FRIEDRICH NAUMANN FOUNDATION For Freedom.

CHINA'S DIGITAL INFLUENCE IN AFRICA

The Case of Zambia and Zimbabwe

Christopher Musodza with Kuda Hove and Otto Saki

ANALYSIS

Imprint

Publisher
Friedrich-Naumann-Stiftung für die Freiheit
Truman Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg
Germany

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit

Authors
Christopher Musodza (Lead author),
Kuda Hove and Otto Saki (Co-authors)

Editor
Ann Cathrin Riedel,
Policy Advisor Global Digitalisation & Innovation
Division Global Themes, Department Research and Political Strategy

Contact
Phone: +49 30 22 01 26 34
Fax: +49 30 69 08 81 02
email: service@freiheit.org

Date
November 2022

Table of contents

Key recommendations

The infrastructural development by Zambia and Zimbabwe in the technology and telecommunications sector has largely been through investments from China, either private sector driven or through state-to-state engagements, though most private actors from China operate with state approval or support. There are mixed levels of understanding and appreciation of the deployment of Chinese technology due to a lack of transparency in the various contracting processes and agreements.

1. Legal and Policy Frameworks

For both countries there is a need for legal and policy frameworks that increase transparency in surveillance activities and build state accountability in the way it conducts its surveillance activities. These policies and legal provisions must be consistent with human rights practices, in compliance with international and regional standards. The alignment of national laws requires Zambia and Zimbabwe to sign on to regional instruments, such as the African Union's Convention on Cyber Security and Data Protection.

2. Transparency in Procurement and Contracting

Most African governments, Zambia and Zimbabwe being no exception, have limited transparency in respect of large state contracts or loans, despite provisions in their national laws. There is need for more transparency around the procurement of technologies to carry out state-sponsored surveillance, as well as technologies which have the potential to be repurposed for surveillance. This contracting transparency must also cover infrastructure development that creates room for abuse of genuine projects to advance surveillance.

3. Oversight of existing surveillance infrastructure

Legal limitations to be applied to surveillance activities to ensure surveillance is conducted only when it is lawful, necessary and proportionate. The internet and technology boom has seen many laws being enacted, which together with existing surveillance laws need to be evaluated against human rights principles and standards. Existing surveillance institutions and agencies in Zambia and Zimbabwe have limited accountability, parliamentary or judicial oversight. Reports by any surveillance, capable or empowered, agencies must be presented in Parliament.

4. Privacy impact assessments on technology

The introduction of oversight and accountability measures to specify privacy impact assessments before the adoption and rollout of any technology deployed on a massive scale. Privacy impact assessments must be mandatory for all public agencies, in particular telecommunications agencies, national registration authorities, mobile and telecommunications operators, and access and internet service providers (ASP/ISPs), which reports be publicly available.

5. Regional and global regulation of trade in surveillance tools

Digital rights advocates to be supported to document accurately and investigate any acts of state-sponsored surveillance technologies, along with the nature of the surveillance and its potential harms. Stronger regulation is required to strengthen international and regional mechanisms to hold countries accountable, mainly those manufacturing surveillance capable technologies. All countries that provide and sell surveillance tools which are being used to infringe citizens' fundamental rights, must

1. Introduction

Zambia and Zimbabwe inherited a raft of surveillance laws from the colonial governments that once governed those two countries, which have continued to be used for conducting surveillance activities, ostensibly for national security but in reality for consolidating political power. China's relationship with the two countries, along with its own ambitions to dominate the manufacture and supply of technologies globally, have created fertile ground for China to supply surveillance technologies to the southern African countries, which are comparatively cheaper than those from other parts of the world. Over the past decade, a number of media reports have chronicled the adoption and rollout of Chinese sourced technologies in the telecommunications industries of these two countries, although these have tended not to examine how the different layers of Chinese technologies may be used by the Zambian and Zimbabwean governments to carry out targeted and mass surveillance.

The use of Chinese technologies for surveillance purposes does not take place in a vacuum and both countries use legislation that enables the often-unjustifiable use of surveillance technologies on unsuspecting members of the public that curtails their enjoyment of their fundamental rights. China is not foisting these technologies on African states. Both historical and current political and economic relations make these governments more amenable to such technological and security cooperation.

This research paper seeks to identify then discuss some of the key factors which have led to the adoption of Chinese surveillance technologies in Zambia and Zimbabwe. The two countries have been chosen because of their strategic interest to Friedrich Naumann Foundation for Freedom. In both countries, the press has revealed an increase in the use of state sponsored surveillance programs but there has been little in the way of research which seeks to understand the factors driving the introduction of such surveillance mechanisms in either country.

2. Methodology

The research findings are drawn from desk research, combined with key informant interviews based on an online survey sent to a selected group of people in Zambia and Zimbabwe with experience of state sponsored surveillance and the use of Chinese technologies.

3. Background: China's Strategy for Strategic Influence and Surveillance

The role of China both in digital information and technology development and the supply of surveillance technologies and infrastructure is not a straightforward discourse, as with most debates on the role of China in the world. China's rising position, demonstrated by its capacity to reduce poverty for millions of Chinese nationals, develop modern infrastructure, become a major global manufacturing hub of technology items, has led much of the global south to seek or strengthen partnerships with China. China was a key supporter in the political and liberation struggles in Zambia and Zimbabwe. After independence from Britain, both countries strengthened their diplomatic and economic ties with China through reciprocal arrangements and major infrastructure projects, as well as military exchanges.

This part of the research follows a number of themes which uncover some of China's reasons for producing and exporting surveillance technologies. Having outlined and discussed China's reasons for exporting surveillance technologies, the conversation will focus on how those plans coincide with an environment which is conducive for the use of such technologies in Zambia and Zimbabwe.

3.1 China's Digital Silk Road and Associated Concerns

From as early as 1964 China developed principles to guide their economic and technical assistance that were presented as reaffirming national sovereignty, removing conditio-

nalities, and aid dependency. These principles are outlines in the Digital Silk Road (DSR), the digital dimension of the Belt and Road Initiative (BRI) supported by the Chinese President Xi Jinping.[1] The Chinese government gives support and preferential treatment to telecommunications companies through lines of credit from state owned banks, which allows these firms to win major telecommunications infrastructure projects with lower costs. Civil society, privacy and surveillance watchdogs are concerned about the possibilities this opens for privacy violations, illicit data collection and risks to other freedoms.[2]

The biggest concern with this rolling out of telecommunications technologies is that China may use the data generated through the infrastructure it has supplied to enhance its own position as a global superpower, as well as using the technologies for surveillance purposes. The Council on Foreign Relations (American think tank) observed that the actions of the Chinese government in installing backdoors in encryption technology increase its intelligence and propaganda capacities.[3] China, through its Digital Silk Road activities, is partnering mainly with low and middle-income countries in the Middle East, Asia, and Africa, most of which, including Zambia and Zimbabwe, have poor human rights records, disregard for the rule of law and an appetite for surveillance. These factors make it likely that some, including Zambia and Zimbabwe, will intentionally use Chinese technologies to carry out surveillance activities and the Chinese manufacturers are not deemed bold enough to refuse to work with national law enforcement and security agents.[4]

3.2 The Emergence of Digital Authoritarianism

China dominates Africa's telecommunications infrastructure, supplying approximately 70 percent of the continent's internet networks. Most African countries see the development of infrastructure and communications as a sign of developmental progression.[5] And yet governments are known to be using information technology to carry out surveillance, repression and manipulation of views, which impact adversely on democratic practices, including holding of free and fair elections, freedom of expression, and right to privacy. Such practices are not limited to non-democratic countries but also found in democratic liberal leaning regimes.[6]

The USA, for example, banned the Chinese TikTok application owned by Byte Dance, alleging surveillance and data gathering for Chinese authorities.[7] China itself has used firewalls to block social media platforms such as Facebook, and Twitter inside China since 2009[8] even though Chinese diplomats are active on these platforms defending Chinese policies.[9] Other countries have stated security concerns about the unauthorised use of personal information and data transfers to outside data storage facilities to drive similar decisions to ban platforms.[10]

3.3 China's geopolitical and economic gains from exporting surveillance technologies

China's geopolitical interests and authoritarian "instincts" are not the only explanations of its motivation to build 5G networks abroad. Several Chinese technology manufacturers allegedly build backdoors into their technology platforms and systems, which are used to harvest user data surreptitiously to send back to the manufacturer, without the users' consent or knowledge. In this instance, Chinese technology manufacturers may be motivated to roll out their surveillance technologies as a way to gather data that may be useful in developing and improving their technologies. If Chinese technologies are more accurate in processing biometric information belonging to diverse races, information that they could use in future to target people and nations, they would have a competitive edge over other similar Western technologies, which are less accurate in the processing of biometric data of racial groups.

1 Yong, H. (2019, April 24). *Construction of digital Silk Road lights up BRI cooperation - People's Daily Online.* Retrieved October 17, 2022, from http://en.people.cn/n3/2019/0424/c90000-9571418.html
2 Omolaoye. S. (2022, March 1). *Doubts, queries over China's interest in Nigeria's telecom sector.* The Guardian Nigeria News - Nigeria and World News. Retrieved October 17, 2022, from https://guardian.ng/features/doubts-queries-over-chinas-interest-in-nigerias-telecom-sector/
3 Chandran, N. (2018, July 12). *Surveillance fears cloud China's "Digital Silk Road."* CNBC. Retrieved October 17, 2022, from https://www.cnbc.com/2018/07/11/risks-of-chinas-digital-silk-road-surveillance-coercion.html
4 Whereas manufacturers such as Blackberry and Apple have in the past refused to comply with requests to breach the privacy of their users at the behest of national law enforcement and security agencies.
5 Mackinnon, A. (2019, March 19). *For Africa, Chinese-Built Internet Is Better Than No Internet at All.* Foreign Policy. Retrieved October 17, 2022, from https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/
6 Coleman, V., & Napolitano, J. (2022, March 14). *Digital authoritarianism is on the rise, and democracies can't stand on the sidelines.* Foreign Policy. Retrieved October 17, 2022, from https://foreignpolicy.com/2022/03/14/digital-authoritarianism-tech-human-rights/
7 Merrill, N., & Komaitis, K. (2020, December 17). *The consequences of a fragmenting, less global internet.* Brookings. Retrieved October 17, 2022, from https://www.brookings.edu/techstream/the-consequences-of-a-fragmenting-less-global-internet/
8 Barry, E. (2022, January 18). *These Are the Countries Where Twitter, Facebook and TikTok Are Banned.* Time. Retrieved October 17, 2022, from https://time.com/6139988/countries-where-twitter-facebook-tiktok-banned/
9 Brandt, J., & Schafer, B. (2021, November 17). *How China's 'wolf warrior' diplomats use and abuse Twitter.* Brookings. Retrieved October 17, 2022, from https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/
10 Ministry of Electronics & IT (2020, June 29). *Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order.* Retrieved October 17, 2022, from https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206#

4. Public-Private-Surveillance Partnerships in Africa and beyond

Digital surveillance requires some form of infrastructure to operate. Mass surveillance is usually conducted through the monitoring and interception of communications, and this form of surveillance is conducted over telecommunications infrastructure. That is why it is important to understand the level of prevalence of Chinese digital infrastructure which may be vulnerable to use for surveillance purposes.

Africa has a huge infrastructure gap which is being addressed through Chinese infrastructure support coming either in government-to-government partnerships or with a private sector implementation arm, usually Huawei or ZTE.

The Australian Strategic Policy Institute International Cyber Policy Centre has produced analysis and coverage of over 27 Chinese firms providing different services, including artificial intelligence, facial recognition, 5G, biotechnology, surveillance, e-commerce, finance and entertainment.[11] The clients and receivers of these services are both national governments and local authorities, such as Huawei-Gelsenkirchen Smart City Project, Germany (2019)[12] and the Smart Zambia project in partnership with Huawei. They also engage private mobile telecommunications operators or internet service providers interested in the setting up of independent 5G networks, such as Huawei-Rain South Africa (2020).

Table 1 | ...

INVESTMENT	LOCATIONS
Research partnerships	America, Europe, Asia, Africa
Technical and capacity building (students, IT workers)	Africa, Asia, South America
Smart City	Europe, South America and Africa
5G infrastructure	Europe, Africa, Asia
Data centres	Asia, Africa, Europe, South America
Critical Infrastructure (internet exchange points, cabling, buildings)	Africa, Asia
Digital Identities	Africa, Asia

Source: authors; ASPI Mapping

5. TikTok, WeChat, FortNite – Chinese surveillance through consumer products

China has positioned itself as a global leader in the development and export of video games and Apps, which are widely accepted as having surveillance capabilities. One example which has gained global popularity is *TikTok*, a short video sharing platform and App, developed by the Chinese company ByteDance, which by 2021, just 5 years after its launch, was ranked the most visited website in the world, surpassing Google.[13] Along with its massive growth have been concerns over the user privacy. In June 2020, India banned *TikTok* and 58 other Chinese developed applications, citing "concerns that these apps were engaging in activities that threatened "national security and defence of India, which ultimately impinges upon the sovereignty and integrity of India.'"[14] At the time, India was *TikTok*'s biggest market outside of mainland China. Similarly, in August 2020, then US president Donald Trump banned *TikTok* and *WeChat* from transacting in the US and with any US based companies.[15] (Although this ban was reversed in June 2021 by current US president Joe Biden.)

Most recently TikTok has been warned by several European Union data protection authorities, that its plans to use large-scale data mining and profiling to introduce targeted adver-

11 Brandt, J., & Schafer, B. (2021, November 17). *How China's 'wolf warrior' diplomats use and abuse Twitter.* Brookings. Retrieved October 17, 2022, from https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/

12 Huawei (2019, February 28). *Huawei and Gelsenkirchen Sign MoU for Smart City Cooperation at MWC2019.* Retrieved October 17, 2022, from https://archive.fo/WCmIu#selection-2591.0-2591.71

13 Adey, O. (2021, December 23). *2022 - TikTok becomes most visited website, surpassing Google.* The Latest News. Retrieved October 17, 2022, from https://gettotext.com/tiktok-becomes-most-visited-website-surpassing-google/

14 Singh, M. (2020, June 29). *India bans TikTok, dozens of other Chinese apps.* Retrieved October 17, 2022, from https://tcrn.ch/3gaX2nW

15 Carvajal, N., & Kelly, C. (2020, August 7). *Trump issues orders banning TikTok and WeChat from operating in 45 days if they are not sold by Chinese parent companies.* CNN. Retrieved October 17, 2022, from https://edition.cnn.com/2020/08/06/politics/trump-executive-order-tiktok/index.html

tising without user consent were in violation of the EU's General Data Protection Regulations (GDPR) including Ireland's Data Protection Commission is currently investigating *TikTok* in relation to the processing of children's personal data and transfers of personal data to China.[16,17]Additionally, a Forbes investigation revealed ByteDance's plans to monitor targeted United States of America based individuals using their *TikTok* location data.[18] This revelation shows ByteDance's ability to use *TikTok* to monitor persons of interest in other jurisdictions including Zambia and Zimbabwe.

WeChat is an App developed by the Chinese company Tencent, which is pushing to gain traction across the African continent.[19] (It should be noted that these companies are global in terms of their shareholders, which are spread across Europe, America and Africa.) Unlike *TikTok*, viewed mostly as a leisure/ entertainment App, *WeChat* combines a number of functions: instant messaging, money transfers, prepaid electricity and airtime purchases. In South Africa, *WeChat* has partnered with local entities such as Standard Bank to offer mobile money services. By 2015, *WeChat* had 5 million registered users in South Africa while WhatsApp had 10 million users. Digital rights organisations like Mozilla have raised privacy and security concerns over *WeChat*.[20]

Chinese video game companies have developed or are involved in the publishing of globally dominant online gaming titles such as FortNite, PUBG, and Call of Duty: Mobile. Some of the privacy concerns of these games include the use of a real name policy, which requires online gamers to use their real names on their gaming profiles. Another privacy concern stems from Tencent's announcement in July 2021 that it was incorporating facial recognition technology[21] in its games for age verification purposes to ensure compliance with the Chinese government's rule on allowing young gamers to play games for only a limited amount of time each day.

The possibility that these Apps and games send information to Chinese servers, coupled with the fact that facial recognition technology and other forms of spyware may be added onto these platforms and games, raises legitimate concerns that these Apps and video games may be quietly repurposed for surveillance of their users, by either the corporations themselves or at the behest of governments.

6. Built-in surveillance: Chinese-Constructed Government Buildings Across Africa

To date Chinese corporations have constructed some 186 government buildings throughout Africa and 14 intra-governmental telecommunication networks, all such corporations being required by law to assist the Chinese Communist Party in gathering intelligence.[22] In January 2018 the French newspaper *Le Monde* reported that the servers installed by the Chinese telecommunications company Huawei in the African Union (AU) headquarters were uploading their content to servers in Shanghai, China. The Financial Times newspaper corroborated Le Monde's account three days later. The AU building, constructed by the state-owned China State Construction Engineering Corporation, was also found during an inspection to include listening devices. It is possible that Beijing has digital surveillance on a much wider range of African government facilities than just the AU headquarters.

16 Euronews. (2022, July 13). *TikTok delays changes to privacy policy for targeted advertising over Europe data concerns.* Retrieved October 17, 2022, from https://www.euronews.com/next/2022/07/13/tiktok-delays-changes-to-privacy-policy-for-targeted-advertising-over-europe-data-concerns
17 Euronews. (2022, July 13). *TikTok delays changes to privacy policy for targeted advertising over Europe data concerns.* Retrieved October 17, 2022, from https://www.euronews.com/next/2022/07/13/tiktok-delays-changes-to-privacy-policy-for-targeted-advertising-over-europe-data-concerns
18 Baker-White, E. (2022 October, 20). *TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens.* Retrieved October 23, 2022, from https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=5e69225d6c2d
19 Motsoeneng, T. (2016, July 22). *China's WeChat takes on WhatsApp in Africa.* U.S. Retrieved October 17, 2022, from https://www.reuters.com/article/us-messaging-africa-idUSKCN10205A
20 Mozilla. (2021, September 8). **Privacy Not Included: WeChat.* Retrieved October 17, 2022, from https://foundation.mozilla.org/en/privacynotincluded/wechat/
21 Baron, J. (2018, November 1). *Chinese Video Game Using Facial Recognition To Monitor Its Players.* Forbes. Retrieved October 17, 2022, from https://www.forbes.com/sites/jessicabaron/2018/11/01/chinese-video-game-using-facial-recognition-to-monitor-its-players/
22 Meservey, J. (n.d.). *Government Buildings in Africa Are a Likely Vector for Chinese Spying.* The Heritage Foundation. Retrieved October 17, 2022, from https://www.heritage.org/asia/report/government-buildings-africa-are-likely-vector-chinese-spying

7. A closer look: Chinese Technologies and Companies in Zambia and Zimbabwe

More than 70% of Africa's 4G networks were built by Huawei,[23] and the company is moving forward with plans to set up 5G networks on the continent. Huawei, ZTE and other Chinese telecoms have built and / or outfitted at least 14 government networks, including dedicated military and police telecoms systems, providing surveillance capabilities beyond just telecommunications infrastructure. Chinese entities such as Huawei also produce a diverse range of consumer devices such as mobile phones, mobile Wi-Fi devices, laptops, tablets Wi-Fi routers for the home. In instances where a Chinese manufacturer builds backdoors or vulnerabilities which may be exploited by State security agencies, the diverse products would ensure a wide range of surveillance entry points and methods available to the state.

In Zambia and Zimbabwe, Huawei and ZTE have played a major role in providing the telecommunications infrastructure. Having introduced 3G technology to Zambia in 2009, Huawei was then contracted to supply and install cell phone towers across parts of rural Zambia in 2015. In 2017 the national data centre, financed by Chinese banks, and the technology and equipment provided by Huawei, was handed over to the Zambia Information and Communications Technology Authority (ZICTA). Total cost for this data centre was estimated to be $75 million.[24]

Huawei and ZTE have also contributed to the core national telecommunications infrastructure in Zimbabwe. In 2010, Econet, Zimbabwe's largest mobile network operator, launched its plans to build links to the SEACOM and EASSy submarine fibre optic cable systems,[25] along with a 7,500-kilometre fibre network connecting all major cities in Zimbabwe.[26] Huawei was the technical partner and supplier for these contracts. In 2015, Econet Wireless announced a $500 million loan from the China Development Bank and Huawei's Chinese state-owned competitor in the telecommunications equipment market, ZTE. In 2019, Econet was reported to team up with ZTE to replace redundant core network components, originally supplied by Ericsson.

In 2015, the state-owned mobile network operator NetOne started rolling out an LTE network upgrade led by Huawei, worth an estimated $218 million financed via a loan received from the China Exim Bank.[27] In 2017, NetOne received an additional US$71 million from China Exim Bank for Huawei to expand and upgrade its networks. In 2019, TelOne, the state-owned telecommunications service provider, commissioned its National Backbone Fibre Link, culmination of a US$23,6 million project funded by the China Exim Bank and built by TelOne and Huawei. An indication of the close ties enjoyed by Zimbabwe and Huawei was the tax exemption granted by the Zimbabwean government to Huawei in 2020, backdated to apply from December 2009.[28]

Both state owned and private media in both countries have reported widely on the different public private partnerships and other agreements between the governments of the two countries and Huawei or ZTE. However, there is less transparency about the extent of surveillance conducted through the use of the national telecommunications infrastructure. There is a lack of public information on the extent of state surveillance undertaken in terms of laws that enable surveillance in Zambia[29] and Zimbabwe[30]. These laws do not provide any avenues for public scrutiny, for example, having telecommunications companies report how many interception requests they received from state security or law enforcement entities.

The surveillance laws also do not place any duty on the state or judiciary proactively to provide information on the number of interception of communications warrants applied for or processed. Surveillance activities are classified as national security endeavours and as a result are immune from parliamentary and judicial oversight or scrutiny. This sense of autonomy is bolstered by the fact that the security and intelligence agencies responsible for surveillance are under the direct authority of the President's office.

Survey participants cited Huawei and Hikvision as suppliers of surveillance cameras introduced to monitor public spaces deemed crime hotspots, traffic and a country's borders. Huawei was identified as one of the main suppliers of technology and infrastructure used in the national data centres in Zambia and Zimbabwe. Additionally, in Zimbabwe, Huawei is believed to play a major role in the design of the Cyber Security and Monitoring Interception of Communications Centre.[31] The

23 Deutsche Welle (www.dw.com). (n.d.). *Huawei, Africa and the global reach of surveillance tech.* Retrieved October 17, 2022, from https://www.dw.com/en/huawei-africa-and-the-global-reach-of-surveillance-technology/a-50398869
24 Moss, S. (2017, February 3). *Huawei's $75m Zambian data center readies for launch.* Data Center Dynamics. Retrieved October 17, 2022, from https://www.datacenterdynamics.com/en/news/huaweis-75m-zambian-data-center-readies-for-launch/
25 Techzim. (2011, April 15). *Econet connects to SEACOM undersea fibre cable.* Techzim. Retrieved October 17, 2022, from https://www.techzim.co.zw/2010/12/econet-connects-to-seacom/
26 Swart, H., & Munoriyarwa, A. (2020, May). *The Case of Zimbabwe. In Video Surveillance in Southern Africa: Case studies of security camera systems in the region* (p. 57). Retrieved October 17, 2022, from https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf
27 Musarurwa, T. (2015, April 19). *Huawei completes first phase of NetOne project.* Retrieved October 17, 2022, from https://www.herald.co.zw/huawei-completes-first-phase-of-netone-project/
28 Moyo, A. (2020, February 5). *Furore as Zim exempts Huawei from tax obligations.* ITWeb. Retrieved October 17, 2022, from https://www.itweb.co.za/content/RgeVDqPoxBQMKJN3
29 Cyber Security and Cyber Crimes Act, 2021
30 Interception of Communications Act, 2007
31 Established in terms of the Interception of Communications Act as amended by the Cyber Security and Data Protection Act, 2021

absence of adequate privacy frameworks which enables the repurposing these technologies is a concern.[32]

In addition to supplying equipment for the core national telecommunications infrastructures in Zambia and Zimbabwe, Chinese manufactured devices are used by the majority of citizens in both countries. Another Chinese company, Transsion Holdings, was the leading supplier in 2017 of mobile devices in Africa, surpassing more established brands such as Samsung.[33] While countries such as Australia, the UK and Canada are banning the use of Chinese sourced 5G infrastructure and technologies over surveillance fears, African countries, including Zambia and Zimbabwe are engaging Chinese manufacturers in the rollout of 5G coverage in their countries.[34]

The Western governments' push against use of Chinese manufactured 5G equipment is based initially on the belief that the companies are subservient to the Chinese government and prone to be forced to include backdoors in the hardware and software, to give Beijing remote access. Secondly, eavesdropping is a risk, even though security experts believe any efforts to listen in would be detected by the host country. A third concern is the possibility that in the event of a larger geopolitical conflict Beijing could use its access to degrade or disrupt communications services which run on networks built on Chinese manufactured 5G technology.[35]

The move from a paper-based voter registration system to a biometric voter registration has provided governments in Zambia and Zimbabwe with more tools that can be repurposed for mass or targeted surveillance. Zambia engaged a German firm[36] for the registration for identity cards, and an American based firm for the biometric voter registration exercise[37] In this case these were not Chinese service providers but the data collected from these registration exercises will be stored in the national data centre, which runs on equipment from Huawei. In Zimbabwe, the government engaged Laxton, a Chinese based supplier for its biometric voter registration[38].

A stark example of how the repurposing of biometric databases can lead to real harm played out in Afghanistan when the US military and its allies pulled out of the country in 2021, leaving it in the hands of the Taliban. Biometric databases which contained data and information of Afghanis who had worked with the US military and other foreign entities were used by Taliban to track and target them.[39] Biometric data collected during national registration and voter registration exercises must be protected with legal frameworks to ensure that the biometric data is not misused.

7.1 Surveillance to consolidate political power

As part of the research survey, that was part of this study, participants were asked to identify factors they believed were drivers of surveillance. These are some of their answers:

> *"Digital authoritarianism is being promoted as a way for governments to control their citizens through technology, inverting the concept of the internet as an engine of human liberation."*

> *"Authoritarian governments use surveillance to monitor the activities of opposition parties, civil society organisations, journalists and human rights advocates and activists who present a threat to governments."*

> *"In most cases the main purpose of digital surveillance is to consolidate power, undermine human and consumer rights while enforcing capitalist systems of extraction of citizen's data which include surveillance, automated decision making, facial recognition systems. They use surveillance to track terrorists and criminals, snoop on political opponents, and spy on citizens."*

Fundamental rights seen as being eroded by surveillance include the right to free expression, access to information and the right to association and assembly.[40]

> *"Digital surveillance has a negative impact on freedom of expression – as experienced in Zambia over the last 10 years. I believe the last government stifled free expression so badly they didn't even notice how much the people hated them."*

32 Harris, L. B. (2021, September 20). *Activists worried street cameras could be used to spy on citizens.* Retrieved October 17, 2022, from https://cite.org.zw/activists-worried-street-cameras-could-be-used-to-spy-on-citizens/
33 Dahir, A. L. (2022, July 21). *China's Transsion dominates Africa's phone market with Tecno, Itel.* Quartz. Retrieved October 17, 2022, from https://qz.com/africa/1374404/chinas-transsion-dominates-africas-phone-market-with-tecno-itel/
34 *MTN, Huawei pilots Zambia's first-ever 5G network.* (2022, January 12). Capital Business. Retrieved October 17, 2022, from https://www.capitalfm.co.ke/business/2022/01/mtn-huawei-pilots-zambias-first-ever-5g-network/
35 Schneier, B. (2020, February 24). *Besides Potential Chinese Backdoors, 5G Has Security Problems the United States Doesn't Want to Fix for Its Own Surveillance Purposes.* Foreign Policy. Retrieved October 17, 2022, from https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/
36 Zulu, B. (2020, May 29). *Biometric citizen identification to enhance voter registration and identification in Zambia.* Biometric Update |. Retrieved October 17, 2022, from https://www.biometricupdate.com/202004/biometric-citizen-identification-to-enhance-voter-registration-and-identification-in-zambia
37 *Voter registration extended in 3 provinces in Zambia.* (2015, July 23). Smartmatic. Retrieved October 17, 2022, from https://elections.smartmatic.com/voter-registration-extended-in-3-provinces-in-zambia/
38 The Engine Room. (2020) *Digital ID in Zimbabwe: A case study.* Retrieved October 17, 2022, from https://digitalid.theengineroom.org/assets/pdfs/%5BEnglish%5D%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
39 *Afghanistan: What Now After Two Decades of Building Data-Intensive Systems?* (2021, August 19). Privacy International. Retrieved October 17, 2022, from https://www.privacyinternational.org/news-analysis/4615/afghanistan-what-now-after-two-decades-building-data-intensive-systems
40 Gullo, K. (2016, May 19). *Surveillance Chills Speech — As New Studies Show — And Free Association.* Electronic Frontier Foundation. Retrieved October 17, 2022, from https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association

7.1.1 State surveillance to suppress opposition and activists

Surveillance has been used in Zambia and Zimbabwe to target and persecute prominent civil society leaders, opposition political leaders and party members and other dissenting voices. In Zambia, Huawei technicians allegedly helped the government access phones and social media pages of bloggers critical of the then Zambian President Lungu's government. Zambia's cyber-surveillance unit was able to locate the bloggers' locations, leading to their arrest, although there was no confirmed evidence that Huawei approved the use of its technology for the purpose.[41]

In Zimbabwe, information collected through communications surveillance was used by the State to dispute a claim that two female members of the opposition were kidnapped, tortured and sexually assaulted by suspected state security agents or members of the ruling party. The Minister of Home Affairs at a press conference shared what he claimed was the location data from both women's mobile phones and car movement to show that they had not been kidnapped but rather wilfully spent time away from Harare.[42] This incident demonstrates the State's use of surveillance although there is no evidence whether these surveillance tools were Chinese sourced.

7.1.2 National security as a pretext for surveillance

National security interests have been used by governments, including the Zambian and Zimbabwean governments, to curtail the legitimate exercise of fundamental rights[43] and democratic political processes such as voting. National security has also been used to justify the drafting and introduction of laws restricting access to information on government activities.

National security interests were cited in the Zimbabwean government's justification for engaging with CloudWalk Technology in 2018, allegedly to improve security and passenger immigration processing at airports when in fact, Zimbabwe was to receive technology to enable the rollout of "... a large-scale facial recognition program throughout the country" that would "... primarily [be] used in security and law enforcement and will likely be expanded to other public programs."[44]

As part of the public-private partnership with CloudWalk Technology, the Zimbabwean government was to turn over biometric data to be used to train CloudWalk's AI to differentiate between facial images and other biometric features of Black people.[45] It is reported the agreement stalled when the Zimbabwean government asked for a discount after learning that facial data would be transmitted to China to help the company perfect its AI technology.

7.1.3 Smart Cities with included state surveillance

Another driver of surveillance identified by survey participants was the repurposing of Smart Cities technologies. China and Zambia are engaged in projects purporting to promote public safety and service delivery. One such project, wholly backed by China, is the Safe City project, a component of the wider Smart City agenda that Zambia embarked on in 2015, with Huawei and ZTE being the main suppliers of technology and infrastructure.[46] In theory, Smart Cities use a variety of Internet-connected technologies (IoT) and databases to improve the efficiency and efficacy of city services, primarily by enabling greater connectivity between service suppliers and consumers. But when Smart Cities are rolled out in jurisdictions which lack adequate checks and balances, such as human rights-based privacy frameworks, the infrastructure may be repurposed for broad and targeted surveillance purposes.[47]

In 2020, Zambia deployed two road surveillance camera projects, Advanced Road Safety Management System (ARSMS) and the Intelligent Mobility Solutions (IMS).[48] The introduction of road traffic cameras on the country's busiest roads and surveillance cameras at crime hotspots was a good initiative on paper but, as China's own experience with Smart Cities has shown, these technologies can be repurposed to restrict fundamental rights such as the right to association and assembly and the right to privacy. 18 of the 20 cities under highest surveillance are in China. Data gathered in part through Smart City infrastructure is used to determine a citizen's standing on the national social scoring system,[49] which critics argue is aimed at regulating behaviour and mass surveillance to enable the government to control every facet of citizens' lives.

41 Villas-Boas, A. (2019, August 14). *Huawei technicians have been helping governments in Uganda and Zambia spy on their political opponents, a new report says.* (2019, August 14). Business Insider Nederland. Retrieved October 17, 2022, from https://www.businessinsider.nl/huawei-workers-helped-african-governments-spy-opponents-report-2019-8?international=true&r=US

42 The Sunday Mail. (2020, June 4). *MDC abduction claims not adding up: Minister Kazembe.* Retrieved October 17, 2022, from https://www.sundaymail.co.zw/mdc-abduction-claims-not-adding-up-minister-kazembe

43 Committee on Legal Affairs and Human Rights. (2015, January 26). Resolution and Recommendation on Mass Surveillance. Retrieved October 17, 2022, from https://www.scribd.com/document/253848295/Mass-Surveillance-Report

44 Chutel, L. (2022, July 21). *Zimbabwe introducing a mass facial recognition project with Chinese AI company CloudWalk.* Quartz. Retrieved October 17, 2022, from https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

45 Capital Markets in Africa. (2019, January 10). *China's Digital Silk Road Is Looking More Like an Iron Curtain.* Retrieved October 17, 2022, from https://www.capitalmarketsinafrica.com/chinas-digital-silk-road-is-looking-more-like-an-iron-curtain/

46 Chiumbu, S. (2021 November). *Chinese Digital Infrastructure, Smart Cities and Surveillance in Zambia. Media Policy and Democracy Project.* Retrieved October 17, 2022, from https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/zambia_report.pdf

47 *Case Study: Smart Cities and Our Brave New World.* (2017, August 30). Privacy International. Retrieved October 17, 2022, from https://www.privacyinternational.org/case-studies/800/case-study-smart-cities-and-our-brave-new-world

48 *ZM: Surveillance camera projects deployed to watch on people.* (2020, October 26). Retrieved October 17, 2022, from http://ifg.cc/en/aktuelles/nachrichten/regionen/568-zm-sambia-zambia/58826-zm-surveillance-camera-projects-deployed-to-watch-on-people.html

49 Kobie, N. (2019, June 7). *The complicated truth about China's social credit system.* WIRED UK. Retrieved October 17, 2022, from https://www.wired.co.uk/article/china-social-credit-system-explained

8. Re-commendations

Most of the recommendations for scaling back the rollout of unrestricted state-sponsored surveillance highlight the need for legal and policy frameworks to increase transparency and build state accountability in the way it conducts its surveillance activities. The second focus for recommendations was on the role civil society can play in minimising the harms of surveillance activities. The third set of recommendations was directed towards global actors.

Legal and policy frameworks

Transparency around the use of surveillance technologies and their use is dependent on the access to information culture in a given country or jurisdiction. Zambia and Zimbabwe have in the past faced challenges in promoting information rights given the absence of transparency on government spending on national security, defence and security services. This lack of transparency extends to telecommunications service providers, including mobile network operators. Telecommunications service providers have to comply with government surveillance requests or requests for user information but they have never proactively published statistics on the number of requests they received from the government. Legal and policy frameworks are required to increase transparency and build state accountability.

Procurement transparency

There is need for more transparency in the procurement of technologies to carry out state-sponsored surveillance as well as technologies which have the potential to be repurposed for surveillance. There needs to be more transparency at procurement level both to understand data processing and the capabilities of technologies being used and to make it easier to understand the harm posed. It is also recommended that states be required to provide reasons for the adoption and rollout of surveillance technologies.

Oversight of existing surveillance infrastructure

Public consultations should be required before the acquisition of surveillance technologies and equipment. There is need to use a human rights framework in guiding policy on surveillance, such as the Necessary & Proportionate principles, to ensure surveillance is conducted only when necessary and proportionate. The introduction of oversight and accountability measures would limit the potential harms of surveillance technologies.

Awareness raising and advocacy

Digital surveillance is hard to prove in African states. CSOs have a role to play in bridging the digital divide and promoting cyber diplomacy to minimise the harms of digital surveillance. Relevant CSOs need to find ways to uncover acts of digital surveillance and raise awareness, advocate for policies on legal surveillance sanctioned by judicial and transparent safeguards.

Interventions by CSOs in response to the rollout of surveillance activities must focus on informing people about their rights and how those rights are affected by surveillance, and why it is important to hold the state and companies engaged in surveillance accountable for their actions. Training on digital safety and security to high-risk groups is important.

Regional and global regulation of trade in surveillance tools

Regional instruments are important, such as the African Union's Convention on Cyber Security and Data Protection and the role it plays in minimising surveillance activities. Zambia and Zimbabwe are encouraged to ratify the Malabo Convention in order to adopt better mechanisms of addressing cyber security and data protection.

Global bodies have an important role to play in holding African governments accountable and ensuring they confirm to global norms and standards as well as themselves regulating the development and trade of digital surveillance tools. The European Union in 2020 announced that it was working on plans to require manufacturers and suppliers who export surveillance and espionage technologies outside of the EU to obtain a licence to sell such technologies and to publish details about the licences they grant.

50 See the International Principles on the Application of Human Rights to Communications Surveillance (the *"Necessary and Proportionate Principles"* or *"13 Principles"*) that show how existing human rights law applies to modern digital surveillance. Retrieved October 17, 2022, from https://necessaryandproportionate.org/

51 Cerulus, L. (2020, October 17). *Europe to crack down on surveillance software exports.* POLITICO. Retrieved October 17, 2022, from https://www.politico.eu/article/europe-to-curtail-spyware-exports-to-authoritarian-countries/

9. Conclusion

The focus of this research paper is on the use of Chinese technology for surveillance purposes in Zambia and Zimbabwe, but it is important to highlight that these two countries have also sourced surveillance equipment from other parts of the world. In 2020, research by Citizen Lab found that at least 25 governments around the world, among these Zambia and Zimbabwe, were using Circles, an Israeli developed espionage technology for surveillance purposes.

While Zambia and Zimbabwe have had strong relations with China, which have manifested in the signing of trade agreements on technological development, it is the opacity of those deals that has been a cause for concern. Information on the extent and level of Chinese investment remains the preserve only of governments and their agencies. Lack of transparency, together with the culture of secrecy that characterises government business, especially on surveillance, is often justified on the basis of fortifying national security and there is no guiding legal framework in line with international normative frameworks or human rights laws.

Consequently, none of the extant laws and policies substantively addresses the risks to personal information in the digital age. This has left citizens susceptible to abuse of their rights, with no effective recourse. Zimbabwean law (the Interception of Communications Act), for example, does not place any obligation on the government to conduct surveillance transparently and ensure that citizens' data is collected, processed, and destroyed in line with international best practice. Nor does it provide for sufficient independent oversight on the security agencies that have broad powers to conduct surveillance.

There is no doubt that digital technologies have indeed brought national security risks, but that is no reason for governments to act outside human rights protocols. Lack of democratic conditionalities attached to trade deals China signs with African countries, Zambia and Zimbabwe included, exacerbates the situation, as the recipient countries do not feel compelled to account to anyone. What is required, is the political will and public service leadership that will not seek to insulate those that wield power from robust public scrutiny but pursue a just and an inclusive society where all citizens enjoy fundamental freedoms and entitlements due to them.

52 Marczak, B., Scottp-Railton, J., Rao P. S., Anstis, S., and Deibert R. (2021, June 29). *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles.* The Citizen Lab. Retrieved October 17, 2022, from https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

About the Authors

Lead Author

Christopher Musodza

is an ICT expert with more than 16 years of experience in digital security, internet governance and cyber policy work. Christopher holds degrees in computer science, Law and post grad qualifications in Cyber Law and Digital security. He has keen interests in cyber security research, training, and capacity support for human rights defenders. A co-founder of the Digital Society of Zimbabwe and The Ethical AI for Africa Project.

Co authors

Kuda Hove

is a researcher with a decade of experience in Information Technology law and policy work. His work is focused on reducing the potential harms that various digital technologies pose for the enjoyment of fundamental rights particularly the right to human dignity, the right to privacy, and the right to free expression. Kuda is a Master of Laws graduand in IT Law and has previously led Digital Rights work at the Media Institute of Southern Africa, Privacy International and Consumers International.

Otto Saki

is an LLD candidate at the University of the Western Cape researching on data protection, and privacy frameworks with a focus on Zimbabwe. He holds an LLBS, LLM in Human Rights Law and LLM in Information Communication Technology law, and currently works for a global philanthropy foundation as a program officer focusing on closing civic space (online and offline), and protection of human rights defenders. He writes in his personal capacity.