CYBER STATECRAFT INITIATIVE

DFRLab

#ACcyber

ISSUE BRIEF

MAY 2023

Africa's Demand for and Adoption of Chinese Surveillance Technology

BULELANI JILI

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

EXECUTIVE SUMMARY

When examining the proliferation of Chinese surveillance systems and cyber capabilities in Africa, research disproportionately focuses on the motivations and ambitions of the supplier. This perspective, while it highlights Chinese diplomatic ambitions and corporate opportunities, ignores local features that drive the adoption of Chinese surveillance tools. This paper discusses African demand factors through an examination of the primary case study of Kenya and examples from South Africa and Uganda. By drawing attention to local efforts to procure and collaborate with Chinese firms to establish public security systems, this work seeks to address the motivations behind the adoption of Chinese information and communication technology (ICT) systems, which include artificial intelligence (AI) surveillance tools and other biometric identification systems, and illustrates the consequences of the proliferation of digital surveillance tools for local and global communities. The paper emphasizes African volition—recognizing its salience—as a way to go beyond myopic representations of Africa as a passive recipient and partner in Africa-China relations.

This work examines the proliferation of Chinese surveillance tools as a dynamic multilateral process. To stem the proliferation of surveillance tools, US policy must understand African demand and accordingly help address local priorities. Accordingly, this paper assesses how demand factors contribute to the proliferation of surveillance technologies, addressing an underexplored facet of the proliferation process, while underscoring the risks of these tools' buildup. Local procurement is critically driven by public security ambitions and justified as a means of achieving development and security aims. While these tools arrive on ostensibly permissible grounds, their acquisition and application come without public consent or robust accountability measures. It is this gap between the adoption of novel digital surveillance technologies and robust regulatory

Surveillance cameras in Nairobi's Central Business District, taken by the author

measures that inspires trepidation. Despite growing concerns over human rights violations domestically and the real risk of installed backdoors in hardware and software, African leaders continue to procure surveillance tools from the People's Republic of China. This decision is predicated on the availability and financial feasibility of Chinese platforms as well as on the technology's supposed capacity to address infrastructure gaps and local public security threats. Discussions of African agency that fail to underscore some of the impediments to its expression only romanticize African volition.

INTRODUCTION

Countries across Africa are procuring and employing surveillance tools from China. This trend is a product of China's diplomatic strategy, its technological ambitions, and growing corporate power and reach, as well as African domestic demands. Thus, both supply and demand factors contribute to the growing proliferation of surveillance tools. A companion paper to this issue brief focused on the key "push factors" from China and their significance for Global South actors.[1] This paper focuses on a diagnostic account of the pull factors in African states.

This paper is divided into three sections. It begins with a brief overview of China's global expansion into African markets.[2] This study's focus on the proliferation and procurement of Chinese surveillance tools does not presume the party-state's exceptional nature in the distribution of digital surveillance tools or seek to obfuscate the broader international market for surveillance tools and cyber intrusive systems, which involves Western firms. Rather, this close examination of the proliferation of Chinese public security systems is an attempt to understand China's growing role in African ICT markets. An investigation into the spread of Chinese digital surveillance technologies in Africa offers a grounded basis for examining how party-state ambitions and corporate firm activities are entangled and, critically, meditated by local vectors. Principally, it expands our understanding of the local and global risks that the adoption of these systems

1 Bulelani Jili, *China's Surveillance Ecosystem & The Global Spread of Its Tools, Atlantic Council*, October 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/.

2 See, for example: *China's Tech-Enhanced Authoritarianism*, House Permanent Select Committee on Intelligence, 116th Cong. (2019) (statement of Samantha Hoffman, nonresident fellow, Australian Strategic Policy Institute's International Cyber Policy Centre); Steven Feldstein, *The Global Expansion of AI Surveillance*, *Carnegie Endowment for International Peace*, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

entails while providing greater insight into the client decision-making process, a crucial and underexamined feature of this proliferation.

Then, this paper examines the factors driving the adoption of digital infrastructure in Africa and the consequences for civil liberties. The size and scope of this inquiry do not permit an exhaustive review of the global ecosystem of surveillance technologies. Instead, primary attention is given to the spread of public security technology from China to Africa. Kenya, South Africa, and Uganda are salient examples of broader China-Africa dynamics, and have been selected to help explore how China's growing cyber footprint is driven by local realities in Africa, how Chinese diplomatic engagements and corporate expansion are mediated by local adoption patterns, and how these local demand factors have their own inertia that drives outcomes. The paper emphasizes African volition—recognizing its salience—as a way to go beyond myopic representations of Africa as a passive recipient and partner in Africa-China relations.

The paper draws attention to drivers for the adoption of digital infrastructure in Africa and the consequences for civil liberties. By privileging the perspective of recipient countries and their local milieu, it demonstrates not only how China promotes its products abroad but precisely how local actors adopt and help drive the proliferation and use of Chinese digital surveillance technology.[3] In light of this, the paper seeks to offer both a grounded study and a systematic analysis of the global and local features at play.

Finally, this paper aims to investigate the features that motivate the procurement of these digital surveillance tools. In so doing, it demonstrates that China's proclivity to provide aid and support to African state actors financially, regardless of their human rights record, thus rendering citizens vulnerable to the misuse of these surveillance technologies. The final sections emphasize that the risks of using these surveillance tools without adequate regulatory frameworks are vast, particularly in a region with established challenges at the intersection of crime, penury, policing, governance, and race. This paper examines the implications of the distribution of Chinese surveillance tools, including the deeper, hidden costs of their adoption, how these new digital tools challenge global norms and standards around data protection, and how American policymakers should respond to the global adoption of these tools. Addressing these questions has significant implications for international security, digital development, and global cybersecurity.

GO GLOBAL

This section highlights some of the key factors that motivate the supply of ICT products into African markets. Current analysis on the distribution of Chinese surveillance tools and cyber capability platforms scrutinizes China's diplomatic activities and questions the degree to which the party-state, with the aid of private firms, enables autocratic digital practices across the globe. These accounts speculate on the level of coordination between Beijing and its corporate actors. While the degree of coordination cannot be empirically fixed, financial incentives in the form of aid and loans are used to incentivize African state procurement and the proliferation of surveillance technologies.

Accordingly, several interconnected economic policy initiatives that helped Chinese firms gain overseas infrastructure development experience were primary contributors to China's global expansion into African ICT markets. Surplus capital is lent abroad to create novel commercial opportunities for Chinese firms.[4] The aim of assisting the internationalization of domestic firms was in part about improving Chinese brand recognition globally, easing fierce domestic competition, and exploiting commercial opportunities made available in part by the absence of US investment in Africa.[5]

A 2011 foreign aid white paper precisely outlines Beijing's approach to global expansion and development aid.[6] Naming this initiative "South-South cooperation," the party-state aims to foster a remunerative orientation with African countries while also simultaneously seeking to carve out a distinct auxiliary role when compared to traditional Western development partners. Therefore, rather than promoting politically conditioned foreign aid that asks for democratic reforms or value-driven commitments like gender equity, Beijing offers aid without political conditions. While this posture suggests a "no strings attached" approach to development, it obfuscates the economic asymmetries that condition relations.[7] China's resource-backed lending finances projects while also demanding that borrowing countries commit to repaying loans with future revenues earned from their infrastructure projects or their natural resources.[8] The posture of "no strings attached" to loans seeks to augment legitimacy for

3 A privileging of the local, while illuminating, can also overlook the broader political and economic forces that shape the particular. However worthy it may be to pursue a strictly grounded study, inquiry risks misidentifying the global forces that—increasingly, with varying degrees of efficacy—are besetting the local.

4 Kevin Cai, "Outward Foreign Direct Investment: A Novel Dimension of China's Integration into the Regional and Global Economy," *The China Quarterly* (1999), 856.

5 Nathaniel Ahrens, *China's Competitiveness Myth, Reality, and Lessons for the United States and Japan, Center for Strategic and International Studies* February 2013, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

6 Ministry of Commerce State Council Information Office, *China's Foreign Aid White Paper (*中国的对外援助白皮书*)*, last updated May 1, 2011, http://fec.mofcom.gov.cn/article/ywzn/dwyz/zcfg/201911/20191102911291.shtml.

7 Bulelani Jili, "Chinese ICT and Smart City Initiatives in Kenya," *Asia Policy* (2022): 44, https://www.nbr.org/wp-content/uploads/pdfs/publications/asiapolicy17.3_africa-china_relations_rt_july2022.pdf.

8 Zainab Usman, *What Do We Know About Chinese Lending in Africa?*, *Carnegie Endowment for International Peace,* June 2, 2021, https://carnegieendowment.org/2021/06/02/what-do-we-know-about-chinese-lending-in-africa-pub-84648.

Beijing's development work in the Global South while also effacing the broad economic features that prompt its engagement and responsibility for the consequences of its financial involvement on the ground.

While China's surveillance system is confined to its national borders, the private firms that make its surveillance architecture possible are selling their tools to an African customer base. With the aid of state funding, Chinese tech firms expanded into African ICT markets. Firms like Huawei initially worked to expand internet connectivity in Kenya, but in 2014 they began selling their smart city products. Proponents of this move argue that public security systems provide vital intelligence to authorities while acting as a deterrent to criminals. Adam Lane, deputy chief executive of government affairs at Huawei Kenya, echoes this sentiment by contending that "authorities can now conduct panoramic video surveillance of Nairobi's urban center, as well as maintain a highly agile command and dispatch setup that runs on satellite-based GPS and software-based geographic information system."[9] Yet, this sanguine outlook does not account for the real risk of exacerbating established problems like the misuse of public security systems and debt stress levels[10]. While Chinese firms promise a technological fix to traditional problems like public safety and state security, they under-deliver in those areas. More significantly, investigative reporting and digital rights organizations have raised concerns about cybersecurity threats, digital surveillance tools, and biometric data collection by these Chinese surveillance tools. These groups contend that the ubiquitous and underregulated use of these technologies threatens privacy rights.[11] Needless to say, they believe that the adoption of digital tools without robust institutional checks and balances, renders citizens more vulnerable to state surveillance and suppression. It is this gap between novel technological adoption and regulatory framework implementation that creates emerging risks.

THE USE OF CHINESE PUBLIC SECURITY SYSTEMS IN AFRICA

This section underscores the demand for digital surveillance tools and their domestic applications. Namely, African states seek out and acquire surveillance systems for a number of reasons, largely as part of a wider effort to augment state security response and capability. Africa's significant digital infrastructure gap is being addressed through Chinese investment and state support. Annually, there is an estimated infrastructure funding gap of up to $107.5 billion a year.[12] China plays a monopolistic role in Africa's telecommunications sector, supplying approximately 70 percent of the continent's digital infrastructure.[13] Surveillance tools are typically purchased as part of a package of ICT systems, which include data centers, closed-circuit television (CCTV) systems, and high-tech biometrics that are integrated and used in tandem with AI products—thus supporting public security authorities and development ambitions.[14]

Digital infrastructure investments, including the promotion of public security systems, in Africa's telecommunications sector have largely been built by China, mostly through state-to-state engagements, but also supplemented by the growing involvement of Chinese private sector actors. According to a review of datasets and reports on the acquisition of Chinese digital surveillance tools in Africa, about 22 African states have contracted with companies like Huawei to adopt digital surveillance technology.[15] Usually procured under the banner of smart city initiatives, these systems collect, integrate, and analyze data from various sources, like national diametric databases that are made available by state partners. The system supports crime prevention and recovery operations. African demand drives the procurement and application of these tools, specifically, to address Africa's digital infrastructure gap.[16] African state and city officials in Kenya, Uganda,

9 N.D. Francois, "Huawei's Surveillance Tech in Kenya: A Safe Bet," *Africa Times*, December 18, 2019, https://africatimes.com/2019/12/18/huaweis-surveillance-tech-in-kenya-a-safe-bet/.

10 Although Beijing does not impose any political conditions on investment, there are economic conditions to its loans. Accordingly, this strategy has permitted resource-rich and high-risk countries the means to secure funds. With the collapse of commodity prices, borrowers in Africa have managed all the risk of debt default. Debt in a way has emerged as the dominant tenure that structures Africa-China relations. Thus far, the party-state has not weaponized debt for geopolitical ends. Rather, it continues to refinance lending terms at lower rates and for longer payment durations. While this willingness to renegotiate does not resolve the problems of accumulating debt, it maintains China's image as an agreeable development partner for Africa.

11 See, for example: Grace Githaiga and Victor Kapiyo, *Kenya's Cybersecurity Framework: Time to Up the Game! KICTANet,* December 2019, https://www.kictanet.or.ke/mdocs-posts/cybersecurity-in-kenya-policy-brief-december-2019/; Karen Allen and Isel van Zyl, *Who's Watching Who? Biometric Surveillance in Kenya and South Africa*, *Enact*, November 2020, https://enactafrica.org/research/research-papers/whos-watching-who-biometric-surveillance-in-kenya-and-south-africa; Tevin Mwenda and Victor Kapiyo, *Personal Data and Elections 2022*, *KICTANet,* February 2022, https://www.kictanet.or.ke/policy-brief-personal-data-and-elections-2022/.

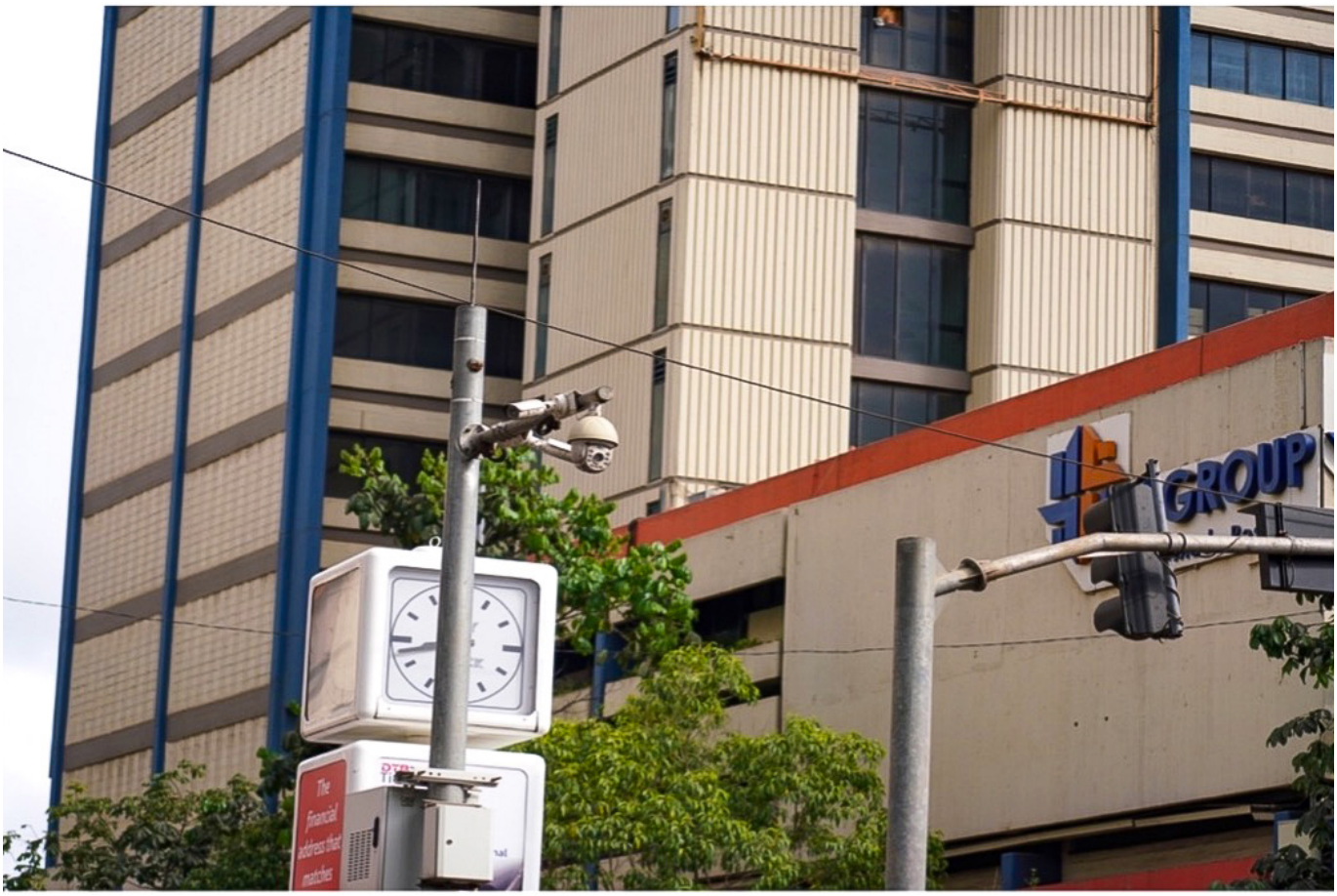
12 African Development Bank Group, "Africa's Infrastructure: Great Potential but Little Impact on Inclusive Growth," Chapter 3 in African Economic Outlook 2018, January 24, 2018, https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/2018AEO/African_Economic_Outlook_2018_-_EN_Chapter3.pdf. See the full report: https://www.afdb.org/en/documents/document/africaneconomic-outlook-aoe-2018-99877.

13 Halligan Agade, "China's Telecommunications Footprint in Africa," *CGTN*, September 2, 2021, https://africa.cgtn.com/2021/09/02/chinas-telecommunications-footprint-in-africa/; Amy Mackinnon, "For Africa, Chinese-Built Internet Is Better Than No Internet at All," *Foreign Policy*, March 19, 2019, https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/.

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

15 Bulelani Jili, *The Rise of Chinese Surveillance Technology in Africa, Electronic Privacy Information Center (EPIC)*, August 25, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-4-of-6/; Feldstein, *The Global Expansion of AI Surveillance*; Sheena Chestnut Greitens, *Dealing with the Demand for China's Global Surveillance Exports*, *The Brookings Institution*, April 2020, https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/; Jonathan Hillman and Laura Rivas, *Global Networks 2030*, *Center for Strategic and International Studies,* March 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210329_Hillman_Global_Networks_2030.pdf?U9r90Zabm5MGoAuHQkVsmqH33SasTi70; Samantha Hoffman, "'Mapping China's Tech Giants: Covid-19, Supply Chains and Strategic Competition,' *The Strategist*, June 8, 2021, https://www.aspistrategist.org.au/china-tech-giants-map-update-3-launch-major-updates/.

16 Huawei, *Rustenburg: World Platinum Capital Deploys Smart City 'Gold Mine'* [Case Study] (2017), https://e.huawei.com/topic/leading-new-ict-ua/rustenburg-smartcity-case.html.



Surveillance cameras in Nairobi's Central Business District, taken by the author

Ethiopia, South Africa, and other countries are reaching out to Chinese firms to aid their varying domestic aims. Together these examples illustrate the establishment of local digital governance regimes. They are not simply a derivative of a Beijing concocted vision, rather, Chinese firms are acquiescing to the ambitions of their host. Crucially, these surveillance regimes are embedded within local private-public ventures. As such, we must consider a more balanced approach that helps to tease out the degree to which local agency is helping shape geopolitical relations while also examining the interplay between Chinese firms and party-state activities on the continent. It is this more balanced approach that offers a vantage point from which to defamiliarize and reimagine politics on the ground.

A CASE FROM KENYA

China's principal entry into Kenya's telecommunication market came through the docking of fiber-optic cables. Led by Huawei and ZTE, two giant Chinese technology firms that specialize in telecommunication, the docking of submarine cables enabled the Kenyan government to liberalize their ICT market, which allowed for a more competitive telecommunication section.[17] In an interview with the author, a former ICT official said, " [the ministry] then set in motion a series of policies, including the National Information and Communications Technology (ICT) Policy, that aimed at the liberalization of the telecommunications sector that created opportunities for more actors to be involved. With financing that came from US banks and the Export-Import Bank of China, we looked to close the infrastructure gap that hampered growth."[18] To establish the country's first National Optic Fiber Backbone Infrastructure, which brought high-speed connectivity, the government jointly contracted Huawei and ZTE.[19] Each company was expected to manage a different region across the country. ZTE laid the cables for the west, and Huawei handled Nairobi and the central parts of the country.[20] This novel digital capacity empowered the state to pursue e-government projects, which include public security systems and cyber intrusion platform solutions.

As such, the Kenyan government primarily enlists these surveillance tools as a means to scale public security capabilities, national security prerogatives, and data security. The

17 Bitange Ndemo and Tim Weiss, *Digital Kenya: An Entrepreneurial Revolution in the Making* (London: Springer Nature, 2017).

18 An one-one interview with the official was conducted with the author during a 11 month fieldwork study in Nairobi.

19 Iginio Gagliardone, *China, Africa, and the Future of the Internet* (London: Zed Books, 2019).

20 Muriuki Mureithi, Telecommunication Ecosystem Evolution in Kenya, 2009-2019: Setting the Pace and, Unbundling the Turbulent Journey to a Digital Economy in a 4IR Era, *Institute of Economic Affairs*, March 2021, https://ieakenya.or.ke/download/telecommunication-ecosystem-evolution-in-kenya-2009-2019-setting-the-pace-and-unbundling-the-turbulent-journey-to-a-digital-economy-in-a-4ir-era/.

adoption of surveillance tools is made possible through the sale of Chinese equipment and soft loans from the Export-Import Bank of China, which are crucial in making public security platforms financially attainable for Nairobi and other African governments. Beyond Huawei, Chinese companies like Dahua, Hikvision, and others are involved in the adoption of digital surveillance systems.[21] In 2012, the Kenyan government awarded Nanjing Les Information Technology, a high-tech provider that offers urban traffic management and urban governance tools, a tender to supply digital surveillance cameras.[22] The goal of the initiative was to augment public security and intelligent traffic management systems in downtown Nairobi. According to official figures, the platform cost the government 463,960,697 Kenyan shillings, which amounts to $3.8 million.[23] The expected date of completion was June 2013, but, due to delays, the project was not completed until April 2014.[24] Constant power shortages and access to privately owned buildings for installation purposes were the main reasons for delays. No less important, the adoption plan for these tools did not include corresponding data protection measures to promote and maintain privacy rights, rather inadequate planning before the start of the program presaged the delays and data policy omissions.

China's oversized role in African ICT markets engenders a dependence on their products and expertise. Digital public security systems are embedded within state-driven processes that are contingent on private-public ventures. The use and effectiveness of these tools, though nominally operated by and for the purposes of Kenyan government officials, are heavily reliant on Chinese contractors to operate public security platforms. An audit by the auditor-general's office found that senior staff sent by the Kenyan government to China to learn how to operate public security systems did not acquire the necessary skills.[25] Instead, the staff spent time inspecting the parts of the system to be delivered. During that visit, no attempts were made to learn or teach how to operate the system.[26] For this reason, questions remain about Kenya's ability to operate and maintain its public security systems. Furthermore, technical matters having to do with the upkeep of the system are managed by the contractor. The National Police, who are tasked with the responsibility of operating the system, had not even developed the capability to work the control room.[27] To complicate matters, the manual language of the control room was in Chinese. Most of the digital surveillance cameras installed within Nairobi's central business district stopped working months after they were installed. Even more worrying is that there were limited security protocols for accessing the system, which increased the possibility of unauthorized access or the launch of malicious code on the server by unauthorized users.

To supplement its earlier public security system, Huawei was invited to install its public security system in Kenya. In Kenya, as in the rest of the continent, Huawei promised that its new product, the safe city, would improve public security. The safe city is a form of a smart city, which is a computational model of urban planning that aims to utilize technological innovation to enhance operational efficiencies. The safe city platform utilizes a series of interconnected technologies like video cameras, tracking devices, software, and cloud storage systems to link technologies and processes as a means to integrate them into a larger and more cohesive whole to advance public initiatives like managing traffic, policing, and streamlining service delivery.[28] The first safe city system by Huawei was able to connect 1,800 high-definition cameras and 200 high-definition traffic surveillance infrastructures across Nairobi.[29] A command center was also installed, which supports over 9,000 police officers in 195 police stations.[30] The Kenyan government is pursuing smart city initiatives as a way to resolve public security challenges and address the country's digital infrastructure gap. Digital surveillance platforms are part of a wider state-led initiative to utilize technologies to help resolve structural challenges and, thus, make development more attainable.

COMPARISONS ACROSS THE CONTINENT

This section highlights the motivations for and incentives of local surveillance procurement in Uganda and South Africa. It lends weight to an examination of the proliferation of Chinese surveillance tools in Africa as a dynamic process shaped by demand and supply factors. Uganda, like Kenya, is also procuring public security systems from Huawei. The Kampala police procured AI facial recognition systems from Huawei in 2019, supposedly to address the city's growing crime rate.[31] Uganda is working with Huawei to help close digital infrastructure gaps and address domestic

21 Bulelani Jili, "Chinese ICT and Smart City Initiatives in Kenya.

22 Office of the Auditor General of Kenya, *Performance Audit Report of the Auditor-General on Integrated Urban Surveillance System for Nairobi Metropolitan Area* , February 2017, https://www.oagkenya.go.ke/wp-content/uploads/2022/08/Integrated-Urban-Surveillance-System-for-Nairobi-Metropolitan.pdf.

23 Office of the Auditor General of Kenya, *Performance Audit Report.*

24 Office of the Auditor General of Kenya, *Performance Audit Report.*

25 Office of the Auditor General of Kenya, *Performance Audit Report.*

26 Office of the Auditor General of Kenya, *Performance Audit Report.*

27 Office of the Auditor General of Kenya, *Performance Audit Report.*

28 Huawei. "Huawei Hosts Safe City Summit in Africa to Showcase Industry Best Practices" October 17, 2016, https://www.huawei.com/us/news/2016/10/safe-city-summit-africa; Frank Hersey, "Digital ID in Africa this Week: Biometrics for Tea Workers, Financial Inclusion with a Thumbprint," *Biometric Update,* August 23, 2019, https://www.biometricupdate.com/201908/digital-id-in-africa-this-week-biometrics-for-tea-workers-financial-inclusion-with-a-thumbprint.

29 Bulelani Jili, *The Spread of Chinese Surveillance Tools in Africa, Oxford University China, Law and Development Project*, June 30, 2020, https://cld.web.ox.ac.uk/files/finaljilipdf.; Hi-tech security, "Safe city summit in a safe city," *Hi-tech security*, February 2017, *http://www.securitysa.com/56445n* ; *China's Strategic Aims in Africa: Goals of China's Africa Policy and Consequences of Beijing's Influence*, US-China Economic and Security Review Commission, 116th Cong. (2020) (statement of Steve Feldstein, nonresident fellow, Carnegie Endowment for International Peace).

30 See, for example: Jili, *The Spread of Chinese Surveillance Tool.*

31 Tom Wilson and Madhumita Murgia, "Uganda Confirms Use of Huawei Facial Recognition Cameras," *Financial Times*, August 20, 2019, https://www.ft.com/content/e20580de-c35f-11e9-a8e9-296ca66511c9 .

challenges with crime. In contrast, Kenya's particular history with terrorist attacks by Islamist militants has motivated the state's adoption of surveillance systems. As in Kenya, Huawei claims that safe city tools meet several service delivery demands, including real-time surveillance, evidence collection, and video browsing that support policing initiatives.

Opposition leaders in Uganda, civil society, and international observers highlight the misuse of surveillance tools, and how these platforms are instead used to monitor and target political opposition to the administration of President Yoweri Museveni.[32] To be sure, the misuse of public security platforms is not the only reason for concern. Facial recognition technologies require mass biometric data for training data collection, software integration, and algorithm development. As a result, acquiring and using these tools without strong privacy safeguards poses a threat to privacy rights.

South Africa's experience with high rates of crime is the primary motivation for the state to adopt public security platforms as a means to manage the perennial threat. While demand is a response to concerns about crime and governance, it also due to state efforts to close infrastructure gaps and bolster state digital capabilities. Smart city initiatives in South Africa seek to resolve structural challenges while also offering solutions to social challenges like crime. Former Rustenburg mayor Mpho Kunou explains that "the Rustenburg Smart City project aims to develop the economy, enhance citizen participation, improve public safety and transportation, expand the scope of government services, and implement digitalized public utilities through leading technologies."[33] The increased presence of Chinese surveillance technology in South Africa has raised concerns in Washington about the party-state's influence over South Africa's digital infrastructure.[34] In addition to Huawei, in South Africa, local company Vumacam is a leading provider of digital surveillance tools. For example, in the city of Johannesburg, Huawei digital cameras are paired platforms from Vumacam and Hikvision, another Chinese digital surveillance tool provider.[35] The various surveillance tools are deployed by the police, local municipalities, and private security firms. This example, like the previously mentioned public security systems in Kenya, illustrates African states' tendency to use multifarious governance and surveillance platforms.

The lack of evidence that public security systems reduce crime does not deter the promotion of public security platforms. In fact, in the case of Kenya, crime rates have risen in areas supported by these technologies.[36] With the growing concern over the promotion and misuse of surveillance tools, Adam Lane, deputy chief executive of government affairs at Huawei Kenya, dismisses these concerns by contending that "Huawei's role is to develop, install, deploy, and maintain the technology according to the request and need of the National Police Service. The National Police Service is responsible for operating it and using it according to their policies in line with any national laws."[37] This popular framing is reductive, if not completely misleading. It rests, somewhat simplistically, on an all-or-nothing approach to responsibility for negative outcomes. The argument draws attention to the behavior of the National Police but says nothing about the consequences of the sale of these systems or whether regulations are necessary to mitigate negative outcomes. The company position de-emphasizes its role in enabling state actors to surveil citizens, instead placing sole blame and responsibility on state actors for any misconduct.

Government officials, including Kenyan, South African, and Ugandan state representatives, see digital surveillance systems as possible solutions to the traditional challenges that their countries face. This contention challenges presuppositions about the adoption of Chinese surveillance tools as strictly a reflection of Beijing's efforts to promote digital authoritarianism. Rather, African governments assemble hybridized surveillance systems, in part from Chinese companies, as part of a broader digital infrastructure initiative that seeks to address infrastructure gaps while connecting various heterogeneous tools whose application promises to ameliorate domestic problems like violent crime and terrorism. These objectives, however, are not supported by robust legal measures to protect civil liberties. With the introduction of public security platforms, policymakers are faced with challenge to devise appropriate data policies and privacy measures to deal with the intensification of datafication and surveillance.

GLOBAL INSECURITIES & US INTERESTS

This section examines the consequences of the global proliferation of Chinese surveillance tools. Precisely, it raises a series of questions for both the international community and local stakeholders, especially about transparency and accountability. For example, most African governments, including Kenya and Uganda, have limited transparency with respect to the acquisition of surveillance tools, despite provisions in their federal laws that demand

32 Elias Biryabarema, "Uganda's Cash-Strapped Cops Spend $126 Million on CCTV from Huawei," *Reuters*, August 15, 2019, https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF.

33 Huawei, *Rustenburg: World Platinum Capital*.

34 Opposing the Republic of South Africa's hosting of military exercises with the People's Republic of China and the Russian Federation, and calling on the Biden administration to conduct a thorough review of the United States-South Africa relationship, 'H.R. Res.145, 118th Cong. (2023).

35 Karen Hao and Heidi Swart, "South Africa's Private Surveillance Machine is Fueling a Digital Apartheid," *MIT Technology Review*, April 19, 2022, https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/.

36 National Police Service of the Republic of Kenya, *Annual Crime Report 2018*, September 12, 2019, http://www.nationalpolice.go.ke/crime-statistics.html.

37 N.D. Francois, "Huawei's Surveillance Tech in Kenya: A Safe Bet," *African Times*, December 18, 2019, https://africatimes.com/2019/12/18/huaweis-surveillance-tech-in-kenya-a-safe-bet/.

state transparency.[38] More saliently, there is a need for more transparency around the use of Chinese loans and procurement of public security platforms, as well as technologies that have the potential to be repurposed deployed for surveillance purposes. The party-state's willingness to support digital infrastructure projects that include public security platforms is problematic in the context of authoritarian states like Uganda or Zimbabwe, which have a history of utilizing cyber intrusion systems to undercut human rights and conduct unwarranted state surveillance.[39] The adoption of public security platforms enhances the state's capabilities to conduct surveillance. Even in a relatively healthy democracy like South Africa or Kenya, skewing power toward the state can result in unwarranted surveillance practices that lead to the atrophy of rights, especially in the absence of robust institutional checks and balances.[40] It is this gap between the adoption of public security systems and regulatory frameworks that poses a critical risk to civil liberties. As such, transparency and accountability measures must extend to digital infrastructure development, which creates room for the misuse of public security products to advance surveillance and other modalities that incentivize democratic backsliding.

The global spread of Chinese surveillance tools could pose threats to privacy and cybersecurity. Several researchers and observers have warned about misuses and various cybersecurity vulnerabilities with Hikvision surveillance products.[41] The incessant product vulnerabilities have led researchers to claim "backdoors" are intentionally designed to enable Chinese intelligence collection.[42] This position is further bolstered by the fact that the party-state recently introduced several laws—the national intelligence law of 2017, the data security law of 2021, the national security law of 2015, and the cybersecurity law of 2016—that establish obligations for private firms to comply with state demands for data while also offering limited means to reject or appeal unwarranted requests from the Beijing government.[43] Vitally, however, this kind of argument still presumes a level of party-state intention and collaboration with firms. At this time, there is no empirical evidence from Kenya, South Africa, or Uganda that establishes coordination and collaboration between Chinese state authorities and Hikvision that results in intentional data theft. Similar allegations leveled against other companies, such as Huawei, cannot be emphatically proven. However, the absence of concrete evidence or attribution does not categorically dispel escalating concerns and vulnerabilities. In fact, it further demonstrates the need for ensuring supply chain security and integrity given the ever-present potential for furtive insertions like backdoors in software and hardware products.

US-CHINA COMPETITION'S IMPACT ON AFRICA

This section details the United States should respond to the proliferation and adoption of Chinese surveillance tools. Currently, the growing adoption of Chinese surveillance tools in Africa and the United States' ambition to mitigate this spread are encouraging the bifurcation of the world, staging Africa and the Global South generally as the theater for a dispute between China and the United States. This division between procurers and non-procurers does not support US interests or the health and inclusive posture of the international liberal order. Indeed, it further ignores the real political challenges and financial motivations behind nation-states' procurement of Chinese tools. To stem the proliferation of these technologies and the real harm felt locally and globally, the United States must develop a more nuanced posture on the proliferation of Chinese surveillance and cyber-offensive systems, one that responds to the real political challenges and financial motivations behind nation-states' procurement of Chinese tools.[44]

American and international observers must pay greater attention to the contextual motivations for the growing demand for Chinese digital infrastructure and public security systems. Precisely, it is important to consider how local factors mediate and condition China's geopolitical footprint. To curtail the spread and misuse of surveillance technologies, Washington and its European allies should focus not on the "supply" side but on the factors driving African demand for public security platforms.

38 Christopher Musodza, Kuda Hove, and Otto Saki, *Digital Influence in Africa*, *Friedrich Naumann Foundation*, November 2022, https://shop.freiheit.org/download/P2@1351/661343/China's%20digital%20influence%20in%20Africa_Friedrich%20Naumann%20Foundation.pdf; "Mapping and Analysis of Privacy Laws in Africa," Collaboration on International ICT Policy in East and Southern Africa (CIPESA), November 2021, https://cipesa.org/?wpfb_dl=479.

39 Allen Munoriyarwa , and Sarah H. Chiumbu, "Big Brother is Watching: Surveillance Regulation and its Effects on Journalistic Practices in Zimbabwe," *African Journalism Studies* (2019), 26-41.

40 Bulelani Jili, "The Spread of Chinese Surveillance Tools in Africa: A Focus on Ethiopia and Kenya.'" in *Africa–Europe Cooperation and Digital Transformation,* ed. Chux Daniels, Benedikt Erforth and Chloe Teevan. (London: Routledge, 2022), 32-49.

41 John Honovich, "Hikvision has 'Highest Level of Critical Vulnerability,' Impacting 100+ Million Devices,' *IPVM*, September 20, 2021, https://ipvm.com/reports/hikvision-36260#:~:text=Hikvision%20has%20admitted%20a%209.8,it%20impacts%20100%2B%20million%20devices; Valentin Weber and Vasilis Ververis, "China's Surveillance State: A Global Project," *Top10VPN*, August 2021, https://www.top10vpn.com/assets/2021/07/Chinas-Surveillance-State.pdf; Wilson and Murgia, "Uganda Confirms Use of Huawei Facial Recognition Cameras".

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

43 "National Intelligence Law of the People's Republic of China." ("中华人民共和国国家情报法"), The National People's Congress of the People's Republic of China, June 12, 2017, http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml; "Data Security Law of the People's Republic of China." ("中华人民共和国数据安全法"), The National People's Congress of the People's Republic of China, June 10, 2021, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml; "National Security Law of the People's Republic of China." ("中华人民共和国国家安全法"), The National People's Congress of the People's Republic of China, July 7, 2015, http://www.npc.gov.cn/npc/c10134/201507/5232f27b80084e1e869500b57ecc35d6.shtml; "Cybersecurity Law of the People's Republic of China" ("中华人民共和国网络安全法"), November 7, 2016, http://www.npc.gov.cn/npc/c30834/201611/270b43e8b35e4f7ea98502b6f0e26f8a.shtml.

44 Greitens, *Dealing with the Demand*.

The primary driver of procurement of surveillance technology in Kenya is contingent on their promise to close digital infrastructure gaps and address traditional challenges like crime and terror. This most prominent example of terrorism in the country is the 2013 al-Shabaab militant attack on an upscale shopping center in Nairobi, killing 67 people and injuring hundreds more. This argument suggests that the United States cannot afford to take a parochial approach and message to the risks posed by the adoption of Chinese technologies. The message shared with the world must speak to the challenges confronting African leaders and partners. Working with African authorities to build digital infrastructure, implement data protection measures, and address challenges like terrorism are ways to mitigate the negative consequences of the proliferation of public security systems. Indeed, a policy that meets African stakeholders where they are with regard to their development challenges is needed. This kind of message will inform a more nuanced approach and understanding, which will help the United States and its allies work within and against the challenges, priorities, and incentives that drive the adoption of Chinese public security systems.

An approach that centers on dissuading African countries from working with companies like Huawei, which are believed to pose cybersecurity threats, risks misunderstanding the objectives and priorities that drive the adoption of Huawei's tools. For instance, the appeal of Huawei's safe city project is its financial feasibility, its comprehensive offerings, and its promise to resolve traditional problems like crime. A message that stresses the risks involved is pivotal, but alone, this point runs counter to local priorities. To limit the proliferation of surveillance tools, US policy must better understand African demand and accordingly help address local priorities by offering attainable and safer alternatives to assist local initiatives, while emphasizing that these tools are not automatic remedy for domestic challenges but rather auxiliary instruments. In fact, their adoption can exacerbate challenges in a region with established concerns around crime, governance, corruption, and policing, particularly in the absence of robust checks and balances.

Initiatives like the smart city blur the distinction between service delivery initiatives and invasive surveillance practices. Accordingly, the adoption of these tools has implications for civil liberties, particularly in legal environments that lack robust regulatory frameworks.[45] This raises questions about the need for mechanisms that govern the distribution and use of these platforms. Chinese firms and actors have been swift in its attempts to establish norms for the application of these systems. As stated before, this effort is pursued through the development of several domestic laws, training programs involving recipient nations, diplomatic exchanges with African partners, and ventures to influence global standards around the regulation of these platforms.[46] Such endeavors include active participation and leadership in intergovernmental institutions like the International Telecommunication Union (ITU), which is responsible for influencing the global standards and regulatory frameworks for the use of surveillance platforms. To counter the concerted push along this front from the Chinese government, the US government must actively promote standards, regulations, and norms that mirror its democratic values and interests domestically and in multilateral institutions like the ITU. Meanwhile, working alongside likeminded democracies can also help strengthen and promote human rights and democratic values.

The United States and its European partners can play a significant role in helping build local data protection and cybersecurity capacity in regulating the use of public security systems. Many countries on the continent, including Kenya, still lack a comprehensive legal and policy framework to address cybersecurity risks. For example, the Data Protection Act (2019) empowers regulators and requires mandatory registration by data processors, yet it remains unclear what authority the data protection commissioner has to enforce state privacy abuses emerging.[47] Likewise, there are no means to audit the algorithms that power facial recognition technology or to halt the harvesting of biometric data from the population without an adequate system of checks and balances. Kenya, like many countries in the continent, must work toward building a more conducive legal and policy environment to address growing cybersecurity threats.

In giving an intelligible account of China's expanding geopolitical footprint, it is important to underscore party-state ambitions and activities in Africa while also illuminating how these aims are mediated by local state and substate actions. Digital surveillance tools on the continent are enlisted to address social challenges like crime, but also a way to index and catalyze digital development. Indeed, while African governments' ambitions are laudable on the surface, without checks and balances, surveillance activities pose a threat to civil liberties, particularly in a region that struggles with challenges at the intersection of policing, governance, surveillance, race, and crime. Work must be done to advance legal measures to mitigate the negative consequences of intensified surveillance practices.

45 Bulelani Jili, 'Africa: Regulate Surveillance Technologies and Personal Data,' *Nature* (2022), 445–448.

46 Emma Rafaelof, Rogier Creemers, Samm Sacks, Katharin Tai, Graham Webster, and Kevin Neville, *China's 'Data Security Law*, *New America*, July 2, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/; Li Wanyi, "Delegation of South African Parliament Police Committee Visits Shanghai (南非议会警察委员会代表团访问上海)," *Jiefang Daily*, October 4, 2107, http://shzw.eastday.com/shzw/G/20171014/u1a13342865.html; Li Zhengwei, "The China-Africa Internet Development and Cooperation Forum Held (中非互联网发展与合作论坛举办)," *Guangming*, August 24, 2021, https://m.gmw.cn/baijia/2021-08/24/35106965.html; Ministry of National Defense People's Republic of China, *Wei Fenghe Meets with Representatives of the First China-Africa Defense and Security Forum (*魏凤和会见首届中非防务安全论坛代表*)* [Press release], July 10, 2018, http://www.mod.gov.cn/topnews/2018-07/10/content_4818896.htm.

47 Office of the Data Protection Commissioner of Kenya, *Data Protection Act*, 2019, https://www.odpc.go.ke/dpa-act/.

ACKNOWLEDGEMENTS

Without friends and colleagues' support, it would have been an arduous task to bring this work to conclusion. It is their advice, research, and critical reflections that enable this work and its insights.

AUTHOR

Bulelani Jili is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative. His research interests include ICT development, Africa-China relations, cybersecurity, post-colonial thought, and privacy law. He is also a Meta Research PhD fellow at Harvard University, visiting fellow at Yale Law School, cybersecurity fellow at the Harvard Kennedy School, scholar-in-residence at the Electronic Privacy Information Center, visiting fellow at Hong Kong University Law, and research associate at Oxford University. He can be reached at bulelanijili@g.harvard.edu.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

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

TREASURER
*George Lund

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

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

**Executive Committee Members*

List as of March 6, 2023