Chinese Digital Infrastructure, Smart Cities and Surveillance in Zambia

Sarah Chiumbu

November 2021

The Media Policy and Democracy Project
exploring how the media can work better for society

Chinese Digital Infrastructure, Smart Cities and Surveillance in Zambia

A report compiled by

Sarah Chiumbu

Prof. Sarah H. Chiumbu is an Associate Professor in the School of Communication at the University of Johannesburg. She holds a PhD and MA in media studies from the University of Oslo, Norway. Her research interests include media, democracy and citizenship, digital and alternative media, policy studies and social movements.

This report was commissioned by the Media Policy and Democracy Project (MPDP) supported by a grant from Luminate. The MPDP is a joint project of the University of Johannesburg's Department of Communication and Media and the University of South Africa's Department of Communication Science.

November 2021

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

Table of Contents

List of Acronyms

ANR	National Intelligence Agency
AU	African Union
APNAC	African Parliamentarians Network Against Corruption
AI	Artificial Intelligence
BRI	Belt and Road Initiative
CCTV	Closed-Circuit Television
CETC	China Electronics Technology Group Co
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
CSIS	Centre for Strategic and International Studies
CSO	Civil Society Organisation
FOCAC	Forum on China-Africa Cooperation
FDI	Foreign Direct Investment
ICTs	Information and Communication Technologies
IMF	International Monetary Fund
IOT	Internet of Things
NDC	National Data Centre
ITU	International Telecommunication Union
MMD	Movement for Multi-party Democracy
RCS	Remote Control System
RTSA	Road Transport and Safety Agency
SJCCS	Special Joint Cybercrime Crack Squad
UNIP	United National Independence Party
UPND	United Party for National Development
ZCCM	Zambia Consolidated Copper Mines Company
ZICTA	Zambia Information and Communications Technology Authority

Executive summary

- Zambia has embarked on Smart City projects. The government has established a three-phase project towards reaching the smart city status: establishment of national data and cloud; creation of advanced digital communication infrastructure, and putting in place Cloud platforms and Smart grid systems.
- The Smart City initiative is funded by China and implemented by Huawei and ZTE under the China Zambia Security Cooperation.
- Part of the Smart City projects is the Safe City initiative. Safe Cities incorporate various technologies and Internet of Things (IoT) devices to improve policing and security efforts. In December 2019, the government approved a proposal by Huawei Technologies to turn Lusaka into a Smart City by mounting 24-hour Close Circuit TV (CCTV) cameras in strategic places and along main roads in Lusaka, including public markets and bus stops.
- Digital rights organisations such as CIPESA and Paradigm Initiative have accused Chinese technology companies of using the Smart city project to sell surveillance technologies to African governments and help to undermine human rights in these countries.
- The government has updated ICT laws by promulgating the Cybersecurity and Cybercrimes Act and Data Protection Act to provide cybersecurity, protect against cybercrime and ensure data protection and privacy. The adoption of these laws shows the commitment of the Zambian government to manage and regulate the digital space, but the laws bestow broad discretionary powers on certain officers, and they have the potential to infringe on certain constitutionally guaranteed rights and freedoms.
- The flaws in the cyber security and data protection laws as well as existing repressive laws that impinge on the freedom of expression and past instances of spying actions, cyber-space monitoring, and interception of communications by the government create a conducive environment for state digital surveillance.
- The Smart City initiative exists without a legal architecture that fences off human rights against encroaching surveillance practices. Smart Cities are surveilled cities as they heavily rely on collecting enormous amounts of citizens' data. Digital rights organisations have raised concern that the CCTV cameras were installed in the absence of guidelines regarding acceptable standards for installing surveillance camera systems in public spaces that balance privacy rights and public safety and security imperatives. Although the Cabinet approved in 2019 the introduction of a bill in Parliament to control the use of CCTV in private and public premises, this bill has stalled and not been gazetted.
- While the broad justification for installing surveillance tools has been to fight crime, civil society organisations fear that the surveillance cameras, which rely on facial recognition technology, will be used instead to track and target government critics.
- Like many countries in Africa, Zambia mainly uses Chinese surveillance technology made possible by the ease of access, cost, and increased foreign direct investment (FDI) from the Belt and Road Initiative (BRI). There are fears that the entanglement of the Chinese state and its vast array of technology companies in Zambia is promoting the emergence of a surveillance culture.
- The new President Hakainde Hichelema, elected in August 2021, has vowed to change the political culture of Zambia. It is hoped that the new regime creates a conducive environment for digital rights.

Summary of recommendations

- Freedom of expression CSOs and digital rights activists should study and understand the emerging surveillance architecture built by the government in Zambia. They should monitor Chinese infrastructure investment in the country and determine areas where freedom of expression and digital rights are infringed.
- Create public awareness on the Smart City in terms of its objectives and mandate.
- The media should scrutinise the Smart City initiative and Chinese technology infrastructure and report their human rights implications.
- The government should ratify the African Union Convention on Cyber Security and Personal Data Protection.
- The government should amend some of the provisions of the Cyber Security and Cyber Crimes Act to align with Zambia's human rights obligations, both domestically and globally.
- The Zambia Information and Communications Technology Authority (ZICTA) should establish guidelines regarding acceptable standards for installing surveillance camera systems in public spaces. The guidelines should follow best practices in balancing privacy rights and public safety and security imperatives.
- The government should draft a National Data and Cloud Policy to ensure the implementation of effective cybersecurity privacy and data and cloud infrastructure protection measures.
- Funders should capacitate freedom of expression CSOs and digital rights activists on cyberlaw issues, IoT, AI, and surveillance to effectively lobby on encroaching surveillance practices.

Introduction

The use of surveillance technologies in Africa is spreading. There are concerns that these surveillance tools are being used without adequate checks and balances.[1] Freedom of expression activists and digital rights organisations have raised the alarm that the dissemination of these technologies is reinforcing and driving repression and human rights abuses. Citizen Lab, an interdisciplinary research unit at the University of Toronto, Canada, found that seven African countries – Botswana, Equatorial Guinea, Kenya, Morocco, Nigeria, Zambia, and Zimbabwe – are using spyware technologies.[2] The report identifies Circles as the surveillance firm that sells its products to nation-states. The Circles technology is being used in those countries to snoop on the personal communications of opposition politicians, rights activists, and journalists. Circles is a sister company of the NSO Group, an Israeli company accused of licensing its invasive iPhone and Android spyware called Pegasus to several authoritarian governments.[3] While growing accessibility of surveillance products in Africa is made possible by private cyber-security firms from several countries, most notably the USA and Israel, China seems to dominate the provision of digital surveillance supported by soft loans. The China Export-Import Bank has been able to offer large loans, as part of deals with African governments, with the condition that these loans will be used to deploy technologies using a Chinese company.[4] China's large digital footprint on the continent is a result of the Belt and Road Initiative (BRI). As of 2020, 42 African states were members of the BRI. As part of the "Digital Silk Road" (DRS), an appendage to BRI focusing on internet connectivity, artificial intelligence, the digital economy, telecommunications, smart cities, and cloud computing, major Chinese firms, such as Huawei, ZTE, Hikvision and others are building surveillance networks and supplying advanced social media monitoring capabilities worldwide.

This report focuses on Zambia's Smart City project and its potential for enabling the government to deploy invasive, broad, and targeted surveillance. Smart Cities use a variety of Internet-connected (IoT) technologies and databases to improve the efficiency and efficacy of city services.[5] The International Telecommunication Union defines a smart city as "an innovative city that uses ICTs [information and communication technologies] and other means to improve quality of life, the efficiency of urban operation and services and competitiveness while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects." (Recommendation ITU-T Y.4900).[6] Globally, many countries are adopting smart city strategies to manage urban challenges through technologically driven solutions.

Notwithstanding their benefits for urban connectivity, there is a dark side to smart city

[1] Bulelani Jili (2019). Chinese Surveillance Tools in Africa. Research Brief. *China, Law and Development*. No. 8/2019.

[2] Citizen Lab (2020). *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*. Retrieved at: https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

[3] Suraya Dadoo (2020). Opinion: Israel helping African governments to place us all under surveillance. *TimesLive*, 18 December 2020. Retrieved at: https://www.timeslive.co.za/ideas/2020-12-18-opinion-israel-helping-african-governments-to-place-us-all-under-surveillance/

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

[5] Market. Research.Com. The Convergence of 5G, Artificial Intelligence, Data Analytics, and Internet of Things. Retrieved at: https://blog.marketresearch.com/the-convergence-of-5g-artificial-intelligence-data-analytics-and-internet-of-things

[6] ITU-T, Smart Sustainable Cities at a Glance. Retrieved at: https://www.itu.int/en/ITU-T/ssc/Pages/info-ssc.aspx#:~:text=%E2%80%8B%E2%80%9CA%20smart%20sustainable%20city,generations%20with%20respect%20to%20economic%2C

projects, and the risks seem to outweigh the benefits. Because smart city initiatives are deploying surveillance technologies such as data mining, facial recognition, and other forms of artificial intelligence, they are increasingly becoming a euphemism for surveillance. In a increasing number of countries, there are growing concerns about how technologies associated with smart cities are infringing on free speech, privacy, and data protection.

Zambia, like many African countries, adopted the Smart City agenda in 2015. Part of this agenda involved the creation of Smart Cities, which incorporates the Safe City project. The Smart City initiative is funded by China and implemented by Huawei and ZTE under the China Zambia Security Cooperation.[7] Safe City initiatives are Huawei's flagship public safety solution and on a series of Internet of Things (IoT) devices intended to improve policing efforts. Although the Smart City project is dressed in a language of urban sustainability and effective policing, there are emerging debates over these projects' national security ramifications.

Freedom of expression NGOs on the continent have accused Huawei of using the Smart City project to sell surveillance technologies to African governments and help to undermine human rights in these countries. For instance, Juliet Nanfuka of the digital rights advocacy organisation, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), has also raised the concern about these Safe City projects and their implications in African countries wherein most cases lack regulatory safeguards and privacy legislation.[8] Dorothy Mukasa, CEO of Unwanted Witness, a Ugandan digital rights advocacy organisation, believes that Huawei's Safe City initiative threatens human rights in Uganda, including the right to peaceful assembly and association.[9]

[7] Brenda Zulu (2020). Surveillance camera projects deployed to watch on people. *The Mastonline*. Retrieved at: https://www.themastonline.com/2020/10/18/surveillance-camera-projects-deployed-to-watch-on-people/

[8] Samuel Woodhamd (2020). Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused. *QuartzAfrica*. Retrieved at: https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/

[9] Ibid.

Scope and aims of the study

This study examines digital surveillance by the government of Zambia through the Smart Zambia initiative funded by Huawei Technologies and ZTE. It looks at the current and future digital surveillance capabilities of the Zambian government. The research further explores the actors and interests behind China's involvement in Zambia's digital surveillance architecture.

Methodology

The research was conducted through a literature review on China's telecommunication infrastructure development in Africa and Zambia, digital surveillance, and smart city initiatives in Africa, Zambia and beyond. It also included reviewing other secondary sources such as academic publications, industry reports, government documents and media reports, and a limited number of interviews.

Limitations

Difficulty in accessing respondents for interviews constrained the research. Several attempts were made to contact Smart Zambia agents, the Department of Home Affairs and opposition party members who were against the Smart City initiative in Zambia. Efforts to get comments from freedom of expression and digital rights organisations also proved to be difficult. Only three people were interviewed from digital rights organisations – Bloggers from Zambia, Paradigm Initiative and the Internet Society Zambia Chapter. It should be noted that in the absence of an Access to Information law, getting information from public figures is difficult. The three respondents interviewed also attested to this. They mentioned that government officials in Zambia are generally reluctant to speak due to the State Security Act.

Zambia: Political and socio-economic context

Zambia became independent in 1964 with Kenneth Kaunda as the county's first postcolonial President. The country adopted a one-party state in 1972, with the United National Independence Party (UNIP) as the only legal party. Until 1964, Zambia had been part of the Central African Federation comprising Southern Rhodesia (present-day Zimbabwe), Northern Rhodesia (present-day Zambia) and Nyasaland (present-day Malawi). Even though the federation was abolished in 1963, the Zambian economy was intertwined with that of the hegemonic partner of the federation, Southern Rhodesia, which became Zambia's largest trading partner.[10] The imposition of sanctions on Rhodesia in 1965 affected Zambia's economic growth to some extent. This forced the country to invest in large capital projects and mining. With its genesis in 1920, copper mining was nationalised in 1973 and remained in government hands for over 24 years.[11] At that time, a worldwide recession caused the copper price to collapse. The output from the mines fell, and capital for investment in equipment and exploration dried up.[12]

As in most sub-Saharan African countries, Zambia returned to multi-party democracy in the early 1990s. In 1991, the country held its first multi-

[10] A. King (2001). *Identity and Decolonisation:the policy of partnership in Southern Rhodesia* 1945–62. PhD Dissertation. St Anthony's College, Oxford University.

[11] J.Sikamo, A. Mwanza, C. Mweemba (2016). Copper mining in Zambia – History and future. *Journal of the Southern African Institute of Mining and Metallurgy*. 491–496.

[12] R. De Stagé, A. Holloway, D. Mullins, L. Nchabaleng, and P. Ward (eds) (2002). *Learning about livelihoods. Insights from southern Africa*. Oxfam, 330–333.

party elections in 23 years. Frederick Chiluba's Movement for Multi-party Democracy (MMD) defeated Kaunda's UNIP. In the same year, the new government embarked on the World Bank and International Monetary Fund (IMF) economic structural adjustment programme, which led to the restructuring of the economy, abandonment of subsidies, and privatisation.[13] The country sold both its loss and profit-making parastatals. For example, the government privatised the state-owned Zambia Consolidated Copper Mines Company (ZCCM). Despite these measures, Zambia had negative economic growth between 1991 and 1995. Copper production declined sharply. In 2020, Anglo America withdrew from its copper interests in Zambia, which caused a severe blow to the mining sector. Persistent drought in the 1990s affected agriculture, and the Zambian kwacha depreciated.[14] The social consequences of structural adjustment, coupled with bad governance, have been enormous and continue to affect Zambia today. Poverty, livelihood vulnerability and HIV/AIDS have dogged the country over the years. Zambia remains one of the least developed countries in Africa, with 64% of the population living on less than $1.90 a day and a life expectancy of 60.[15]

The MMD ruled Zambia from 1991 to 2011, when political power was transferred to the Patriotic Front (PF) under its leader Michael Sata, who defeated the incumbent President, Rupiah Banda, of the MMD. Sata ruled Zambia for only three years, and he died in October 2014. This necessitated a presidential by-election in January 2015 to elect a president to serve the remainder of the term of the late President Michael Sata. Edgar Lungu of the PF party won the election by a low margin.[16] The scheduled election was held in August 2016. President Edgar Lungu was re-elected to a full five-year term when he scored above the 50%+1 mark of the vote, defeating opposition leader Hakainde Hichilema of the United Party for National Development (UPND).[17] In the latest national elections held in August 2021, Hakainde Hichilema of the United Party for National Development won the elections with 59.4% of the vote against Edgar Lungu.

Under Lungu's presidency, Zambia's economic fortunes did not improve. The economy weakened due to a combination of corruption, poor governance and external shocks. Drought also contributed to an energy crisis that saw power cuts lasting 20 hours a day.[18] These factors, among others, halved Zambia's annual growth rate from nearly 4% in 2016 to just 2% in 2019, while external debt and inflation have surged.[19] The new President has vowed to revive the economy and show "zero tolerance" for corruption.[20]

[13] E. Matambo (2017). *The role of identity and interest in the evolution and sustenance of Sino-Zambian relations: a constructivist perspective*. PhD dissertation, University of Kwa-Zulu Natal.

[14] BTI (2020). Zambia Country Report 2020. Retrieved at: https://www.bti-project.org/en/reports/country-report-ZMB-2020.html

[15] Ibid.

[16] Ibid.

[17] BBC News (2021). *Zambia's President Edgar Lungu declared election winner*. Retrieved at: https://www.bbc.com/news/world-africa-37086365

[18] http://www.times.co.zm/?p=107106

[19] https://www.imf.org/en/Countries/ZMB

[20] Zambia's new leader vows 'zero tolerance' on corruption. *AfricaNews*. Retrieved at: https://www.africanews.com/2021/09/10/zambia-s-new-leader-vows-zero-tolerance-on-corruption//

Human rights and freedom of expression context

Although smart cities promise safer streets, cleaner air, more efficient transportation, and improved communication, on the surface, their dependence on technology can deepen mass surveillance and erode personal privacy. When smart cities are built into countries with poor human rights infrastructure, they can threaten democracy. Even though Zambia turned to multi-partyism in 1991 and has established democratic principles over the years, the legacy of an authoritarian political culture and ingrained pattern of neo-patrimonial governance under the former one-party system has influenced human rights environment in the country. Zambia's human rights record has been poor over the years. Significant human rights violations have included arbitrary detentions by police, arbitrary interference with privacy, restrictions on freedom of expression and media freedom, censorship, including the arbitrary application of criminal libel laws against critics of the government, and unjustified arrests or prosecutions of journalists and interference with the right of assembly.[21] The Zambian Constitution guarantees freedom of expression in Article 20, but application and enforcement are a challenge.[22] In addition, there are still some laws which reduce the freedom of expression guaranteed in the Constitution as outlined below.

Penal Code Act

The Act serves as the main legal framework used to prosecute online misdemeanours and cybercrimes, particularly those relating to defamation of the President, sedition and criminal libel. The Penal Code provides for criminal prosecution for defaming a person. Other laws in Zambia provide for civil defamation. Sections 53–54 criminalise and prohibit the importation, publishing, sale, distribution, or reproduction or possession of any prohibited publication or extract and allows for prosecution of persons engaged in such activities. Sections 57, 60 and 61 prohibit seditious practices made through publications and utterances. Section 67 criminalises "the publication of false news with intent to cause fear and alarm to the public". Section 69 criminalises defamation of the President with "intent to bring the President into hatred, ridicule or contempt, by publishing any defamatory or insulting matter, whether by writing, print, word of mouth or in any other manner".[23]

State Security Act 1969

The Act makes "provision relating to State security; to deal with espionage, sabotage and other activities prejudicial to the interests of the State; and to provide for purposes incidental to or connected therewith". The Act allows for members of the public to be charged with sedition for publishing information that could endanger the state in times of war. The law also prohibits the possession or distribution of classified information. The grounds for classification are vague. The Act was used to arrest an employee of the Ministry of Finance in 2020 for disclosing what was essentially public information. The charge, brought under Section 4, Chapter 111 of the State Security Act, was subsequently ruled unconstitutional and is thus no longer part of Zambian law. However, the sections on sedition restrict freedom of expression.[24]

[21] US Department of State (2019). Country Reports on Human Rights Practices: Zambia 2019. Retrieved at: https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/zambia/

[22] African Media Barometer reports of 2013, 2018, 2021.

[23] Anneke Meerkotter (2019). Zambia: challenging the enforcement of the offence of defamation of the President. *Southern African Litigation Centre*. Retrieved at: https://www.southernafricalitigationcentre.org/2019/05/25/zambia-challenging-the-enforcement-of-the-offence-of-defamation-of-the-president/

[24] Fesmedia (2018). *Africa Media Barometer*, 2018, 2021.

Security Intelligence Service Act 1973

Section 11(1) prohibits any intelligence officer or employee of the Intelligence Service from disclosing any information obtained as a result of his office without the written consent of the President. The penalty for such publication is a fine, imprisonment or both. Section 11(3) of the Act makes it an offence to publish any information obtained in contravention of Section 11(1).

Public Order Act 1995

The Public Order Act maintains public order and the rule of law, but it has been used several times as a tool to undermine the human rights that are essential to a democracy. This Act negatively affects the rights to both freedom of expression and freedom of assembly.[25] Permission to hold a rally, peaceful march or public gathering can be denied pursuant to the Act. The government regularly invokes the law to restrict freedom of expression and ban peaceful demonstrations and meetings.

At the same time, the opposition often faces harassment and arrest on trumped-up charges and spend most of their time dealing with tedious legal processes that hinder their operations. Section 13 sets penalties for "making statements or doing acts intended to promote hostility between sections of the community".

Anti-Terrorism and Non-Proliferation Act 2018

The Anti-Terrorism Act of 2007 was repealed to enact the Anti-Terrorism and Non-Proliferation Act, 2018. The Act aims "to prevent and prohibit the carrying out of terrorism financing and proliferation activities; provide for measures for the detection and prevention of terrorism and proliferation activities".[26] Section 27, in particular, has been used to arrest journalists for online posts seen as having the potential to incite violence. The Section gives power to "convict and imprison for life a person who incites another person or organisation to commit an act of terrorism or proliferation".

[25] Fesmedia (2018). *Africa Media Barometer: Zambian Report*. Retrieved at: http://library.fes.de/pdf-files/bueros/africa-media/14071.pdf

[26] Anti-Terrorism and Non-Proliferation Act of 2018, Preamble.

Laws and legal instruments in the digital space

In line with developments in other African countries, the government of Zambia embarked on the formulation of a National ICT Policy. The process was completed in 2005, and the policy was launched in 2007. To implement the ICT policy, the government promulgated in 2009 the Information and Communication Technologies Act (ICT Act) and the Electronic Communications and Transactions Act 2009 (ECT Act). These two laws governed the Internet in Zambia for a long time.

Over the years, civil society actors and the technical community called for improved and updated legal and regulatory frameworks that considered the advanced nature of technology. To this end, the government repealed the Electronic Communications and Transaction Act to facilitate the introduction of three standalone Bills:

- The Electronic Commerce and Transactions Bill
- The Cybersecurity and Cybercrimes Bill of 2017, and
- The Data Protection Bill.

There was minimal consultation on the drafting of these bills. Zambian media, bloggers, journalists and civil society organisations launched the #OpenSpaceZM campaign, which sought to promote openness and participation of relevant stakeholders in the cyber law drafting process.[27] In June 2020, the government passed a resolution to approve the African Union Convention on Cybersecurity and Personal Data Protection to harmonise the new cyber laws and regional cooperation on cybersecurity, cybercrime, and data protection.[28] The three Bills have since been passed into law.

The Electronic Commerce and Transactions Act 2021

The ECT Act 2021 was passed in March 2021 and replaced a 2009 law which had afforded the government sweeping surveillance powers with little to no oversight. The Act regulates electronic communications and transactions.

The Cybersecurity and Cybercrimes Act 2021

On 23 March 2021, former President Edgar Lungu signed the Cyber Security and Cyber Crimes Bill into law. The law aims to provide for cyber security, to protect persons against cybercrime, promote child online protection, and facilitate identification, declaration and protection of critical information infrastructure, the collection and preservation of evidence of computer and network-related crime, admission in criminal matters of electronic evidence, and registration of cyber security service providers. When the law was introduced in 2018, several concerns were raised by civil society organisations who argued that while "the bill addressed legitimate cybercrimes issues and offered some protections to freedom of expression and the right to privacy, it had numerous shortfalls, such as a chilling effect on freedom of expression, promoting censorship by the state and self-censorship, as well as an unfettered intrusion on the right to privacy by the state through systematic monitoring, interception and surveillance".[29] While proposals were made to

[27] Digital Rights Africa (2019). *Violations Reloaded: Government Overreach Persists Despite Increased Civil Society Advocacy*. Paradigm Initiative Publication. Retrieved at: https://paradigmhq.org/download/dra19/

[28] The African Union Convention on Cyber Security and Personal Data Protection was established in 2014 to provide a framework for cybersecurity in Africa. As part of this, member states are asked to establish national cybersecurity policies as well as legal, regulatory, and institutional frameworks for cybersecurity governance.

[29] CIPESA (2021). Implications of Zambia's Act 2021 on Digital Rights Cybersecurity and Cybercrimes. Retrieved at: https://cipesa.org/?wpfb_dl=447

revise the bill to address these concerns, the law was passed without addressing the concerns. As a result, the law has negative ramifications for the enjoyment of digital rights in Zambia.

Civil society organisations are concerned that the Act has a chilling effect on freedom of expression, media freedom and Zambians' right to privacy. There are fears that the cyber law emulates China's approach to policing the internet. The legislation could be used to monitor and punish social media users and limit freedom of expression. Opposition lawmakers have expressed fear that the law might stifle internet usage, especially during elections.[30]

Areas of concern

CIPESA[31] outlines critical areas of concern in the Act as follows:

Limited Safeguards over Interception of Communications: Section 27 provides for the establishment of the Central Monitoring and Coordination Centre as an authorised centre for interception of communications. Under Section 28, the interception is conducted by a law enforcement officer if there are reasonable grounds to believe that an offence has been committed, is being committed or is likely to be committed. Before intercepting communications, a law enforcement officer applies to a judge for an interception of communications order after making a written application to the Attorney General for written consent, and such consent has been obtained. The interception order is valid for an initial period of three months, renewable by a judge for an unspecified period. The failure to limit the period of validity of an interception order could subject individuals, especially government critics and political opponents, to continued surveillance.

Section 27(3) provides for the management, control and operation of the Central Monitoring and Coordination Centre by the department responsible for Government communications in liaison with ZICTA. However, the department is not specified in the Act, and this silence provides a possible room for abuse of the processes associated with the handling of personal data and state surveillance. Under Section 29, similar to Section 30, an enforcement officer may intercept any communication and request a service provider orally. These sections and the one above provide limited safeguards over interception of communications, have the potential to violate privacy rights and are not aligned to established principles of limitations to privacy under international law.

Heavy demands on service providers: Section 38 requires electronic communication service providers to use hardware and software facilities to enable lawful interceptions. The penalty for non-compliance is a fine of 150 000 Kwacha (USD 6 643), imprisonment for up to five years, or both. This high penalty will compel service providers to render interception assistance even when they receive dubious oral orders.

Restrictions of anonymity: Section 39 of the Act requires electronic communication service providers to collect personal data from individuals, including names, residential addresses and identity numbers, before entering into a contract to provide any service. While the collection of such information is essential for tracking criminal elements, there is no guarantee of safety and protection of collected personal data despite the enactment of the Data Protection Act, 2021.

[30] Zambia passes sweeping cyber laws ahead of elections, *AFP*. Retrieved at: https://telecom.economictimes.indiatimes.com/news/zambia-passes-sweeping-cyber-laws-ahead-of-elections/81427180

[31] CIPESA (2021). Implications of Zambia's Act 2021 on Digital Rights Cybersecurity and Cybercrimes. Retrieved at: https://cipesa.org/?wpfb_dl=447

Limitation on freedom of expression: Section 59 criminalises any printed or visual object or "any other object tending to corrupt morals". The term "any other object" in the provision makes it ambiguous and so broad in scope that it has a chilling effect on freedom of expression and speech.

Broad definition of hate speech: Section 65 of the Act prohibits hate speech. The definition of hate speech is overly broad and vague and does not delineate legitimate expression, which would not amount to hate crime. Accordingly, this provision could be abused to persecute critics through arbitrary arrests and detention. It could thus have a chilling effect on freedom of expression and information, promote self-censorship, and limit the exercise of the profession of journalism.

The Data Protection Act 2021

The government passed the Data Protection Act, Number 3 of 2021, on 24 March 2021. The Act was created to govern the use of individuals' personal information. In addition, it seeks to prevent unlawful use, collection, processing, transmission and storage of personal information, thus protecting the right to privacy. The Act also establishes the Data Protection Commissioner and spells out its functions, provides for the regulation of data collectors, processors, and controllers and provides for the rights of data subjects. The positive aspect of the Act is that it is a sign of commitment by the government to implement Article 17 of the Constitution, which provides for the right to privacy. The principles and rules related to processing personal data laid down in Section 12 reflect the internationally acceptable data protection standards as encapsulated in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and Europe's General Data Protection Regulation (GDPR). If rightly employed, these principles will enhance individuals' data protection and promote the right to privacy.[32]

Again, CSOs have warned that the Act has several provisions that are likely to be abused. For instance, Section 3(1) potentially raises privacy issues. Subsection 3(2) provides that, "This Act does not apply to the processing of personal data by an individual for personal use." However, it does not define what individual or personal use is. Hence, the provision ignores the possibility that individuals could process personal data in the guise of "personal use" yet put it to other uses that undermine other individuals' privacy. Section 4 establishes the Office of the Data Protection Commissioner, whose functions include, among other things, registration of data controllers and processors, licensing data auditors, providing information to stakeholders, giving advice, and representing the government on data protection. The problem is that this Office is placed under the ministry responsible for communications. Since personal data issues are very sensitive, common practices in data protection regimes require the establishment of independent data protection commissions.[33] There is a strong possibility of political influence based on the history of government information and communication departments.

The adoption of both the Cybersecurity and Cybercrimes Act and Data Protection Act shows the commitment of the Zambian government to manage and regulate the digital space, but due to their vague provisions and broad discretionary powers bestowed on certain officers, the Acts instead have the potential to infringe on certain constitutionally guaranteed rights and freedoms.

[32] CIPESA (2021). Zambia: The Insights into the Data Protection Act 2021. Retrieved at: https://cipesa.org/?wpfb_dl=449

[33] Ibid.

China's Smart City initiatives in context

The Chinese government is a champion of Smart City initiatives. It identified Smart City development as a national priority in 2012 and viewed it as a cornerstone of its future economic and urban development strategies.[34] The BRI, China's signature foreign policy, highlights smart cities as a "strategic opportunity" for Chinese firms to expand abroad. Several China-based hi-tech giants, including Huawei, Baidu, Alibaba, and Tencent, have been behind the country's smart city movement based on their experience with AI, big data, and cloud computing technologies.[35] China has the highest number of smart city initiatives in the world. Although the Chinese smart city initiative fits into policy discourse marked by urbanisation, innovation, sustainability and the knowledge economy, it emphasises safety and security.[36] This approach fits in with the "Safe City" idea, a component of the Smart City which highlights surveillance. China now has the most extensive surveillance system in the world. The country is home to 18 of the top 20 most surveilled cities in the world.[37]

Over the years, the country has invested heavily in a comprehensive surveillance system that includes facial recognition cameras, closed-circuit television (CCTVs) and sensors. Smart City initiatives follow a top-down approach controlled by the central government.[38] China's defence and security entities are deeply involved in Smart City initiatives. For instance, the state-owned defence electronics conglomerate China Electronics Technology Group Co., Ltd. (CETC) established its own Smart City Research Institute in April 2016 and partnered with several city governments to develop smart city initiatives.[39]

The Chinese government uses smart city technologies to expand its mass surveillance capabilities. Thanks to advanced AI, China uses its smart and safe cities projects to build a surveillance architecture. An example is the social credit system, a surveillance system that leverages big data to monitor and assess the trustworthiness of individuals, companies and government entities. A good rating offers social and economic benefits, such as health care, deposit-free renting of public housing. In contrast, a negative rating could see individuals banned from flights, trains or hotels.[40] There is a social credit system for businesses, individuals, government officials, and numerous regional variations in interpretation and application. The system draws on vast amounts of data about every individual, gathered from several digital platforms and through video surveillance systems with help from facial recognition technologies. A social credit system is an integrated tool for datafication, dataveillance and data-driven authoritarianism.[41]

[34] Alice Ekman (2019). *China's Smart City: The New Geopolitical Battleground*. French Institute for International Relations, December 2019. Retrieved at: https://www.ifri.org/en/publications/etudes-de-lifri/chinas-smart-cities-new-geopolitical-battleground

[35] Richard Hu (2019). The state of Smart Cities in China: The case of Shenzhen. *Energies* 2019, 12, 4375. Retrieved at: https://www.mdpi.com/1996-1073/12/22/4375/htm

[36] Ibid.

[37] Paul Bischoff (2021). Surveillance camera statistics: Which cities have the most CCTV cameras? *Comparitech*. Retrieved at: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

[38] Wenxuan Yu and Chengwei Xu (2018). Developing Smart Cities in China: An Empirical Analysis. *International Journal of Public Administration in the Digital Age*, 5(3), July–September 2018.

[39] US-China Economic and Security Review Commission (2020). *China's Smart Cities Development*. Retrieved at: https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf

[40] Amanda Lee (2020). What is China's social credit system and why is it controversial? Retrieved at: https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial

[41] Claire Seungeun Lee (2019). Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review*, 43(6), pp. 952–970

Smart Cities in the context of China-Africa relations

China has become a provider of smart city solutions to different global regions.[42] Sub-Saharan Africa has become the main focus. In 2018, Chinese ICT company Huawei Technologies announced a $1.5 billion fund to support Africa's smart cities. As of 2020, there were 12 "Safe City" programmes in sub-Saharan Africa, including in Uganda, Kenya, South Africa and Zambia, according to the Center for Strategic and International Studies (CSIS).[43]

China's foray into smart city developments in Africa needs to be understood in the context of China-Africa relations. China-Africa relations had existed since ancient times, but were first formalised in 1956 when Egypt and China struck diplomatic ties. This move paved the way for China to engage with the rest of Africa.[44] China-Africa cooperation was cemented over the following decades by a shared socialist ideology. During the Cold War, China used foreign aid as a political tool to gain Africa's diplomatic recognition and to compete with the West for Africa's support.[45] After the Cold War, the China-Africa relationship moved from being driven solely along ideological lines to a more institutionalised one based on a framework called the Forum on China-Africa Cooperation (FOCAC) established in 2000. This framework promotes diplomatic, trade, security and investment relations between China and African countries. All African countries except Eswatini are members. Since its formation, FOCAC is held every three years, alternately in China and Africa.[46]

Since China's formalised entry into Africa in the 1960s, it has emphasised infrastructure development, focusing on hydropower, dams, and transport (mainly railroads), ports, and to a smaller extent, water and sanitation.[47] A considerable percentage of the continent's infrastructure initiatives are driven by Chinese companies and/or backed by Chinese funding. In recent years, China's infrastructure development has moved to telecommunications and digital technologies, which have become vital for its strategic interests. In the digital realm, China is competing with the West to establish spheres of technological influence, and seeks to establish itself as a great power, both through soft power and economically.[48]

China's economic engagement in Africa follows an approach that uses state resources to underpin state-controlled business entities.[49] Therefore Chinese companies, backed by senior political leaders, government financing and foreign aid instruments, are willing to invest in countries with high political risk for reasons that promote China's strategic and business interests. The state-backed China Export-Import Bank (China Exim Bank) provides massive loans to Chinese companies to invest in these high-risk countries.[50]

From 2013 to the present, China has been reforming its economic strategy. With more resources at its disposal and more opportunities for economic growth, China "has renewed the geographic layout and emphasised 'opening to

[42] Alice Ekman (2019). China's Smart City: The New Geopolitical Battleground. *French Institute for International Relations*, December 2019. Retrieved at: https://www.ifri.org/en/publications/etudes-de-lifri/chinas-smart-cities-new-geopolitical-battleground

[43] Samuel Woodhams (2020). Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused. *Quartz Africa*. Retrieved at: https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/

[44] A. Kinyondo (2019). Is China Recolonizing Africa? Some Views from Tanzania. *World Affairs*, 182(2), pp. 128–164, p. 130.

[45] Sun (2014). Cited in Kinyondo (2019). p. 138.

[46] B. Osei-Hwedie (2012). The dynamics of China-Africa cooperation. *Afro Asian Journal of Social Sciences*, 3(3), pp. 1–25.

[47] Executive Associates (2009). *China in Africa: A strategic overview*. Retrieved at: https://www.ide.go.jp/library/English/Data/Africa_file/Manualreport/pdf/china_all.pdf

[48] China's ICT engagement in Africa: A comparative analysis. *The Yale Review of International Studies*. Retrieved at: http://yris.yira.org/essays/4702

[49] D. Cissé (2012). Chinese telecom companies foray into Africa. *African East Asian Affairs: The Chinese Monitor*, p, 69, Retrieved at: https://aeaa.journals.ac.za/pub/article/view/9

[50] Ibid.

the West"'.[51] This move evolved from a series of government pronouncements and policy documents. Most influential among them is the BRI, which Chinese president Xi Jinping initially proposed in 2013.[52] The core pillars of the Initiative are "promotion of policy coordination, facilitating connectivity, unimpeded trade, financial integration, and people-to-people bonds".[53] The Initiative cuts across the three continents of Asia, Europe and Africa and targets 4.4 billion people in 67 countries, directly representing 63% of the total global population.[54]

At the Seventh Ministerial Conference of the FOCAC in 2018, an action plan on China-Africa Cooperation for 2019–2021 was adopted. The action plan focuses on smart cities as an area of future cooperation.[55] Although support by China for smart cities on the continent started some years ago, they entered a more concrete phase in 2019. Huawei has developed a special financing solution for smart city development in Africa. The fund supports African smart cities in security and the internet of things (IOT), focusing on communication and intelligent video surveillance.[56] Other IoT services such as water meters, electricity meters, waste bins, traffic lights and street lights are being rolled out in cities such as Cape Town, South Africa, and Nairobi, Kenya.

There are concerns that China's smart city initiatives, including facial recognition cameras and social media monitoring tools, will be used by authoritarian governments to undermine human rights.[57] For instance, Freedom House has stated that most of the smart city initiatives in Africa are in countries deemed "partly free" and "not free" in its 2009–2018 reports.[58] In August 2019, the Ugandan police force announced it had purchased facial recognition cameras from the Huawei company at a $126 million cost as part of a "Safe City" agreement. In Ethiopia, where internet shutdowns are common, the government has also signed a smart city initiative with Huawei.[59] A Wall Street investigation alleged that technicians from the Chinese powerhouse had helped the Ugandan and Zambian governments spy on their political opponents, including intercepting their encrypted communications and social media.[60]

[51] Y. Li (2018). China's Go Policy: A review on china's promotion policy for outward foreign direct investment from a historical perspective. Centre for Economic and Regional Studies HAS *Institute of World Economics Working Paper* 244, September 2018, p. 17. Retrieved at: https://ideas.repec.org/cgi-bin/refs.cgi

[52] Ibid. p. 17

[53] Varlare and Putten (2015), cited in Z. Raphael and Z.C. Mwatela (2016). Africa in China's'One Belt, One Road' Initiative: A critical analysis. *IOSR Journal of Humanities and Social Science* (IOSR-JHSS), 21(12), pp. 10–21.

[54] Ibid. p. 11.

[55] Alice Ekman (2019). China's Smart City: The new geopolitical battleground. *French Institute for International Relations*, December 2019. Retrieved at: https://www.ifri.org/en/publications/etudes-de-lifri/chinas-smart-cities-new-geopolitical-battleground

[56] Jean Marie Takouleu (2019). Africa: Huawei sets up a $1.5 billion fund to boost African smart cities. Retrieved at: https://www.afrik21.africa/en/africa-huawei-sets-up-a-1-5-billion-fund-to-boost-african-smart-cities/

[57] Samuel Woodhams (2020). Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused. *Quartz Africa*. Retrieved at: https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/

[58] Jonathan E. Hillman and Maesea McCalpin (2019). Watching Huawei's "Safe Cities". *CSIS Briefs*, November 4, 2019. Retrieved at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf

[59] Samuel Woodhams (2020). Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused. *Quartz Africa*. Retrieved at: https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/

[60] Joe Parkinson, Nicholas Bariyo and Josh Chin (2019). *Huawei Technicians Helped African Governments Spy on Political Opponents*. Retrieved at: https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

The Smart City agenda in Zambia

One of the countries in Africa with the most enduring relations with China is Zambia. Its ties with China are among the longest of all African countries.[61] Zambia was one of the first Southern African countries to gain independence and hence had to provide support to surrounding states still under the yoke of colonialism. Zambia formed a part of what was then called the Frontline States,[62] established in 1970 to coordinate their responses to apartheid and formulate a uniform policy towards the apartheid government and the liberation movement.[63] The Frontline States received a lot of Soviet aid and hence were more inclined towards the Communist camp in the Cold War. Therefore, China proved a critical player in this regard, as it also supported specific liberation movements.[64] China-Zambia relations were established in this context. Emmanuel Matambo states that relations between Zambia and China have undergone three phases – the first phase was characterised by solidarity, the second by geopolitics and the third by geoeconomics. The last two phases influence China-Zambia relations today, especially in trade and infrastructure development.[65] Zambia and China relations have been boosted by a high level of bilateral trade, which stood at USD100 million to about USD3.5 billion in 2019.

A combination of loans, grants and aid has seen a rise in Chinese projects in Zambia, especially for the country's infrastructure projects.[66] These projects have included roads, bridges, airports, hospitals, stadiums, hydropower, migration from analogue to digital terrestrial television and telecommunication towers. Zambia is spending $1 billion on Chinese-made telecommunications, broadcasting, and surveillance technology. It's all part of China's "Digital Silk Road," a subset of its "Belt and Road" initiative that contributes an estimated $79 billion in projects around the world.[67]

In this context, in March 2015, former President Edward Lungu signed a joint framework and financing agreement for the Smart Zambia project, with Huawei as the primary project supplier. The government launched the SMART Zambia agenda in September 2015. Riding on the back of Zambia's vision 2030 agenda of transforming the nation into a middle-income country, the SMART Zambia Agenda's goal is to achieve social and economic transformation by adopting a paradigm shift from traditional paper and file format approaches to that of electronic service delivery[68] such as electronic billing and revenue collection, electronic health monitoring systems and Intelligent Mobility Systems in the form of cameras to address Road safety challenges.[69] The Smart Zambia initiative has also introduced an e-Cabinet where cabinet materials are now electronically generated. Huawei has acted as a lead planner to help the government implement the Smart Zambia ICT Master Development Plan over the next 50 years.[70]

[61] E. Matambo (2017). *The role of identity and interest in the evolution and sustenance of Sino-Zambian relations: a constructivist perspective*. PhD dissertation, University of KwaZulu-Natal.

[62] The Frontline states were made up of Angola, Botswana, Lesotho, Mozambique, Swaziland, Tanzania, Zambia and, from 1980, Zimbabwe.

[63] South African History Online,

[64] E. Matambo (2017). *The role of identity and interest in the evolution and sustenance of Sino-Zambian relations: a constructivist perspective*. PhD dissertation, University of KwaZulu-Natal, p. 46

[65] Ibid. p. 47.

[66] C. Chileshe (2010). Chinese Debt, Aid and Trade: Opportunity or Threat for Zambia? Occassional Paper No 72: China and Africa Project, South African Institute of International Affairs. *African perspectives. Global insights*. Retrieved at: https://media.africaportal.org/documents/SAIIA_Occasional_Paper_no_72.pdf

[67] Sheridan Prasso (2019). *China's Digital Silk Road Is Looking More Like an Iron Curtain*. Retrieved at: https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain

[68] Shadrick Sikaonga and Simon Tembo (2020). E-Government Readiness in the Civil Service: A Case of Zambian Ministries. *International Journal of Information Science* 2020, 10(1): 15–28.

[69] Martine Ntonga (2019), Smart City Initiatives in Zambia. Paper presented at the African Smart Cities Summit. Retrieved at: https://www.africanconstructionexpo.com/wp-content/uploads/2019/07/Martine.pdf

[70] Huawei New ICT Helps Build Smart Zambia. Retrieved at: https://partners.wsj.com/huawei/news/huawei-new-ict-helps-build-smart-zambia/

This Development Plan includes the Smart Zambia e-Government Master Plan which was approved by the government in 2019.[71] The Master Plan intended having 180 government services online by 2021, but the target has already been surpassed, as 212 government services were online by the end of 2019.[72] Part of the SMART Zambia agenda is the Smart City Initiative, adopted in December 2015. The long-term objective of this initiative is to enhance the quality of services provided to citizens and ultimately improve their quality of life.[73] The initiative has been operationalised in three phases.

Phase I

Smart Zambia Initiative is predicated on cloud computing. Therefore, the first phase involves building a National Data Centre (NDC) whose goal is to build a national cloud data centre. This phase was funded to the tune of US$65.5 million, and the loan for the project was acquired from the Export-Import Bank of China.74 The NDC also includes an email system, ICT talent training, tele-presence, unified communication system and maintenance support for the national ICT backbone. With this phase, Huawei will literally control the entire Zambian surveillance network. The centre can store 3 pegabytes of data, equivalent to 3 million high-definition movies. The establishment of cloud data centres raises challenges in the face of privacy regulations and evolving cybersecurity threats. Bulanda Nkhowani, Programmes Officer for Paradigm Initiative, states that digital rights organisations are concerned about how the data collected and stored in the NDC is managed.[75]

Phase II

As part of China-Africa relations, China seeks to promote digital infrastructure connectivity on the continent, expanding Internet access in remote areas to connect the last mile of the information network. The second phase of the Smart City project in Zambia is part of China's digital innovation plans for Africa. Zambia and China signed an agreement worth 280 million US dollars for this phase. This phase involves building a national broadband network and eGovernment platform to benefit 17 cities across the country. The eGovernment platform will facilitate the electronic collection of revenue by the Government through mobile money transfers.

This phase also aims to construct communications towers across the country, involving the construction of 808 new communications towers, which will take the country to almost 100% voice coverage and 40% in data coverage. Airtel, MTN and state-owned Zamtel are expected to use the new base stations, along with a new company, Vodafone Zambia, which operates data services only.[76]

Phase III

The third phase focuses on Cloud platforms and Smart Grid. The Smart Grid puts information and communication technology into electricity generation, delivery, and consumption and is used by electric power utilities to track and control the power usage of consumers.

[71] Republic of Zambia, Office of the President (2018). *SMART Zambia Electronic Government Master Plan 2018–2030*. Lusaka, Electronic Government Division, Office of the President.

[72] The World Bank (2020). Accelerating Digital Transformation in Zambia. Retrieved at: penknowledge.worldbank.org/bitstream/handle/10986/33806/Accelerating%20Digital%20Transformation%20in%20Zambia.%20Chapter%205.pdf?sequence=10&isAllowed=y

[73] Ibid.

[74] China has also built National Data Centres with funding from the Export-Import Bank of China in Senegal, Cameroon and Kenya (https://www.voanews.com/a/economy-business_analysts-china-expanding-influence-africa-telecom-network-deals/6209516.html)

[75] Interview with Bulanda Nkhowani, Programme Officer at Paradigm Initiative, 13 October 2021.

[76] Phase II of Communication Towers on course. *Lusaka Times*, March, 8, 2018, https://www.lusakatimes.com/2018/03/08/phase-ii-communication-towers-co

Safe City project

A component of the Smart City initiative is the Safe City project spearheaded by the Ministry of Home Affairs. Under this project, the government is mounting 24-hour surveillance cameras in public places and on the main road networks. The capital city Lusaka became the first city to install closed-circuit television (CCTV) cameras under the smart city initiative. In late 2019, the City of Lusaka permitted Huawei to mount security cameras across Lusaka at the cost of US180 million.[77] Another CCTV camera project is managed by the Ministry of Transport and Communication Road Transport and Safety Agency (RTSA) under contract with Intelligent Mobility Solutions (IMS), a joint venture between Lamise Trading and Kapsch International of Austria. This project seeks to provide traffic management, smart urban mobility, traffic safety and security services.[78] The two CCTV projects are similar in conceptualisation and implementation.

In 2019 the Cabinet approved the introduction of a bill in Parliament to control the use of CCTV in private and public premises. The Chief Government spokesperson Dora Siliya said that the bill was introduced because the country had no legal framework to regulate the use of CCTV in private and public premises.[79] According to Bulanda Nkhowani, Programmes Officer for Paradigm Initiative, the bill has not been gazetted. Her organisation has made several follow-ups with the government, to no avail.[80]

There is a concern that the government has not consulted on its processes to develop the Smart City project. Bulanda Nkhowani also stated that there is very little information in the public domain on the nature of this project because of this secrecy.[81]

[77] Lusaka Times (2019). Huawei to plant 24-hour cameras across Lusaka. Retrieved at: https://www.lusakatimes.com/2019/12/07/huawei-to-plant-24-hour-cameras-across-lusaka/

[78] Ministerial statement on the road traffic and safety agency contract with Intelligent Mobility Solutions by the Minister of Transport and Communication. Retrieved at: https://www.parliament.gov.zm/sites/default/files/images/publication_docs/MINISTERIAL%20STATEMENT%20BY%20THE%20HON.%20MUSHIMBA.pdf

[79] Brenda Zulu (2020). Surveillance camera projects deployed to watch on people. *The Mastonline*. Retrieved at: https://www.themastonline.com/2020/10/18/surveillance-camera-projects-deployed-to-watch-on-people/

[80] Interview with Bulanda Nkhowani, 13 October 2021.

[81] Ibid.

The capabilities of the Zambian state in digital surveillance

In many African countries, including Zambia, safe cities are not yet employed as key instruments of control. Their repressive outcomes have not yet made a significant impact, but they provide governments with powerful capabilities.[82] Because Smart City initiatives depend on collecting vast amounts of data and rely on CCTV cameras equipped with facial recognition software, this should naturally raise concerns. Governments may exploit safe cities for repressive purposes. In Zambia, the existence of authoritarian colonial-era laws, plus recently adopted ICT laws that have shortfalls, creates a conducive environment for state digital surveillance.

Already the newly promulgated Cybersecurity and Cybercrimes Act is having an impact on freedom of expression. During the 2021 elections, on election day, August 12, Internet users in Zambia lost access to WhatsApp. They could not access other social media platforms such as Facebook, Instagram, Twitter, and Messenger. All these services remained unavailable without the use of a virtual private network. Chapter One Foundation made an urgent chamber application against Zambia Information, Communication Technology Authority's (ZICTA) closure of the above social media platforms. On 13 August, the High Court of Zambia ordered the President to restore internet services to the populace.[83] Access to all platforms was restored on August 14. The 2016 elections also witnessed several internet connectivity interruptions.[84] Mobile networks were throttled and suspended for about 72 hours in opposition party strongholds protesting and alleging electoral fraud by the Electoral Commission of Zambia.[85] In February 2020, the internet was inaccessible for two days in Southern Province, a stronghold of the then opposition party United Party for National Development (UPND), now the ruling party. Government authorities attributed the disruption to seasonal rains, but digital activists saw the shutdown as politically motivated.[86] The state partially owns the country's fibre backbone and controls connections to the international internet. This provides an opportunity for the government to restrict connectivity at will. Zambia's national fibre backbone is provided by three operators: the state-owned Zamtel, the state-owned ZESCO and the privately-owned Liquid Intelligent Technologies.[87]

The examples below indicate the current and future capabilities of the Zambian state to create a digital surveillance architecture:

- **Spying fears:** In a State of the Nation address in March 2020, former President Lungu stated the ZICTA and Zambian police could track down social media abusers. As stated in the Introduction, concerns about possible surveillance on citizens by the government were first widely raised by the 2018 report by Citizen Lab that identified Zambia as one of 45 countries worldwide using Pegasus, a targeted spyware software[88] developed by the Israeli technology firm NSO.[89] The Citizen Lab researchers said they had identified what

[82] Steven Feldstein (2020), *Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa*. May 8, 2020. Retrieved at: https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf

[83] Zambia: High Court Orders Restoration of Internet Services. Retrieved at: https://allafrica.com/stories/202108150063.html

[84] OONI (2016). 'Zambia: Internet Censorship During the 2016 General Elections?', Open Observatory of Network Interference, 11 October. Retrieved at: https://ooni.org/post/zambia-election-monitoring/#:~:text=Out%20of%20a%20total%20of,duration%20of%20the%20testing%20period

[85] Zambian government suspected of causing internet shutdown following outage in opposition strongholds. *Tech Zim*, 18 August 2016. Retrieved at: https://bit.ly/3aSZeic

[86] Interview with Bulanda Nkhowani, 13 October 2021.

[87] *Freedom on the Net: Zambia 2021*. Retrieved at: https://freedomhouse.org/country/zambia/freedom-net/2021

[88] This software enables the remote surveillance of smartphones.

[89] *Freedom on the Net: Zambia 2018*. Retrieved at: https://freedomhouse.org/country/zambia/freedom-net/2019

appears to be a single Circles system in Zambia, operated by an unknown agency. A Wall Street Journal 2019 article also reported that Huawei technicians carried out social media surveillance to help government officials spy on political opponents in Uganda and Zambia. This included "intercepting their encrypted communications and social media, and using cell data to track their whereabouts."[90] According to Freedom House (2018), subscriber details may be passed directly to the secret service to create a mobile phone user database.[91] Three years earlier, in 2015, emails from the Italian surveillance firm Hacking Team were leaked. It revealed that the company might have sold sophisticated spyware known as Remote Control System (RCS) to Zambian authorities. Although it is unclear whether the sale occurred, these emails pointed to the government's intent to acquire technologies that monitor and intercept user communications.[92] Two journalists Clayson Hamasaka and Thomas Zgambo, sued Airtel Zambia in June 2015 for "hacking, blocking and diverting" their phone calls and messages and those of other opposition Members of Parliament to third parties. They claimed that this happened between 2013 and 2014.[93] Brenda Zulu of Bloggers of Zambia and Bulanda Nkhowani of Paradigm Initiative state that there has also been an increase in phone tapping in Zambia. Several high profiles have had their phones hacked or tapped. There is a sense among civil society organisations that the government is spying on people and that there is a decrease in digital security.[94] The President of the Internet Society Zambia Chapter, Levy Syanseke, believes that the government has established an advanced surveillance infrastructure that is capable of tracking opposition politicians and activists. He pointed out that training in digital security for political parties, NGOs and even ordinary people is crucial. The Internet Society is involved in this kind of training.[95]

- **Cyberspace monitoring:** In 2019, the government, through the Ministry of Transport and Communications, spearheaded the formation of a Special Joint Cybercrime Crack Squad (SJCCS), a collaboration of security agencies.[96] The government has stated that the squad was created to curb cyber abuse and the spreading of fake news, but citizens see the squad as an opportunity by the state to monitor activities in cyberspace. It is believed that Huawei technicians are housed in the Cybercrime Crack Squad. In April 2020, journalists disclosed that the government's 2018–2021 strategic plan revealed plans to create a media intelligence unit housed within the ruling party's offices staffed with bloggers and hackers who would shape the online media environment.[97]

- **Interception of communication:** In May 2018, the ZICTA announced new rules requiring WhatsApp group administrators to register their WhatsApp groups and create a code of ethics or risk arrest. Critics saw the

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

[91] *Freedom on the Net: Zambia 2020*. Retrieved at: https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf

[92] *Freedom on the Net: Zambia 2020*. Retrieved at: https://freedomhouse.org/country/zambia/freedom-net/2020

[93] Airtel Zambia sued for phone hacking. *Lusaka Voice*, 19 October 2015. Retrieved at https://bit.ly/2EGxba6

[94] Interviews with Brenda Zulu, 6 October 2021, and Bulanda Nkhowani, 13 October 2021.

[95] Interview with Levy Syanseke, Founding president of the Internet Society Zambia Chapter, 28 October 2021.

[96] Chris Phiri (2019). Cyber crack squad formed in Zambia. *Zambia Reports*. Retrieved at: https://zambiareports.com/2019/02/03/cyber-crack-squad-formed-zambia/

[97] Chambwa Moonga (2020). PF Planning Covert Operations. *The Mast*. Retrieved at: PF PLANNING COVERT OPERATIONS …training intelligence unit members and manage a fully-equipped PF media centre with permanent bloggers, hackers, reporters

new rules as part of the Zambian government's efforts to control online speech.[98] Under the 2009 Electronic Communications and Transactions Act, intermediaries were held liable for the content; the state and its agencies could approach intermediaries without following legal and policy procedures in the name of upholding national security and morality.99 The ECA Act has been repealed, and issues of interception of communication have been included in the Cyber Security & Cybercrimes Act. While the new Act broadly prohibits the interception of communication, it permits law enforcement and security officials to intercept communications in the execution of their duties in accordance with an order from a designated judge of the High Court of Zambia. However, suppose the delay caused by obtaining a High Court order would result in harm to a person or property. In that case, the Act permits a law enforcement officer to intercept the communication without an order. The Central Monitoring and Coordination Centre will facilitate interception requests, managed, controlled and operated by the Government communications department in liaison with the ZICTA. Therefore, the Act has not reduced but considerably broadened the scope of law enforcement authorities to intercept communications in Zambia.

- **SIM card registration:** As in many African states, the Zambian government instituted SIM card requirements in 2012 as provided under the Information and Communication Technologies (ICT) Act No.15 of 2009 and the Statutory Instrument the Registration of Electronic Communication Apparatus No. 65 of 2011. While the government stated that the registration requirements were instituted to combat crime, investigative reports have found that subscriber details may be passed directly to the secret service to create a mobile phone user database.[100] Starting in January 2020, Zambia began to implement biometric SIM card registration. ZICTA ordered all mobile network operators to comply with the biometric standards, conduct regular interval verification exercises to ensure accuracy of the SIM database and furnish the authority with a report of all deregistered SIM cards.[101] This means that mobile network operators have to ask their mobile subscribers to register their personal information for a second time to integrate biometric data into the process. This means not just the provision of identity information but also facial biometric data.

SIM card registration has long been seen as one key modality for an emerging mobile-centric surveillance society. It may allow for a more pervasive system of mass surveillance of people.[102] The United Nations High Commissioner for Human Rights has stated that "biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals".[103] This is especially in instances where there are no adequate data protection laws. Zambia has just adopted a data protection law in March 2021. Before, data protection laws were provided under the Electronic Communications and Transaction Act No. 9, 2009, which provided data protection and privacy. Part VII, Sections 41 and 42 of that Act protected personal

[98] Ibid.

[99] Youngson M. Ndawana (2017), State of the internet freedom in Zambia 2017. Research Gate, August 2017. Retrieved at: https://www.researchgate.net/publication/331044593_State_of_the_internet_Freedom_in_Zambia

[100] Freedom House (2020). Freedom on the Net: Zambia. Retrieved at

[101] Zambia moves ahead with biometric SIM card registration (2019). ITWeb. Retrieved at: https://itweb.africa/content/JN1gP7OYZmKqjL6m

[102] Privacy International (2019). *Africa: SIM Card Registration Only Increases Monitoring and Exclusion*. Retrieved at: https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion

[103] Ibid.

information and listed principles governing the collection of personal information.[104] Despite this, the government and institutions still collected citizens' personal data for various purposes, including SIM card registration.[105] It is early to determine how the new data protection law would be implemented.

- **Fifth-generation technologies:** In April 2019, the then minister of transport and communications, Brian Mushimba, announced that fifth-generation (5G) technology for mobile networks would be introduced with backing from Huawei.[106] Although 5G mobile technologies will increase the speed of data transfer and improve bandwidth over existing fourth-generation (4G) technologies, there are national security implications. It is feared that 5G technologies could enhance the surveillance capabilities of states.[107] Chinese 5G technology is designed to instantly transmit vast amounts of data and deploy extensive surveillance cameras and facial recognition software networks.

What is worrying about these developments is the absence of a legal architecture that fences off human rights against encroaching surveillance practices. Although the Zambian Constitution guarantees freedom of expression in Article 20, application and enforcement are a challenge.[108]

[104] CIPESA (2016). *State of Internet Freedom in Zambia 2016*. Retrieved at: https://cipesa.org/?wpfb_dl=244

[105] Ibid.

[106] 5G network coming to Zambia-Mushimba,. *Lusaka Times*, Retrieved at: https://www.lusakatimes.com/2019/04/17/5g-network-coming-to-zambia-mushimba/

[107] Sue Halpern (2019). The terrifying potential of 5G Network. *The New Yorker*. Retrieved at: https://www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network

[108] Fesmedia (2018). *Africa Media Barometer: Zambia*. Windhoek, Namibia

Implications for Smart Cities

The above instances of evidence of surveillance have implications for smart cities. Smart Cities by nature are surveilled cities. When services and utilities are connected, the door is open to all kinds of digital threats. Established Smart Cities have deployed surveillance technologies that are powered by automatic data mining, facial recognition, and other forms of artificial intelligence. Therefore, Smart Cities rely heavily on collecting enormous amounts of citizens' data and the technology these smart cities rely on — huge numbers of internet of things (IoT) devices raise privacy concerns. There are growing concerns about how these technologies can infringe on free speech, privacy, and data protection.[109] One of the concerns with Smart Cities is that people cannot opt out from their data being collected and that this data may be shared with third parties.

While the Smart City project in Zambia has not reached the sophisticated and complete status as in the USA, Europe and East Asia, loopholes in data protection and cybersecurity legislation can undermine basic freedoms. Despite passing the Data Protection Act and the Cyber Security Act, the rollout of CCVT cameras in Zambia is not properly regulated. There are no clear guidelines on balancing public safety with human rights imperatives. The two Acts fall far short of regional and international standards and instruments on human rights, such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which sets the standards for cybersecurity and personal data protection laws. Another challenge is that there is a lack of policy framework on Smart Zambia.[110] The surveillance technology for the Smart City was brought in and installed before the two laws on data protection and cybersecurity were adopted, so "the government of Zambia did this whole thing the wrong way around".[111] As stated earlier, there is also no regulation to manage the use of CCTV cameras. There are also no notices on the equipment that say that these cameras are for 24-hour surveillance.[112] Bulanda Nkhowani of Paradigm Initiative states that if the government uses CCTV cameras for crime prevention, this should be transparent. The Ministry of Home Affairs should release quarterly reports stating which people were under surveillance under the reporting period and for what criminal justice purpose. So far, "there has not been any breaking news about a major criminal case breakthrough that the police have handled, and in the absence of this, then we can assume that the CCTV cameras are being used for other purposes".[113]

There was some suspicion that the Smart City technologies were used to follow the movements of political opposition members and civil society activists during the August 2021 elections. Many of them were stopped on the roads, prevented from travelling to some districts and from entering airports. The cameras are very sophisticated, and the government can follow the movements of people. There is thus a need to conduct deeper research to ascertain how surveillance technologies are being used and were used in the recent elections.[114]

[109] Wajeeha Ahmad and Elizabeth Dethy (2019). Preventing Surveillance Cities: Developing a Set of Fundamental Privacy Provisions. *Journal of Science Policy & Governance*. Vol. 15, Issue 1,

[110] Shuller Habeenzu (2021). The adoption and diffusion cloud computing in the public sector – A case study of Zambia Adoption. Retrieved at: https://researchictafrica.net/wp/wp-content/uploads/2018/01/2017_Adoption-and-diffusion-of-Cloud_Zambia_RANITP.pdf

[111] Interview with Brenda Zulu, Bloggers of Zambia, 6 October 2021

[112] Interview with Bulanda Nkhowani, Paradigm Initiative, 13 October 2021

[113] Ibid.

[114] Ibid.

Actors and interests in the digital surveillance architecture in Zambia

State actors

The Chinese state and technology companies work in tandem to export digital infrastructure projects globally. Huawei and ZTE are the most active Chinese technology firms, but other key players include Dahua, Hikvision, China Telecom, Meiya Pico and China Mobile.[115] As stated earlier, in Zambia, Huawei and ZTE are the major actors building the digital surveillance infrastructure in the country. While the broad justification for installing surveillance tools has been to fight crime, there are fears that the entanglement of the Chinese state and its vast array of technology companies in Zambia is promoting the emergence of a surveillance culture. Levy Syanseke of the Internet Society Zambia Chapter said that it is also important to note that Zambia has a high population of Chinese people. So, "it is possible that China is also installing surveillance infrastructure in Zambia to track its own people. The surveillance system in China is being extended to countries where China has many citizens".[116]

Before the current President Hakainde Hichilema came into power, the central political consideration driving rapid surveillance practices in Zambia was the imperative by the ruling party to forestall possible opposition-led rebellions through digital authoritarianism. As the country's economy worsened, so dissent grew and the government became more repressive. The opposition often faced harassment, were arrested on trumped-up charges, and spent most of their time dealing with tedious legal processes that hindered operations.[117] Surveillance interests in Zambia should be understood within these burgeoning political pressures. Therefore, the Zambian regime should not be viewed as a "blank slate" where the Chinese are bringing their oppressive (surveillance) ways. Instead, the Chinese state and technology companies "are spinning their products to fit the political demands of African elites".[118] Semi-authoritarian countries such as Zambia may find China's form of state surveillance quite appealing for their own political interests.

The involvement of the security cluster in the digital infrastructure space in both Zambia and China also raises concerns. Chinese technology companies have alleged ties to the Chinese military and intelligence.[119] China-Africa military ties are also deepening and becoming more complex. Between 2003 and 2017, African countries signed USD 3.56 billion for military and domestic security purposes. CCTV systems and military/security wares form part of purchases from the loans. In the 2015 China-Africa White Paper, it is stated that China would play a role in "maintaining and promoting peace and security in Africa" through, among other factors, helping African countries improve their counter-terrorism capabilities.[120] Zambia stands out with the largest number of loans (8) and the highest military and/or domestic

[115] Fergus Ryan, Danielle Cave and Vicky Xiuzhong Xu (2019). Mapping more of China's technology giants: AI and surveillance. *Issues Paper Report No. 24/2019*. ASPI's International Cyber Policy Centre. Retrieved at: https://www.aspi.org.au/report/mapping-more-chinas-tech-giants

[116] Interview with Levy Syanseke, 28 October 2021.

[117] Freedom House 'Freedom in the World report: Zambia'. Retrieved at: https://freedomhouse.org/country/zambia/freedom-world/2019

[118] Iginio Gagliardone, (2018). Is China changing information societies in Africa? *Bridges Africa*, 7(5), p. 12.

[119] Executive Associates (2009). *China in Africa: A Strategic Overview*. Retrieved at: https://www.ide.go.jp/library/English/Data/Africa_file/Manualreport/pdf/china_all.pdf

[120] Full Text: China's second Africa policy paper. *China Daily*, 12 May 2015. Retrieved at: https://www.chinadaily.com.cn/world/XiattendsParisclimateconference/2015-12/05/content_22632874.htm

security-related borrowing (USD 1.42 billion).[121] The Safe City Project reflects the China- Zambia Security Cooperation with increased support to the military. Research has shown a strong relationship between a country's military expenditure and a government's use of AI surveillance systems. This should raise concern in the Zambian context.[122] Therefore, military interests are implicated in the Zambian digital surveillance architecture. The entanglement of the Chinese state and military, and the vast array of technology companies that are now all too evident in Zambia is promoting the convergence of various surveillance and data-mining practices from different spaces.[123]

Participation of non-state actors

The sale of surveillance technology in Africa is often opaque. This is no different in Zambia. Although there is some evidence that the government has started to build a surveillance infrastructure, little is known about its surveillance practices and capabilities.[124] Freedom of expression and digital rights organisations were not involved in discussions on Smart City initiatives and their implications for digital rights, despite Zambia having several quite influential organisations engaged in digital rights work, such as Bloggers of Zambia MISA-Zambia, Internet Governance Forum and Paradigm Initiative. Ordinary people were also not informed on the Smart City projects, and "people woke up one day and found cameras in markets and along the major roads".[125]

Concerns about the Smart City project came from the African Parliamentarians Network against Corruption (APNAC). For instance, APNAC was concerned that the Zambian government had single-sourced Huawei to construct the US$65.5 million phase 1 of the Smart Zambia project. It has described the Safe City project as one of Zambia's worst corruption scandals in the Patriotic Front (PF) government. APNAC chairperson Cornelius Mweetwa, an opposition party Member of Parliament, wrote to the Ministry of Home Affairs to clarify the Safe City Project project. APNAC demanded that the government furnish the nation with the Safe City Project's Phase I and Phase II information. Single sourcing demonstrates Huawei's cosiness to ruling elites. APNAC thus raised concerns from a financial perspective and not from digital rights and human rights angles.

Internet rights organisation Bloggers of Zambia and other CSOs such as MISA-Zambia, Chapter One Foundation, Gears Initiative, People's Action for Accountability and Good Governance in Zambia, and the Alliance for Community Action have been vocal in raising concerns over broad digital rights issues such as the cyber security and cybercrimes legislation. By setting up the #OpenSpaceZM campaign, Zambian CSOs expressed deep concerns over the three cybercrime bills; the Cyber Security and Cybercrime Bill, the Data Protection Bill, and the Electronic Commerce and Transaction Bill that aims to regulate the online/digital space in the country. Now that the cybersecurity and data protection laws have been passed, these CSOs have raised concerns about both acts, and argue that specific provisions within the laws are unjustified and unconstitutional in a democratic society.

[121] *Chinese Lending to Africa for Military and Domestic Security Purposes* (9 April 2019). Retrieved at: http://www.chinaafricarealstory.com/2019/04/chinese-lending-to-africa-for-military.html

[122] Steven Feldstein (2019). The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace. Retrieved at: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

[123] K. Haggerty and R V Ericson (2001). The Surveillant Assemblage. *British Journal of Sociology* 51(4):605-22

[124] *Freedom on the Net Zambia 2020*. Zambia moves ahead with biometric SIM card registration (2019). ITWeb. Retrieved at: https://itweb.africa/content/JN1gP7OYZmKqjL6m

[125] Interview with Brenda Zulu, independent digital rights consultant, 6 October 2021.

While CSOs have been vocal in expressing concerns over laws that violate digital rights, they don't link these concerns to the broader surveillance practices supported by China. These organisations have not effectively engaged with the surveillance implications of the Smart City project. Thus, there are no holistic advocacy strategies for confronting surveillance laws and practices. There is very little understanding about Zambian government exchanges with China over digital infrastructure development and the growing area of surveillance and its impact on freedom of expression and digital rights. Bulanda Nkhowani of Paradigm Initiative states that there is very little knowledge of surveillance among many CSOs and also that "surveillance is hard to prove".[126] To this end, there have been weak responses to encroaching surveillance by CSOs and other non-state actors in Zambia. This is likely to strengthen the ruling regimes' hand and make them gun for blanket surveillance.

[126] Interview with Bulanda Nkhowani, Paradigm Initiative, 13 October 2021.

Conclusion and recommendations

A new digital surveillance architecture, building on the old one based on repressive colonial-era laws, is taking form in Zambia. China is positioning itself to play a core role in the development of this architecture. Like many countries in Africa, Zambia mainly uses Chinese surveillance technology, made possible by the ease of access, cost, and increased foreign direct investment (FDI) from the BRI. The adoption of surveillance products in Zambia is closely linked to Huawei's Smart Cities project. The China-sponsored Smart City initiatives in Zambia, involving installing CCVT cameras with facial recognition technologies and other digital infrastructure projects, should not be viewed in isolation from the human rights environment in the country. Over the last four years, Zambia has witnessed growing intolerance towards freedom of expression, and public and social media. Despite the guarantee of freedom of expression in the Constitution, the Zambian government has arrested journalists and individuals for critical social media posts, shut down mobile services in some parts of the country, and closed down newspapers and radio and TV outlets. Taken together, these developments indicate the current and future capabilities of the Zambian state to create a digital surveillance architecture. The emergent surveillance culture in Zambia occurs in the absence of a legal architecture that fences human rights against encroaching surveillance practices. The lack of a clear regulatory framework leaves citizens in Zambia susceptible to the misuse of surveillance technologies.

There is very little public debate on surveillance due to limited knowledge of the subject matter or an underappreciation of its implications. In the context of the ongoing global COVID-19 pandemic, surveillance is becoming critical as governments worldwide turn to surveillance technologies such as contact-tracing apps. Although the Zambian government has not put in place contact-tracing legislation, they have, like other governments in sub-Saharan Africa, tightened their hold on communication flows and used COVID-19-induced lockdowns to curb the freedom of journalists.

The new President, Hakainde Hichelema, elected in August 2021, has vowed to change the political culture of Zambia. In his debut address a few days after his election, he pledged to foster "a better democracy … the rule of law, restoring order, respecting human rights, liberties and freedoms".127 It is hoped that the new regime creates a conducive environment for digital rights.

It is therefore recommended that several things be done by civil society groups, digital rights activists, government and international funders in dealing with the emergent surveillance culture in Zambia:

[127] Sofia Christensen and Obert Simwanza (2021). Zambia's new president vows 'better' democracy after landslide win. *The Mail & Guardian*, 17 August. Retrieved at: https://mg.co.za/africa/2021-08-17-zambias-new-president-vows-better-democracy-after-landslide-win/

For Civil Society Organisations

- View surveillance practices within the broader purview of civil liberties and political rights.
- Study and understand the emerging surveillance architecture built by the government in Zambia. They should monitor Chinese infrastructure investment in the country and determine areas where freedom of expression and digital rights are infringed.
- Collaborate with scholars to examine the nature of surveillance and how it works.
- Research could help improve understanding of surveillance and strategies to lobby the government against its problematic aspects.
- Lobby the new government to sign and ratify the African Union Convention on Cyber Security and Personal Data Protection.
- The Convention on Cyber Security and Personal Data Protection was adopted in 2014 by the African Union (AU) to provide a framework for cybersecurity in Africa. The Convention obliges signatories to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime. However, five years since its adoption, only 14 of 55 AU member states have signed it, and only seven have ratified it. Zambia is not of the countries that have ratified the Convention. For the Convention to come into force, it must be signed and ratified by a minimum of 15 states.128 There should be a concerted effort by CSOs to ensure that Zambia ratifies the Convention.
- Increase awareness and advocacy for digital rights in the country.
- Design innovative campaigns to inform the public about digital rights and their importance for exercising freedom of expression. In addition, the public should be informed about governments' censorship and surveillance efforts.

For Policymakers

- Amend some of the provisions of the Cyber Security and Cyber Crimes Act to align with Zambia's human rights obligations, both domestically and globally.
- The Zambian government has made strides by adopting the Cybersecurity and Cybercrime Act and Data Protection Act. The laws have numerous shortfalls and a chilling effect on freedom of expression. The Cyber Security Act promotes censorship by the state and self-censorship, and intrusive interception and surveillance. Although the Data Protection Act has made significant strides in protecting data, the independence of the data protection commissioner, which reports to the minister of transport and communications, has raised some concerns.

[128] Yarik Turianskyi (2020). Africa and Europe: Cyber Governance Lessons. *Policy Insights 77*, January 2020. Retrieved at: https://media.africaportal.org/documents/Policy-Insights-77-turianskyi.pdf

- Draft a National Data and Cloud policy.

- The Data Protection Act requires personal data to be stored in Zambia, with cross-border data transfer subject to review by the data protection commissioner. The Smart City project also includes the establishment of the National Data Centre. There is a need to ensure the implementation of effective cybersecurity privacy, and data and cloud infrastructure protection measures.

- Establish guidelines for the Smart City project.

- The Zambia Information and Communications Technology Authority (ZICTA) should establish guidelines regarding acceptable standards for installing surveillance camera systems in public spaces. The guidelines should follow best practices in balancing privacy rights and public safety and security imperatives.

- Create public awareness on the Smart City in terms of its objectives and mandate.

- The success of a government programme cannot be separated into public understanding and impact on how the community responds to the programme. The government should create public awareness of the Smart City project and why it has embarked on it, who is funding it, and what its benefits are. The public should be able to raise concerns about the project.

Enact an Access to Information Law.

- Since its adoption in 2011, the Access to Information Bill has not been enacted. Access to Information is not only a fundamental right that empowers citizens to make informed decisions concerning how they are governed. It also allows people to participate in the decision-making process of their country meaningfully.

- For Zambian Media

- Report on the Smart City project.

- The media should scrutinise the Smart City initiative and report on its human rights implications. In addition, the media should report on China's infrastructure projects and the Belt and Road Initiative (BRI). They should expose any evidence of Chinese-style censorship or surveillance methods emerging from the Smart City project.

- For International Funders

- Capacitate digital rights organisations.

- Funders should capacitate freedom of expression CSOs and digital rights activists on cyberlaw issues, IoT, AI, and surveillance to effectively lobby on encroaching surveillance practices.

- Establish a digital rights fund.

- Funders should increase support for digital rights organisations by establishing a standalone digital rights fund. This fund should also target training for journalists to report on, follow trends in and analyse digital rights issues.

Media Policy and Democracy Project

The Media Policy and Democracy Project (MPDP) was launched in 2012 and is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg (UJ). The MPDP aims to promote participatory media and communications policymaking in the public interest in South Africa.

Visit mediaanddemocracy.com for more information.

This report was supported by a grant from Luminate.

The Media Policy & Democracy Project
exploring how the media can work better for society