

City Research Online

City St George's, University of London

Citation: Da Vinha, L. (2024). Smart for Whom? Africa's Smart Cities and Digital Authoritarianism. International Journal of Intelligence and CounterIntelligence, 37(3), pp. 941-959. doi: 10.1080/08850607.2023.2284629

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/38639/

Link to published version: https://doi.org/10.1080/08850607.2023.2284629

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

Smart for Whom?: Africa's Smart Cities and Digital Authoritarianism

Luis da Vinha

Luis da Vinha is a Senior Lecturer in International Relations and coordinator of the Master of International Relations at Flinders University (Adelaide, Australia). Luis is also a member of the Jeff Bleich Centre for the US Alliance in Digital Technology, Security & Governance and a research affiliate of the Space Power and Policy Applied Research Consortium (SPPARC). He is the author of Geographic Mental Maps and Foreign Policy Change and co-author of Three Approaches to Presidential Foreign Policy-Making in the Twenty-First Century. The author can be contacted at luis.davinha@flinders.edu.au.

Abstract

The predicament of digital authoritarianism is particularly grievous for Africa since democratic institutions have been gradually eroded in several countries throughout the region. Illiberal regimes, in particular, exploit digital technologies to undermine such fragile democracies as Ethiopia, Tanzania, Uganda, and Zambia.[1] Moreover, surveillance technology is expanding throughout the region as national and local governments seek to increase their capacity to monitor and control their populations – a trend that has been aggravated with the COVID-19 pandemic.[2] As such, while authorities normally claim that surveillance technologies are used to protect the people, manage urban services, and improve the citizen's quality of life in the city, the information and data collected can also be used to enable digital authoritarianism and undermine democratic institutions and processes.[3] As smart cities increasingly employ surveillance technologies, the challenges to fragile democracies in Africa grow. This article assesses the risks posed by smart cities to democratic institutions and processes. It begins by identifying the main models of smart city development and how they conceive of the state's and citizens' relationship. It subsequently assesses how smart cities can potentially foster and consolidate digital authoritarianism with a particular focus on the technology that a regime can exploit to pursue illiberal goals. It then provides cases to illustrate how smart city systems promote digital authoritarianism. The article concludes by discussing proposals to mitigate the technological risks and promote democratic smart cities.

Keywords:

Africa, Digital Authoritarianism, Digital Democracy, Smart Cities, Surveillance Technology

Africa's projected population growth in the coming decades foreshadows several regional social, economic, and political challenges. According to the United Nations (UN) Population Division, the region represents the fastest-growing population in the world as estimates project that over half of the global population growth through 2050 will occur in sub-Saharan Africa.[4] More precisely, sub-Saharan Africa is expected to almost double its population by mid-century, from 1.15 billion

inhabitants to 2.1 billion.[5] Much of this growth will be in urban areas as studies estimate that 56% of the region's population will live in cities by 2050.[6] With rapid urbanization come several daunting challenges for the region's cities[7]—most notably, inadequate physical infrastructure, urban density and congestion, urban slums and informal settlements, low quality and unsustainable social services, environmental vulnerability, and rising unemployment in the informal urban economy.[8] Not surprisingly, as Slavova and Okwechime posit, in the coming years urbanization will be "the main policy narrative for Africa."[9]

There has been a growing call by policymakers to embrace "smart" development policies and solutions to address the challenges associated with Africa's rapid urbanization process. In particular, "smart cities" are viewed by many international officials, scholars, and experts as the best path for "African cities to help solve their needs and leapfrog other nations in their development," as Echendu and Okafor argue.[10] By harnessing the potential of digital technologies, smart cities offer an opportunity to exploit the latest innovations to try to solve the most pressing contemporary urban problems. To be sure, smart cities can enhance a city's technological, institutional, and social milieu. These services contribute to solving problems in several distinct, but interrelated urban components such as the economy, education, environment, governance, infrastructure, lifestyle, mobility, resources, and security, among others.[11] Accordingly, in recent years African officials have announced several smart city projects to try to capitalize on the potential that smart cities offer in fostering development and improving the quality of life for the region's growing urban populations.[12]

Notwithstanding the discernible benefits in improving aspects of urban life, smart cities also pose many risks to their users. Numerous scholars forewarn how smart city technologies offer inroads into surveilling and controlling groups and individuals, and suppressing their civil liberties and political rights.[13] More precisely, there is a growing concern among scholars and human rights

groups that smart city technologies allow for an ever-greater capacity to observe, collect, and process data regarding people's behavior, activities, and communications. In short, for all the technological advances and advantages they seem to proffer, smart cities also represent an innovation in domestic intelligence.

The predicament of digital authoritarianism is particularly grievous for Africa since democratic institutions have been gradually eroded in several countries throughout the region. Illiberal regimes, in particular, exploit digital technologies to undermine such fragile democracies as Ethiopia, Tanzania, Uganda, and Zambia.[14] Moreover, surveillance technology is expanding throughout the region as national and local governments seek to increase their capacity to monitor and control their populations—a trend that has been aggravated with the COVID-19 pandemic.[15] As such, while authorities normally claim that the surveillance technologies are used to protect the people, manage urban services, and improve the citizen's quality of life in the city, the information and data collected can also be used to enable digital authoritarianism and undermine democratic institutions and processes.[16]

As smart cities increasingly employ surveillance technologies, the challenges to fragile democracies in Africa grow. This article assesses the risks posed by smart cities to democratic institutions and processes. It begins by identifying the main models of smart city development and how they conceive of the relationship between the state and citizens. It subsequently assesses how smart cities can potentially foster and consolidate digital authoritarianism with a particular focus on the technology that a regime can exploit to pursue illiberal goals. It then provides cases to illustrate how smart city systems promote digital authoritarianism. The article concludes by discussing proposals to mitigate the technological risks and promote democratic smart cities.

SMART CITIES AND THE THREAT OF DIGITAL AUTHORITARIANISM

Smart cities present a formidable challenge to democracy since they employ a host of surveillance technologies that can be used inappropriately, jeopardizing basic civil liberties and political rights. While definitions of smart cities have proliferated as they are increasingly the subject of scrutiny in several different disciplines and fields of inquiry, most accounts emphasize the use of digital technologies to improve the quality of life of urban communities.[17]

Just like other smart systems, smart cities have several key components, ranging from the technology infrastructure formed by the networks of connected devices and sensors to the smart components that allow for processing and analyzing the data obtained. According to Charalampos et al., data is critical to smart cities since the "key for the success of a smart city is the collection and the proper exploitation of data coming from these technologies."[18] To collect data, smart cities take advantage of the ever-growing availability of technologies that observe, collect, and process the behavior, activities, and communications of urban dwellers. Besides traditional visual surveillance, smart cities obtain data through biometric surveillance (which collects an individual's biological characteristics) and dataveillance (which collects an individual's data through information systems).[19] While the technologies employed vary in accordance with each individual project, researchers can identify a slew of technologies commonly used in smart cities to collect information about the urban environment, particularly about a city's residents and users (Table 1).

Table 1: Surveillance Technologies Employed in Smart Cities

Type of Surveillance	Technology
Visual surveillance	• Automatic license plate recognition (ANPR) • Body-worn cameras • Closed-circuit television (CCTV) • Crowd density scanning

	• Crowd management • Dash cams • Drones with cameras
Biometric surveillance	• Behavioral detection • Body sensors • Environmental sensors (noise, pollution, land movement) • Facial recognition • Fingerprinting • Gunshot detection • Iris scanning • Lifestyle wearables
Dataveillance	• App controlled smart appliances • Bike sharing • Car sharing • Digital payments • e-government / e-democracy • e-identity • e-ticketing • Electronic voting • Home security system • i-beacons • Remote patient monitoring • User-generated databases, dashboards, and interfaces

	• Vehicle information services • Wi-Fi connected city

A key feature of smart cities is the capacity to integrate and exploit big data collected from networked urban infrastructures and services. As one of the main commercial smart city platform providers argues, "Without a central place or command centre to capture, process, [and] share information across city functions, smart city initiatives become siloed."[20] Smart cities can acquire, integrate, and process data from multiple sources that make it a system of systems capable of monitoring, controlling, optimizing, and autonomizing urban functions and services.[21] In other words, surveillance, particularly in the smart city, is ubiquitous and not limited to suspected individuals or groups. Much of the data obtained by smart cities is voluntarily, if not consciously, provided by individuals as they use a growing number of digital products and services.[22] Furthermore, data is increasingly collected, categorized, and processed by private actors who actively commercialize it and provide it to third parties or to the general public.[23]

In this context, the growing integration and processing of personal information and data has transformed the smart city into a "system of surveillance" that is deleterious to democracy as it advances authoritarian practices.[24] Particularly concerning is that much of the surveillance in the smart city deviates from the practices traditionally conducted by state actors. In recent years, surveillance has not only been expanded by new technologies, but its very nature has undergone a significant qualitative transformation, as MIT's Gary Marx clarifies:

> The new surveillance relative to traditional surveillance extends the senses and has low visibility or is invisible. It is more likely to be involuntary. Data collection is often integrated into routine activity. It is more likely to involve manipulation than direct coercion. Data collection is more likely to be automated involving machines rather than (or in addition to) involving humans. It is relatively inexpensive per unit of data collected. Data collection is often mediated through remote means rather than on scene and the data

> often resides with third parties. Data is available in real time and data collection can be continuous and offer information on the past, present and future (ala statistical predictions).[25]

Accordingly, without robust regulatory and legal frameworks, as well as respect for the rule of law, the threat of digital authoritarianism—where governments use digital technologies to monitor, repress, and coerce their citizens—increases significantly with the growth of smart cities, particularly in regions with fragile democratic institutions and processes.

Digital authoritarianism allows illiberal regimes to consolidate and maintain power by employing more subtle and sophisticated means of repression and control, averting more traditional forms of "high-intensity coercion" associated with traditional dictatorships such as firing on crowds of demonstrators, suppressing elections, and carrying out targeted assassinations of opposition leaders. Emerging forms of "low-intensity coercion" seek to weaken challenges to governments before they threaten the regime by exploiting systematic, yet less visible, initiatives to monitor, manipulate, and suppress any potential opposition activity.[26] With the capacity to collect, integrate, and process boundless amounts of data, smart cities increasingly afford government regimes and officials the ability to carry out low intensity coercion. Governments may use smart city technologies to foster digital authoritarianism in several ways:[27]

- Surveilling and tracking individuals or groups;
- Blocking, censoring, or manipulating data and digital information;
- Keeping tabs on popular discontent and controlling mass protests;
- Using disinformation to delegitimize critics and/or opponents;
- Harassing and repressing dissenting or threatening individuals and/or groups.

In recent years, illiberal regimes have increasingly used technologies to violate their citizen's civil liberties and political rights. In fact, research demonstrates that illiberal regimes are more prone to exploit digital technologies to harass and repress critics, opposition figures, dissidents, and anyone the regime finds threatening.[28] Furthermore, research suggests that "dictatorships that increase their use of digital repression also tend to increase their use of violent forms of repression 'in real life,' particularly torture and the killing of opponents."[29] However, the main goal of digital authoritarianism is to induce positive behavior from citizens since it is assumed that by knowing that they are being surveilled and monitored people will "normalize" their conduct. In other words, just like the panopticon, individuals are believed to change their behavior and comply with expected social norms due to their awareness of being subject to the widespread use of surveillance technologies.[30]

Equally disturbing is that by integrating the windfall of data and employing AI and big data analytics, smart cities provide would-be-autocrats with the ability to implement predictive profiling. More precisely, state and city officials can use complex algorithms to analyze the myriad of data points and develop real-time behavioral profiles of individual citizens, allowing for more targeted preemptive actions with the allocation of fewer resources.[31] With the rapid pace of technological innovations, soon "algorithms will be able to string together data points from a broad range of sources—travel records, friends and associates, reading habits, purchases—to predict political resistance before it happens."[32] Moreover, smart technologies will allow responses to be autonomized, for instance, by applying rewards and penalties in accordance with an individual or group's behavior or profile.[33] While one can see a semblance of this optimization and autonomization in the realm of predictive policing, a more accurate paradigm is China's social credit system. While still in its incipient stage, the social credit system allows Chinese authorities to collect an individual's bank data, hospital records, domestic movements, shopping habits, and

online activity, among other records, to assign a comprehensive score that rewards loyalty and punishes critics and dissidents.[34]

COMPETING MODELS OF SMART CITY DEVELOPMENT: THE AFRICAN CASE

To address the challenges resulting from rapid population growth and urbanization, policymakers across Africa have embraced the concept of smart cities—capitalizing on competing smart city technologies from Europe, the United States, and China.[35] However, these actors provide different models of smart city development that can significantly impact the future of Africa's democratic institutions. The European Union (EU) and China, in particular, have developed strategies and programs specifically focused on promoting smart city technologies in Africa.[36]

While smart cities flourished throughout the EU for over two decades, they lacked an integrated approach.[37] As competition with international actors like China increased, the EU has sought to overhaul existing policies and institute a comprehensive strategy to make Europe a key player in the digital realm. In order to position the EU as a leader in the digital space by 2030, the president of the European Commission (EC), Ursula von der Leyen, promised to invest 20% of the approximately €800 billion NextGenerationEU recovery program on digital initiatives.[38] The EU also issued the *2030 Digital Compass: The European Way for the Digital Decade* which established a strategy for achieving a "human-centric" digital environment that reinforces citizens' rights, such as their rights to privacy and data protection and freedom of expression. It outlined Europe's commitment to digital societies that "support open democracy initiatives by contributing to inclusive policymaking, enabling wide-ranging engagement with people and stimulating grass-roots action for developing local initiatives as enabler factors to improve social acceptability and public support for democratic decisions."[39] The emphasis on individual rights was further consolidated in the recent *European Declaration on Digital Rights and Principles for the Digital*

Decade and in the EU's General Data Protection Regulation which provides a regulatory framework for upholding its citizens' data privacy and security and which is showcased as a model for digital governance around the world.[40] These policy initiatives have increased Europe's confidence that they can have a key role in shaping the development of smart cities around the world.

Africa is central to Europe's international digital strategy. According to the EU's *Towards a Comprehensive Strategy with Africa*, both regions share several core interests and values such as sustainable development and strengthening the multilateral rules-based order by "promoting universal values, human rights, democracy, rule of law and gender equality."[41] While several areas of this strategy have a direct impact on Africa's urban agglomerations, it is by harnessing its strengths to help build a regulatory framework to protect city residents and their data, as well as ensure greater digital inclusion and equality, that the EU can best engage with Africa's smart cities. The EU and the African Union strengthened their strategic relationship by issuing the *Joint Vision for 2030,* emphasizing their commitment to the rules-based international order.[42] To help operationalize this partnership, the EU announced over €150 million of investments in Africa as part of its Global Gateway Investment Package. This initiative presents Europe's alternative to China's Belt and Road Initiative (BRI) while it also includes a digital component through the EU's Digital for Development (D4D) Hub.[43] The AU-EU D4D hub commits both actors to a human-centric approach to digital transformation and seeks to foster greater knowledge sharing and technical assistance among the multiple European and African stakeholders in areas such as connectivity, cybersecurity, e-commerce, digital skills, entrepreneurship, e-governance, and privacy and data protection.[44] Accordingly, the EU seeks to promote this approach in its involvement in developing Africa's smart city projects.

In its attempt to assume a more significant role in global leadership and counter attempts by the United States and the EU to contain its behavior, President Xi Jinping and the Communist Party

of China (CPC) have identified technological innovation as the linchpin of international competition in the future.[45] In order to create an international system that is more favorable to their interests and strategic objectives, Chinese leaders are increasingly committed to enhancing their standing and influence in the Global South. Africa is particularly important for Beijing's global political ambitions. Not only are the continent's resources important for China, but the region's demographic and economic growth provides new markets for Chinese exports and services at a time when the Chinese domestic market is saturated by its overcapacity.[46] Furthermore, Africa has become a critical region in determining if China can achieve its goal of being the global leader in technological innovation.[47] China's ambitions were apparent in its China-Africa Partnership Plan on Digital Innovation announced in 2021 and which sought to promote Chinese digital technology in the region, along with fostering greater technological integration and interconnectivity.

Among the many areas of anticipated cooperation, China seeks to bolster its role in the region by "building 'smart cities' and leveraging digital technologies to strengthen state governance," as The Ministry of Foreign Affairs explains.[48] Indeed, China has made smart cities a national priority and an integral part of its agenda for global technological leadership. In his opening speech at the 2017 Belt and Road forum, Xi Jinping emphasized the importance of smart cities in fostering innovation-driven development.[49] China has used the BRI's Digital Silk Road (DSR) component to promote and develop smart cities internationally.[50] China's political system, which allows the CPC to compel private companies and financial institutions to coordinate their operations with the government's political strategy and objectives, facilitates the exportation of Chinese-designed smart cities.[51] As a result, Chinese companies are actively involved in countless smart city projects, disseminating the Chinese model in Africa.[52] The active involvement of Chinese companies was evident in the 2018 Forum on China-Africa Cooperation Beijing Action Plan that stated that China would support African states in building Smart Cities and "enhancing the role of

ICT [information and communications technologies] in safeguarding public security, counter terrorism and fighting crime and work with the African side to uphold information security."[53]

Moreover, in contrast to the European model, China promotes a "people-oriented" ("yi ren wei ben") approach to smart cities which emphasizes the role of technologies in solving urban problems, namely improving resident's living standards and fostering efficient public services, rather than protecting their personal data and digital rights.[54] While the Chinese approach to smart city development places people at the center, its objectives are purely pragmatic and focus on improving people's living standards. This model of smart cities is consistent with the CPC's political tradition emphasizing "collective welfare" and its recently formulated concept of "whole-process people's democracy" that posits that political legitimacy is based on state performance rather than on popular consent.[55] Therefore, the Chinese model's emphasis on technological performance over citizen's rights poses a greater risk that illiberal regimes throughout Africa can use the technology to reinforce their power and undermine democratic institutions and processes.

In fact, the growth of smart cities in Africa has largely been the result of the promotion of China's model of digital governance, which creates challenges to fragile democracies.[56] China is an "end-to-end" provider of the digital supply chain that underscores smart city development and is already a world leader in smart city initiatives.[57] For example, the Chinese corporate giant Huawei has built over 25 data centers and e-governance projects across the African continent and Chinese tech companies have built over 200 government facilities in Africa, equipping them with computers, routers, and other technological equipment.[58]

However, research has diverged in assessing China's role in exporting its model of digital governance and actively undermining democracy.[59] Also, several democratic states—including, the United States, France, Germany, Israel, and Japan—have themselves provided technological systems that enabled such illiberal regimes as Egypt, Indonesia, Saudi Arabia, and United Arab

Emirates (UAE), to surveil their citizens and suppress civil liberties and political rights for political or personal gain, which in turn has (even if unintentionally) helped dilute democracy in the recipient countries.[60] The recent disclosure of the use of the Pegasus spyware illustrates this risk. The Israeli NSO Group developed the Pegasus software which, can infiltrate smartphones undetected and collect all the device's data, and sold this technology to governments such as Bahrain, Hungary, Kazakhstan, Morocco, Saudi Arabia, and the UAE. While the Israeli government has tried to distance itself from these states' behavior, reports claim that the software was used to collect over fifty thousand phone numbers, many belonging to politicians, government officials, business executives, journalists, and activists.[61] To be sure, even if, as Steven Feldstein rightly points out, "surveillance *per se* is not anti-democratic,"[62] how governments use these technologies poses a threat to democracy. In other words, do they use them justifiably and in a way that enhances individual's liberties and rights, or are they employed to strengthen political power at the expense of citizens?[63]

CHALLENGES TO AFRICA'S SMART CITIES

Under these circumstances, despite the growing concern about the risks of digital authoritarianism, African leaders have embraced smart cities as key drivers of development.[64] In recent years, governments throughout the region – including, for example, Kenya, Nigeria, Rwanda, and South Africa—have implemented numerous smart city initiatives varying from retrofitting existing cities with new technological infrastructure to the creation of smart districts, economic zones, and neighborhoods. However, several challenges befall the African nations that implement and import smart city technologies. To begin with, there is a growing trend in developing new cities which are built-from-scratch to catalyze economic development and circumvent the challenges inherent to existing urban settlements.[65] In contrast to retrofitting existing areas, master-planned, greenfield

projects allow for an integrated approach to planning and developing smart cities.[66] Therefore, these new cities are planned and designed from the outset to integrate a broad array of technologies that can be employed to strengthen the regimes in power and undermine democracy. These cities would fit the criteria of "systems of surveillance" in which the entire urban population would be subject to constant surveillance and monitoring, and the integration and processing of city-wide data would allow for greater control and normalization of individual's behavior, as well as the effective development of predictive profiling.

In the last decade, countless new city projects have been announced – most notably, African Coastal Smart City (South Africa), Akon City (Senegal), Alaro City (Nigeria), Appolonia City (Ghana), Centenary City (Nigeria), Cidade do Gás (Mozambique), Ciudad de la Paz (Equatorial Guinea), Eko Atlantic (Nigeria), Enyimba Economic City (Nigeria), Kiswishi (Democratic Republic of Congo), Machakos New City (Kenya), Modderfontein New City (South Africa), Mohammed VI Tangier Tech City (Morocco), New Administrative Capital (Egypt), Nkosi City (South Africa), Nova Cidade de Kilamba (Angola), Nkwashi (Zambia), Peninsula City (Sierra Leone), Talent City (Nigeria), Tatu City (Kenya), Vision City (Rwanda), and Waterfall City (South Africa).

Most of these projects involve foreign actors that contribute to designing, financing, and providing the technology underpinning smart cities. National governments usually drive these projects, yet virtually all smart city projects in Africa rely on funding from other states, as well as hedge funds, banks, and other private investors that many times prioritize economic and political opportunities over issues concerning citizens' liberties and rights.[67] The dependence on foreign resources for developing and implementing smart city projects can jeopardize democracies in Africa and strengthen digital authoritarianism throughout the region. China is already a major financier of digital technologies in Africa, such as facial recognition technology and the region's

4G network.[68] Capitalizing on the DSR, Chinese companies are involved in developing smart city projects in Ethiopia, Ghana, Kenya, Mozambique, Nigeria, South Africa, Zambia, and Zimbabwe, among others.[69] The state-owned China International Trust and Investment Corporation (CITIC) has also funded several projects for new cities in Angola and Egypt and which favor Chinese technology companies.[70] Due to the active support of the Chinese government and its affordability and commercial promise, Huawei has been particularly successful in advancing its "safe city" system in several African nations—including, Angola, Botswana, Cameroon, Ethiopia, Ghana, Ivory Coast, Kenya, Madagascar, Mauritius, Nigeria, South Africa, and Uganda.[71] The system integrates a host of technologies and services such as closed-circuit television (CCTV) cameras, intelligent video surveillance, facial and license plate recognition technology, crowd monitoring, situational awareness detection, noise monitoring, social media monitoring, and command centers.[72]

Ultimately, then, while many individuals and communities benefit from the improvements brought on by these investments, the political threats also loom large. There are abundant reports exposing how some states in Africa have used smart city technologies to track and monitor individuals and suppress basic political freedoms. For example, in 2019 the Ugandan government used Huawei's technological resources and staff to surveil and detain political opponents. The relationship between Huawei and Kampala began in 2014 when Huawei offered 20 CCTV units to the government. After Uganda's Assistant Inspector General of Police, Andrew Felix Kaweesi, was murdered in 2017, the government acquired Huawei's safe city system for US $126 million.[73] Currently the CCTV system is composed of about 5,000 cameras, over 80 monitoring centers and uses AI to integrate facial recognition, license plate recognition, and social media monitoring.[74] The system also employs Huawei middleboxes, which examine individuals' online browsing data and digital communications, as well as manipulating and filtering information by diverting visitors

to fake websites that can steal passwords and install malware.[75] Human rights groups quickly sounded the alarm that these technologies have been used to suppress the opposition and dissidents. For instance, the Museveni regime had been exposed for previously using technology from the UK-based Gamma Group to monitor political opponents.[76] However, in 2019 the regime counted on the aid of Huawei technicians to intercept communications and track opposition figures. More precisely, the surveillance technology and the technical assistance provided by Huawei's staff allowed the government to hack presidential hopeful Robert Kyagulanyi's (a.k.a., Bobi Wine) WhatsApp and Skype communications, undermining his attempts to organize street rallies. The surveillance ultimately led to the location and the arrest of Kyagulanyi and over 800 of his supporters.[77]

A similar situation occurred in Zambia. In the context of the DSR, the country invested over $1 billion in Chinese telecommunications, broadcasting, and surveillance technology and in 2015 the Lungu government received financial support from China to develop the Smart Zambia project. As part of the project, Huawei implemented a safe city system, with Lusaka taking the lead by installing CCTV cameras and other surveillance technologies across the city.[78] Governments in these countries have used these technologies to access and monitor the phones and social media pages of individuals operating a pro-opposition news site, and not for national security purposes.[79] Just as in Uganda, the Zambian government also relied on the collaboration of Huawei technicians to help the government spy on its citizens. The company's experts allowed the regime to locate the news bloggers, facilitating their subsequent arrest.[80] Besides monitoring and tracking opposition supporters and dissidents, the Zambian government has also repeatedly used its control of the country's technological infrastructure to cut access to the internet and social media platforms such as Facebook, Instagram, Twitter, and Messenger.[81] However, African officials are not immune from being monitored. The fact that internal information from the AU's headquarters in Addis

Ababa—built by China—was systematically being diverted to Shanghai for several years attests that anyone or any organization is susceptible to surveillance.[82]

These examples illustrate the challenges facing African societies. Surveillance technologies have been repeatedly employed in the region by illiberal regimes to track individuals and groups, block and censor data and information, and harass and repress critics and members of the opposition. More worrisome, on several occasions, Chinese companies have actively assisted these governments in stifling civil liberties and political rights. The widespread dissemination and implementation of these technologies through the growing number of smart city projects projected for Africa raise serious concerns for the future of democracy. Without the necessary safeguards, illiberal regimes can employ and exploit smart city technologies to expand and consolidate digital authoritarianism throughout the region.

CONCLUSION

Demographic growth and urbanization are creating significant challenges for African policymakers. Smart cities offer solutions to many of the predicaments facing today's urban settlements and have been embraced by officials across the region. As one of the main advocates of smart cities, Rwandan president Paul Kagame, argues "The word 'smart' is really about leveraging digital technologies to narrow the gap between the high quality services we need, and those we can afford, and to do so quickly."[83] However, it poses the question of who ultimately benefits from smart cities? Surely many of the technologies contribute to improving the lives of countless individuals and communities by optimizing urban products and services. Nevertheless, smart cities also pose a legitimate threat to civil liberties and political rights, particularly in fragile democracies.

Smart cities are generally promoted as mere technical solutions to urban problems. But, by embracing this view, many actors eschew addressing complex questions, particularly regarding the

relationship between government institutions and citizens. While many promoters and providers of smart city technologies may claim to simply satisfy the demands of emerging markets, their behavior ultimately allows illiberal regimes to exploit these technologies to suppress their citizens' civil liberties and political rights. Therefore, one must consider balancing development and security with liberties and rights.

Some have called for the sanctioning of digital authoritarians.[84] However, such coercive measures should only be considered as a last resort. A more constructive step is to promote and support greater regulation of smart city technology, particularly regarding personal data. To begin with, democratic governments should invest in building public awareness of the dangers of digital authoritarianism in both fragile democracies as well as in their own countries. Having robust and resilient democracies domestically is still the best way to promote political values internationally without appearing hypocritical. Therefore, liberal democracies need to take the lead in developing domestic regulatory frameworks protecting personal data and preventing state and private companies from abuses. Developing and implementing robust regulatory frameworks would create the impetus for promoting greater international governance for addressing the challenges posed by AI such as algorithmic bias, implicit discrimination, and privacy.[85]

To this end, several actors, most notably the EU, have already taken important steps in this direction and can provide a template to build standards that are compatible with civil liberties and political rights. Many African countries have already demonstrated they are amenable to these concerns when they signed on to the AU's Convention on Cyber Security and Personal Data Protection.[86] It is incumbent on democratic nations to capitalize on this opportunity to transcend geopolitical considerations and wholeheartedly embrace the region's democratic potential.

REFERENCES

[1] Sarah Repucci and Amy Slipowitz, "Freedom in the World 2022: The Global Expansion of Authoritarian Rule." Freedom House (Washington, DC: 2022).

[2] Josh Miller, Antoine Sander, and Sharath Srinivasan, "Control, Extract, Legitimate: Covid-19 and Digital Techno-Opportunism across Africa." *Development and Change* (2022): 1-25.

[3] Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models.* Brookings Institution (2019). https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

[4] United Nations, *World Population Prospects 2022: Summary Results.* Department of Economic and Social Affairs and Population Division, United Nations (New York: 2022). https://www.un.org/development/desa/pd/content/World-Population-Prospects-2022#:~:text=World%20Population%20Prospects%202022%20is,analyses%20of%20historical%20demographic%20trends.

[5] Ibid.

[6] United Nations, *World Urbanization Prospects: The 2018 Revision.* Population Division Department of Economic and Social Affairs, United Nations (New York: 2019). https://population.un.org/wup/publications/Files/WUP2018-Report.pdf.

[7] Urbanization refers to a "shift in a population from one that is dispersed across small rural settlements in which agriculture is the dominant economic activity towards one where the population is concentrated in larger, dense urban settlements characterised by industrial and service activities." United Nations, *World Urbanization Prospects: The 2014 Revision*. Department of Economic and Social Affairs (New York: 2015): 1.

[8] Mira Slavova and Ekene Okwechime, "African Smart Cities Strategies for Agenda 2063." *Africa Journal of Management* 2, no. 2 (2016): 210-29.

[9] Ibid, 584.

[10] Adaku Echendu and Peter Okafor, "Smart City Technology: A Potential Solution to Africa's Growing Population and Rapid Urbanization?" *Development Studies Research* 8, no. 1 (2021), 89.

[11] Vito Albino, Umberto Berardi, and Rosa Maria Dangelico, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives." *Journal of Urban Technology* 22, no. 1 (2015): 3-21; Andrés Camero and Enrique Alba, "Smart City and Information Technology: A Review." *Cities* 93 (2019): 84-94; Martina Fromhold-Eisebith, "Cyber-Physical Systems in Smart Cities - Mastering Technological, Economic, and Social Changes." In *Smart Cities: Foundations, Principles, and Applications*, edited by Houbing Song, Ravi Srinivasan, Tamim Sookoor and Sabina Jeschke (Hoboken, NJ: Wiley & Sons, 2017), 1-22.

[12] "Making African Cities Great." *African Smart Cities*, n.d. https://africansmartcities.info/.

[13] Lucas Melgaço and Rosamunde van Brakel, "Smart Cities as Surveillance Theatre." *Surveillance & Society* 19, no. 2 (2021): 244-49.

[14] Sarah Repucci and Amy Slipowitz, "Freedom in the World 2022: The Global Expansion of Authoritarian Rule." Freedom House (Washington, DC: 2022).

[15] Josh Miller, Antoine Sander, and Sharath Srinivasan, "Control, Extract, Legitimate: Covid-19 and Digital Techno-Opportunism across Africa." *Development and Change* (2022): 1-25.

[16] Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models.* Brookings Institution (2019). https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

[17] OECD, *Smart Cities and Inclusive Growth*. OECD (2020). https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf.

[18] Charalampos Alexopoulos, Gabriela Viale Pereira, Yannis Charalabidis, and Lorenzo Madrid, "A Taxonomy of Smart Cities Initiatives." *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* (Melbourne, 2019): 284.

[19] Hille Koselka and Liisa Mäkinen, "Surveillance." In *The International Encyclopedia of Geography*, edited by Douglas Richardson, Noel Castree, Michael Goodchild, Audrey Kobayashi, Weidong Liu and Richard Marston (Chichester: John Wiley & Sons, 2017) 1-9.

[20] Deloitte, *The Integrated Digital City* (Australia: Deloitte, 2019). https://www2.deloitte.com/content/dam/Deloitte/au/Documents/future-of-cities/deloitte-future-of-cities-dtt_citysynergy-whitepaper_20190423.pdf.

[21] Michael Porter and James Heppelmann, "How Smart, Connected Products Are Transforming Competition." *Harvard Business Review* 92, no. 11 (2014): 64-88.

[22] Idem.

[23] Koskela and Mäkinen, "Surveillance."

[24] David Murakami Wood and Debra Mackinnon, "Partial Platforms and Oligoptic Surveillance in the Smart City." *Surveillance & Society* 17, no. 1/2 (2019): 176.

[25] Gary T Marx, "What's New About the 'New Surveillance'? Classifying for Change and Continuity." *Surveillance & Society* 1, no. 1 (2002): 15.

[26] Lucan Way and Steven Levitsky, "The Dynamics of Autocratic Coercion after the Cold War." *Communist and Post-Communist Studies* 39, no. 3 (2006): 387-410.

[27] Feldstein, "Surveillance in the Illiberal State."; Steven Feldstein, "How Artificial Intelligence Is Reshaping Repression." *Journal of Democracy* 30, no. 1 (2019): 40-52; Ronak Gopaldas, *Digital Dictatorship Versus Digital Democracy in Africa*. South African Institute of International Affairs (2019). http://www.jstor.org/stable/resrep25956; Willem Gravett, "Digital Coloniser? China and Artificial Intelligence in Africa." *Survival* 62, no. 6 (2021): 153-78; Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy." *Foreign Affairs* 99, no. 2 (2020): 103-15; Eda Keremoğlu and Nils Weidmann, "How Dictators Control the Internet: A Review Essay." *Comparative Political Studies* 53, no. 10-11 (2020): 1690-703.

[28] Feldstein, "Surveillance in the Illiberal State."

[29] Kendall-Taylor and Wright, "The Digital Dictators."

[30] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Vintage Books, 1977).

[31] Idem.

[32] Ross Andersen, "When China Sees All." *The Atlantic Monthly* 326, no. 2 (2020): 60.

[33] Idem.

[34] Polyakova, and Meserole, *Exporting Digital Authoritarianism*; Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30, no. 1 (2019): 53-67.

[35] For these actors, Africa is part of a broader strategic outlook where technologies, particularly digital technologies, are critical to international geopolitical competition. Mathew Burrows, Julian Mueller-Kaler, Kaisa Oksanen, and Ossi Piironen, *Unpacking the Geopolitics of Technology.* Atlantic Council (Atlantic Council, 2021). https://www.atlanticcouncil.org/in-depth-research-reports/report/unpacking-the-geopolitics-of-technology/.

[36] Luis da Vinha and Hongyi Liang, "China vis-à-vis the EU: The Competition for Africa's Smart Cities." In *The Palgrave Handbook on China-Europe-Africa Relations: Legacies and the New International Order*, edited by Francisco Leandro, Jorge Tavares, Yichao Li, and Carlos Rodrigues (Switzerland: Palgrave Macmillan, forthcoming).

[37] Alice Ekman, *China's Smart Cities: The New Geopolitical Battleground* (Paris: Institut Français des Relations Internationales, 2019). https://www.ifri.org/en/publications/etudes-de-lifri/chinas-smart-cities-new-geopolitical-battleground.

[38] Ursula von der Leyen, *State of the Union 2020*. The European Commission. (2020). https://ec.europa.eu/info/sites/default/files/soteu_2020_en.pdf.

[39] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to the European Parliament and the Council on Strengthening the EU's Contribution to Rules-Based Multilateralism*. (2021). https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52021JC0003.

[40] In this case, Europe differs from the U.S. which has no federal data protection law. Benedikt Erforth and Kerstin Fritzsche. *Towards a Digital Development Partnership That Meets African Interests*. Heinrich-Böll-Stiftung (Washington, DC: 2022).

[41] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to the European Parliament and the Council: Towards a Comprehensive Strategy with Africa*. (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0004.

[42] European Council. *Sixth European Union – African Union Summit: A Joint Vision for 2030*. (2022). https://www.consilium.europa.eu/en/press/press-releases/2022/02/18/sixth-european-union-african-union-summit-a-joint-vision-for-2030/.

[43] Erforth and Fritzsche, *Towards a Digital Development Partnership That Meets African Interests*.

[44] Digital for Development Hub. *Supporting Africa's Digital Transformation*. (n.d.). https://d4dhub.eu/au-eu-project.

[45] Graham Allison, Kevin Klyman, Karina Barbesino, and Hugo Yen. *The Great Tech Rivalry: China vs the U.S.* Belfer Center for Science and International Affairs, Harvard Kennedy School (Cambridge, MA: 2021).

[46] David Abdulai, *Chinese Investment in Africa: How African Countries Can Position Themselves to Benefit from China's Foray into Africa* (London: Taylor & Francis, 2016)

[47] Nadège Rolland, "China's Southern Strategy: Beijing Is Using the Global South to Constrain America." *Foreign Affairs*. (June 9, 2022). Accessed July 1, 2022. https://www.foreignaffairs.com/articles/china/2022-06-09/chinas-southern-strategy.

[48] Ministry of Foreign Affairs of the People's Republic of China, "China Will Work with Africa to Formulate and Implement a China-Africa Partnership Plan on Digital Innovation" (24 August, 2021). https://www.fmprc.gov.cn/eng/wjbxw/202108/t20210825_9134687.html.

[49] Xi Jinping, "Work Together to Build the Silk Road Economic Belt and the 21st Century Maritime Silk Road." Ministry of Foreign Affairs of the People's Republic of China (14 May, 2017). https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/201705/t20170527_678618.html.

[50] Ekman, *China's Smart Cities*.

[51] Stephen Olson, "Are Private Chinese Companies Really Private?" *The Diplomat*. (2020). https://thediplomat.com/2020/09/are-private-chinese-companies-really-private/.

[52] Ekman, *China's Smart Cities*; Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports.* Brookings Institution (2020). https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf.

[53] Ministry of Foreign Affairs of the People's Republic of China, "Forum on China-Africa Cooperation Beijing Action Plan (2019-2021)" (December 9, 2018). http://focacsummit.mfa.gov.cn/eng/hyqk_1/201809/t20180912_5858585.htm.

[54] da Vinha and Liang, "China vis-à-vis the EU: The Competition for Africa's Smart Cities."

[55] State Council Information Office of China, *China: Democracy That Works*. Consulate General of the People's Republic of China in New York (2021). http://newyork.china-consulate.gov.cn/eng/xw/202112/t20211207_10463265.htm.

[56] Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports*; Charles Edel and David Schullman, "How China Exports Authoritarianism: Beijing's Money and Technology Is Fueling Repression Worldwide." *Foreign Affairs*. (September 16, 2021). https://www.foreignaffairs.com/articles/china/2021-09-16/how-china-exports-authoritarianism;

[57] Yujia He and Angela Tritto, "Urban Utopia or Pipe Dream? Examining Chinese-Invested Smart City Development in Southeast Asia." *Third World Quarterly* 43, no. 9 (2022): 2244-68; Rahul Karan Reddy, *Mapping China's Presence in Africa's Digital Economy*. Institute of Peace and Conflict Studies (July 15, 2021). http://www.ipcs.org/comm_select.php?articleNo=5776.

[58] Reddy, *Mapping China's Presence in Africa's Digital Economy*.

[59] There is debate as to whether China's model of digital development actively promotes authoritarianism or whether the misuse of the technologies is dependent on how countries that purchase the technologies use them. Mamoudou Gazibo, "Is Democracy Declining in Africa and What Role for China?" In *Revisisting EU-Africa Relations in a Chaging World*, edited by Valeria Fargion and Mamoudou Gazibo (Cheltenham: Edward Elgar Publshing, 2021), 252-266; He and Tritto, "Urban Utopia or Pipe Dream?"; Bulelani Jili, "The Spread of Chinese Surveillance Tools in Africa: A Focus on Ethiopia and Kenya." In *Africa-Europe Cooperation and Digital Transformation*, edited by Chux Daniels, Benedikt Erforth and Chloe Teevan (New York: Routledge, 2023), 32-49.

[60] Ogala Emmanuel, "How Governors Dickson, Okowa Spend Billions on High Tech Spying on Opponents, Others." *Premium Times* (9 June, 2016). https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html; Jili, "The Spread of Chinese Surveillance Tools in Africa."

[61] Kali Robinson, "How Israel's Pegasus Spyware Stoked the Surveillance Debate." *Council on Foreign Relations* (8 March, 2022). https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate.

[62] Steven Feldstein, "Surveillance in the Illiberal State." In *Routledge Handbook of Illiberalism*, edited by András Sajó, Renáta Uitz, and Stephen Holmes (New York: Routledge, 2022): 353.

[63] Idem.

[64] Laurence Côté-Roy and Sarah Moser, "'Does Africa Not Deserve Shiny New Cities?' the Power of Seductive Rhetoric around New Cities in Africa." *Urban Studies* 56, no. 12 (2019): 2391-407.

[65] He and Tritto, "Urban Utopia or Pipe Dream?"

[66] China Academy of Information and Communications Technology, and EU-China Policy Dialogues Support Facility II, *Comparative Study of Smart Cities in Europe and China 2014*. (Berlin: Springer, 2016).

[67] Femke van Noorloos and Marjan Kloosterboer, "Africa's New Cities: The Contested Future of Urbanisation." *Urban Studies* 55, no. 6 (2018): 1223-41.

[68] China offers several advantages to African nations by providing financial and technical assistance without the "conditionality" demanded by many Western actors. Xiaojun Li, "Does Conditionality Still Work? China's Development Assistance and Democracy in Africa." *Chinese Political Science Review* 2, no. 2 (2017): 201-20. Peter Dauvergne, "Facial

Recognition Technology for Policing and Surveillance in the Global South: A Call for Bans." *Third World Quarterly* (2022): 1-11; and Samuel Woodhams, "China, Africa, and the Private Surveillance Industry." *Georgetown Journal of International Affairs* 21, no. 3 (2020): 158-65. Some funding also comes from European and international institutions.

[69] Dipanjan Chaudhury, "China Reportedly Investing $8.43 Bn in Africa as Part of Digital Silk Road Initiative." *The Economic Times* (October 15, 2021). https://economictimes.indiatimes.com/news/international/world-news/china-reportedly-investing-8-43-bn-in-africa-as-part-of-digital-silk-road-initiative/articleshow/87039334.cms.

[70] Côté-Roy and Moser, "'Does Africa Not Deserve Shiny New Cities?'"; van Noorloos and Kloosterboer, "Africa's New Cities."

[71] Jonathan Hillman and Maesea McCalpin, "Watching Huawei's 'Safe Cities'." Center for Strategic & International Studies. (2019). https://www.csis.org/analysis/watching-huaweis-safe-cities.

[72] Idem: 3.

[73] Monitor, "Across East Africa, Big Brother Is Watching Your Every Move." *Monitor* (December 3, 2022). https://www.monitor.co.ug/uganda/news/national/across-east-africa-big-brother-is-watching-your-every-move-4041896.

[74] Stephen Kafeero, "Uganda Is Using Huawei's Facial Recognition Tech to Crack Down on Dissent after Anti-Government Protests." *Quartz* (November 27, 2020). https://qz.com/emails/daily-brief/1849871650/china-and-saudi-arabia-get-chummy.

[75] David Ehl, "Africa Embraces Huawei Tech Despite Security Concerns." *DW*. (February 8, 2022). https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700.

[76] Kafeero, "Uganda Is Using Huawei's Facial Recognition Tech to Crack Down on Dissent after Anti-Government Protests."

[77] Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents." *The Wall Street Journal*. (August 15, 2019). https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[78] Sarah Chiumbu, "Chinese Digital Infrastructure, Smart Cities and Surveillance in Zambia." Media Policy and Democracy Project (2021). https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/zambia_report.pdf.

[79] Idem.

[80] Parkinson, Bariyo, and Chin. "Huawei Technicians Helped African Governments Spy on Political Opponents."

[81] Chiumbu, "Chinese Digital Infrastructure, Smart Cities and Surveillance in Zambia."

[82] Ghalia Kadiri and Joan Tilouine, "A Addis-Abeba, le Siège de l'Union Africaine Espionné par Pékin." *Le Monde*. (January 27, 2018). https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

[83] Paul Kagame, *Address by President Kagame at Transform Africa Summit*. (May 10, 2017). https://www.paulkagame.com/address-by-president-paul-kagame-transform-africa-summit-2017-kigali-10-may-2017/.

[84] Polyakova and Meserole, *Exporting Digital Authoritarianism*.

[85] Feldstein, "How Artificial Intelligence Is Reshaping Repression."

[86] Gravett, "Digital Coloniser?"; Greitens, *Dealing with Demand for China's Global Surveillance Exports.*