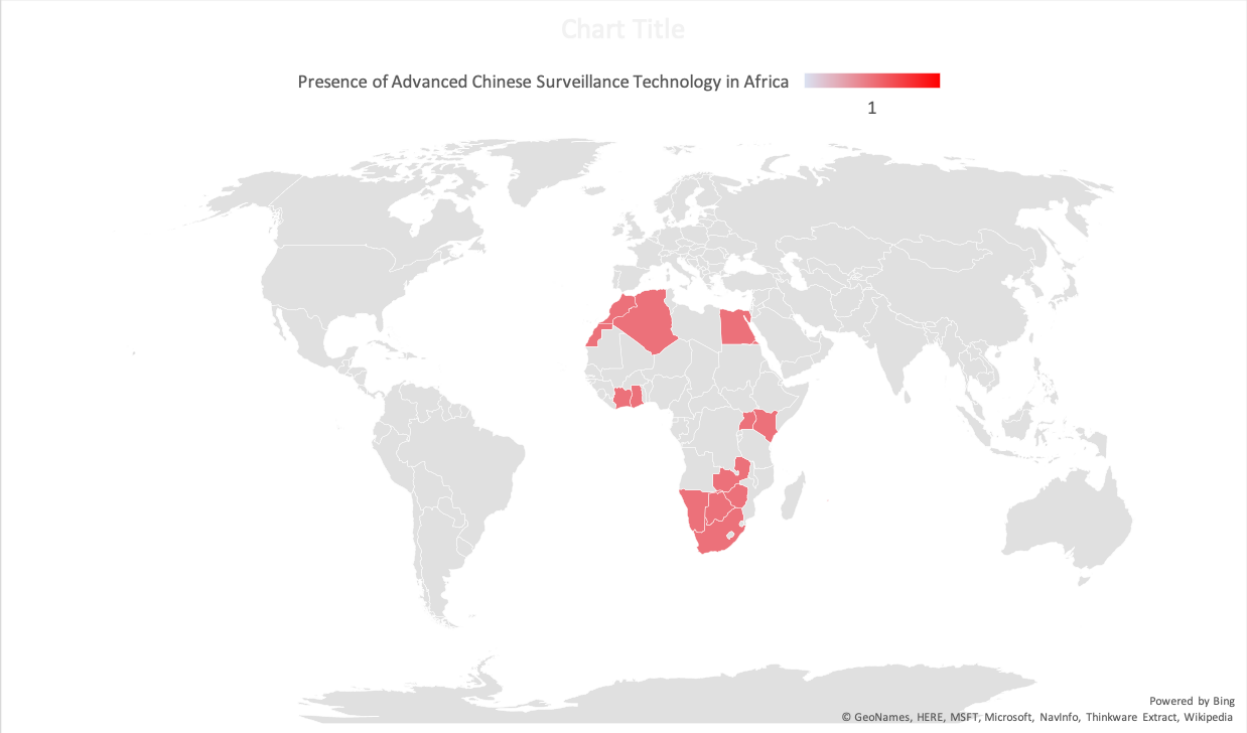

Figure 1. African Countries with AI and big data surveillance technology provided by Chinese firms

Country	Regime Type	Internet Access (% of pop)	Social Media Surveillance Ranking in Africa (lower ranking = more surveillance)*	Online Censorship Ranking in Africa (lower ranking = more censorship)*	Global Military Expenditures Ranking	BRI Member?	Digital Silk Road Member?	Safe City?	Facial Recognition?	Smart Policing?	Social Media Monitoring	Chinese Surveillance Tech?
Algeria	Electoral Democracy	48	4	8	25	x				x		x
Botswana	Liberal Democracy	41	49	54	86			x		x		x
Egypt	Electoral Democracy	45	16	5	51	x			x	x	x	x
Ghana	Liberal Democracy	38	51	45	110	x		x		x		x
Cote d'Ivoire	Electoral Democracy	44	34	39	82	x		x				x
Kenya	Electoral Democracy	18	38	40	69	x		x	x	x	x	x
Mauritius	Electoral Democracy	56	9	16	141			x		x		x
Morocco	Closed Autocracy	62	40	29	47	x		x	x	x	x	x
Namibia	Electoral Democracy	37	27	50	89	x			x	x		
South Africa	Electoral Democracy	56	42	33	48	x		x	x	x	x	x
Uganda	Electoral Democracy	24	11	26	94	x		x	x		x	x
Zambia	Electoral Democracy	28	6	13	98	x	x	x	x			x
Zimbabwe	Electoral Democracy	27	2	18	91	x	x		x	x		x

*Source: Digital Society Project (http://digitalsocietyproject.org/)

Figure 2. Breakdown of countries in Africa that have accessed advanced surveillance technology

Contact Tracing Apps	Digital Tracking	Physical Surveillance	Censorship Controls	Internet Shutdowns
Ghana Kenya* (prospective)	South Africa Kenya	Tunisia	Egypt Niger Kenya Uganda Tanzania Algeria Morocco	Ethiopia

Figure 3. Digital Technology Used by African Countries in Response to COVID-19 (as of April 27, 2020)

[1] Much of the data presented in this testimony is draw from two research pieces I have previously published on this subject: Steven Feldstein, "How artificial intelligence is reshaping repression," Journal of Democracy 30, no. 1 (2019): 40-52; Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace - Working Paper, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

[2] An important resource for compiling data on Chinese technology investments in Africa is Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan and Elise Thomas, "Mapping China's Tech Giants," Australian Strategic Policy Institute, 2020, https://chinatechmap.aspi.org.au/#/splash/. Individual country reports published by Freedom on the Net also provided useful information: "Freedom on the Net 2019: the Crisis of Social Media," Freedom House, 2019, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.

[3] See "Countries of the Belt and Road Initiative," Green Belt and Road Initiative Center," March 2020, https://green-bri.org/countries-of-the-belt-and-road-initiative-bri; Abdi Latif Dahir, "These are the African countries not signed to China's Belt and Road project," *Quartz Africa*, September 30, 2019.

[4] C. Raja Mohan and Chan Jia Hao, "China's Digital Expansion and India," ISAS Working Paper No. 320, October 8, 2019, https://www.isas.nus.edu.sg/wp-content/uploads/2019/10/ISAS-Working-Paper-No.-320.pdf.

[5] Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain," *Bloomberg Businessweek*, January 9, 2019, https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain.

[6] Mohan and Hao, "China's Digital Expansion and India."

[7] Zhao Lili, "Contributing to the Development of Ethiopia with Wisdom and Strength," ZTE Tech, June 12, 2009, https://www.zte.com.cn/global/about/magazine/zte-technologies/2009/6/en_414/172517.html.

[8] Tekleberhan Woldearegay (former director of INSA), interview with the author, February 19, 2020. Tekleberhan's reference to the purchase of Germany, Italian, and Israeli surveillance technology aligns with independent reporting from The Citizen Lab documenting extensive spyware contracts between Ethiopian intelligence and those same firms. See Bill Marczak et al., "Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," Citizen Lab, December 6, 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/; Bill Marczak, John Scott-Railton, and Sarah McKune, "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware," Citizen Lab, March 9, 2015, https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/; Bill Marczak et al., "Hacking Team and the Targeting of Ethiopian Journalists," Citizen Lab, February 12, 2014, https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/; and Morgan Marquis-Boire et al., "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab, March 13, 2013, https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

[9] Danielle Cave, Fergus Ryan, and Vicky Xiuzhong Xu, "Mapping more of China's tech giants: AI and surveillance," Australian Strategic Policy Institute, November 28, 2019, https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

[10] "Smart Cities," World Bank, January 8, 2015, https://www.worldbank.org/en/topic/digitaldevelopment/brief/smart-cities.

[11] "Huawei Smart City White Paper," Huawei Enterprise, 2016, https://e.huawei.com/en/material/onLineView?MaterialID=9b0000e57fa94a2dbc0e43f5817ca767.
[12] "The Road to Collaborative Public Safety," Huawei, 2017, http://e-file.huawei.com/~/media/EBG/Download_Files/Publications/en/Safe%20City%20Extra.pdf.
[13] "Video Surveillance as the Foundation of 'Safe City' in Kenya," Huawei, 2019, https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/videosurveillance-as-the-foundation-of-safe-city-in-kenya.
[14] Joe Parkinson, Nicholas Bariyo and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," Wall Street Journal, August 14, 2019, https://www.wsj.com/articles/huaweitechnicians-helped-african-governments-spy-on-political-opponents-11565793017.
[15] Elias Biryabarema, "Uganda's Cash-Strapped Cops Spend $126 Million on CCTV from Huawei," *Reuters*, August 16, 2019, https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF
[16] Feldstein, "How artificial intelligence is reshaping repression."
[17] Nathan J. Brown, Intissar Fakir, and Yasmine Farouk, "Here to Stay?" Carnegie Endowment for International Peace – *Diwan*, April 22, 2020, https://carnegie-mec.org/diwan/81611.
[18] "Journalist Kaka Touda Mamane Goni arrested in Niger over COVID-19 report," Committee to Protect Journalists, March 24, 2020, https://cpj.org/2020/03/journalist-kaka-touda-mamane-goni-arrested-in-nige.php
[19] https://amabhungane.org/advocacy/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but/.
[20] For a comprehensive global snapshot of digital measures countries are taking in response to the coronavirus, Samuel Woodhams has compiled a useful tracker which can be accessed at: https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/. Privacy International also is documenting relevant digital tracking actions: https://www.privacyinternational.org/examples/tracking-global-response-covid-19.
[21] "Coronavirus: Tunisia deploys robots to enforce lockdown," *Middle East Eye*, March 30, 2020, https://www.middleeasteye.net/news/coronavirus-tunisia-lockdown-robot.
[22] Dickens Olewe, "Coronavirus in Africa: Whipping, shooting and snooping," *BBC News*, April 9, 2020, https://www.bbc.com/news/world-africa-52214740.
[23] Dawit Endeshaw, Giulia Paravicini, "Coronavirus supplies donated by Alibaba's Ma arrive in Africa," *Reuters*, March 22, 2020, https://www.reuters.com/article/us-health-coronavirus-africa/coronavirus-medical-supplies-donated-by-alibabas-ma-arrive-in-ethiopia-idUSKBN2190JU?il=0.
[24] Cobus Van Staden, "Ambassador Lin Songtian's recall signals shifts ahead in China-Africa relationship," *Daily Maverick*, March 30, 2020, https://www.dailymaverick.co.za/opinionista/2020-03-30-ambassador-lin-songtians-recall-signals-shifts-ahead-in-china-africa-relationship/.
[25] "'If you're black you can't go out': Africans in China face racism in Covid-19 crackdown," *AFP*, April 11, 2020, https://www.france24.com/en/20200411-if-you-re-black-you-can-t-go-out-africans-in-china-face-racism-in-covid-19-crackdown.
[26] Simon Marks, "Coronavirus ends China's honeymoon in Africa," *Politico*, April 16, 2020, https://www.politico.com/news/2020/04/16/coronavirus-china-africa-191444.
[27] Rob Berschinski and Benjamin Haas, "How Congress Can Save Lives, Protect Rights, and Exert U.S. Leadership Globally in Response to Coronavirus," *Just Security*, April 8, 2020, https://www.justsecurity.org/69579/how-congress-can-save-lives-protect-rights-and-exert-u-s-leadership-globally-in-response-to-coronavirus/.
[28] See for example Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs*, March/April 2020, https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.
[29] Madhumita Murgia and Anna Gross, "Inside China's controversial mission to reinvent the internet," *Financial Times*, March 27, 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.
[30] David J. Lynch, "Initial U.S.-China trade deal has major hole: Beijing's massive business subsidies," *Washington Post*, December 31, 2019, https://www.washingtonpost.com/business/economy/initial-us-china-trade-deal-has-major-hole-beijings-massive-business-subsidies/2019/12/30/f4de4d14-22a3-11ea-86f3-3b5019d451db_story.html.