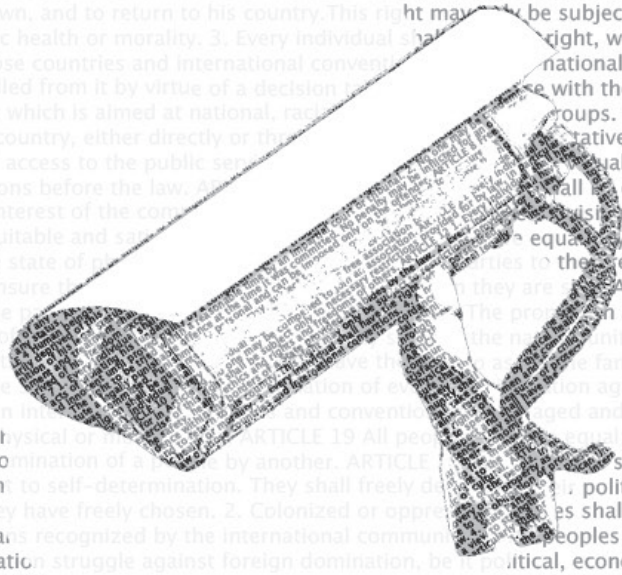
Video Surveillance in Southern Africa

Case studies of security camera systems in the region



A report for the Media Policy and Democracy Project

Main report by Heidi Swart.
Zimbabwe chapter by Allen Munoriyarwa.

Video Surveillance in Southern Africa

Case studies of Internet-based security camera systems in the region

A report for the Media Policy and Democracy Project

The growth in the surveillance of public spaces is a global phenomenon, and Southern Africa is no exception. Increased bandwidth has made it possible for governments, corporates, and private entities to purchase sophisticated, high-definition, Internet-based cameras, creating risks to data protection and other human rights and freedoms. However, little formal research has been done to establish the reach and capabilities of these surveillance systems in this region. This study attempts to address this knowledge gap, focusing on case studies in South Africa, Zimbabwe, Botswana and Angola.

The report notes that each of these countries are headed in the same direction: AI-powered surveillance, with features like facial recognition and a variety of other video analytics, often with the assistance of international industrial partners, in particular from China.

Citizens, civic group, journalists, and academics in countries should take stock of the implications of the current growth of AI video surveillance on their human rights, and plan accordingly.

Main report by Heidi Swart.
Zimbabwe chapter by Allen Munoriyarwa.

May 2020

Cover image: African Charter on Human and Peoples' Rights

Contents

List of Abbreviations and Acronyms

ANC	African National Congress
AU	African Union
BRI	Belt and Road Initiative
BTCL	Botswana Telecommunications Company Limited
BDP	Botswana Democratic Party
CEIEC	China National Electronics Import and Export Corporation
CBD	Central Business District
CCTV	Closed Circuit Television
CISP	Centro Integrado de Segurança Pública
CNEEC	Chinese National Electric Equipment Corporation
CSO	Civil Society Organisation
DPA	Data Protection Agency
DRC	Democratic Republic of Congo
DISS	Directorate of Intelligence and Security Services
FOCAC	Forum on China-Africa Cooperation
HRW	Human Rights Watch
ICA	Interception of Communications Act
ICT	Information and Communication Technology
MISA	Media Institute of Southern Africa
MOU	Memorandum of Understanding
MPDP	Media Policy and Democracy Project
SADC	Southern Africa Development Community
SANRAL	South African National Roads Agency
SAPS	South African Police Services
ZANU-PF	Zimbabwe African National People's Union-Patriotic Front
ZRR	Zimbabwe Republic Police
ZTE	Zhong Xing Telecommunication Equipment Company

1 Introduction

As high-speed global data connectivity has grown, so too have its accompanying technologies. One such technology that is very much dependent on high speed Internet is digital video surveillance. Increased bandwidth has made it possible for governments, corporates, and private entities to purchase sophisticated, high-definition, Internet-based cameras that are increasingly being used to monitor public spaces in cities and towns. These systems generate vast amounts of personal data that needs to be recorded and stored securely, and can be analysed retrospectively. The potential exists to obtain details of citizens' private lives that would not otherwise have been available on such a large scale (Rajput, 2016; Kwet, 2020).

The growth in the surveillance of public spaces is a global phenomenon, and Southern Africa is no exception. However, little formal research has been done to establish the reach and capabilities of these surveillance systems in this region (Kwet, 2016; Orlander, 2019a; Feldstein, 2019). This study was undertaken to address this knowledge gap. This is therefore an exploratory research study of the growing phenomenon of video surveillance in public spaces in selected southern African countries. These four countries include South Africa, Zimbabwe, Botswana and Angola.

Reach and limitations of this study

This study reviews open-source literature and attempts to piece together the growth of video surveillance in public spaces in southern African countries. Because the scope of this study is limited in terms of time and resources, it was not possible to map the physical video surveillance infrastructure of individual nations, or to establish the exact technical capabilities within individual countries' networks. Instead, case studies of selected countries have been undertaken. The countries included in this study are either known to have initiated programmes to install video surveillance equipment in public spaces on a city, district or national level, or have stated their intent to do so.

For the purpose of this study, public spaces are understood to include spaces to which members of the public routinely have free access, including spaces used to commute (roads, pavements, cycling paths, and public transportation lines) as well as gathering places such as parks or town squares. Due to time and financial constraints, public spaces only routinely accessible to certain sections of the population, like schools and government buildings, have not been included in this study. This research draws on a variety of information sources, all available publicly. These include news articles, academic research reports, legislation, press releases, and reports from government and civil society bodies.

Four country case studies from the Southern African Development Community (SADC) region have been included in this research. They include South Africa, Botswana, Angola and Zimbabwe. These countries were chosen for two primary reasons. Firstly, the countries differ in the degree of democratic freedoms enjoyed by their citizens, and this was useful for comparing different factors driving the proliferation of surveillance networks within these states. Secondly, these countries were included because researchers were able to obtain enough open-source information about them to ascertain definite themes that can be used as a basis for further research.

How to read this report

This study is divided into four sections.

Section One provides a brief sketch of China's role in driving the proliferation of public space video surveillance in Africa. It was thought necessary to include this section as background, since China's provision of surveillance equipment and the infrastructure upon which surveillance networks rest was a recurring theme in all countries discussed in this study.

Section Two contains an overview of the technology involved in modern public visual surveillance systems, with a brief discussion of the changes brought about by artificial intelligence in video surveillance. This study is not limited to the use of artificial intelligence in public space surveillance, however, as older forms of surveillance are still widely used (like licence plate recognition, which has been in use since the late 1970s – long before artificial intelligence became a trend in video surveillance).

Section Three includes four country case studies – Angola, Botswana, Zimbabwe and South Africa. In each country's case, a brief overview of the political context is provided, including the degree of democratic freedom that exists in the country. Information from two international human rights organisations was used in the overview to provide an indication of each country's current democratic status. These include Freedom House's *Freedom in the World Report 2019*, and the *Human Rights Watch World Report* of 2019.

The state of each country's intelligence services as well as civil society's freedom to protest, gather and express itself are also briefly visited. This was deemed necessary since intelligence services (whether tied to the police, military, or national intelligence agencies) are usually the parties involved in the use (and abuse) of surveillance systems. The repression of the right to freedom of expression and association are likely to be impacted by such use and abuse of surveillance. (Zimbabwe Lawyers for Human Rights, 2016:31-32; Stanley, 2019:35)

Following this, a brief history of China's influence in the development of each country's telecommunications infrastructure is provided. A short description is given of each country's trade arrangements with China which preceded the establishment of telecommunications infrastructure manufactured and installed by Chinese firms, particularly Huawei and ZTE. After this, each country's public surveillance networks, which usually are an extension of existing data networks, are discussed.

Finally, a short overview of the relevant surveillance legislation is provided, followed by chapter conclusions.

Section Four draws together conclusions and makes recommendations for future studies and actions based on the discussions of the previous chapters.

2 The Role of China in Public Space Surveillance in Africa

Introduction

The People's Republic of China is widely reported to be a major driver of the sale of surveillance camera networks and telecommunications equipment in Africa, including the sale of surveillance equipment to authoritarian governments. That said, China is certainly not the only country taking advantage of the African surveillance market. Many companies from the United States, Europe and Israel also sell surveillance equipment to authoritarian African governments and provide training to those countries for hacking and the use of digital surveillance methods (Kwet, 2016; Orlander, 2019a).

However, open-source information reviewed during this study suggests strongly that Chinese companies are indeed the main drivers of large scale city- and countrywide surveillance. Expanding Chinese video surveillance architecture is a part of China's Belt and Road Initiative (BRI). The BRI is China's worldwide investment and infrastructure development programme, and has been expanded to include parts of Asia, the Middle East, Africa, Europe and South America. In Africa, only 14 countries have not yet signed up for the Belt and Road Initiative. As for the countries examined in this review, South Africa, Angola, and Zimbabwe, have all signed up to the BRI. Botswana has not (Dahir, 2019b).

Some Western observers view the Belt and Road Initiative as a way for China to export not only its technologies, but also its ideologies. Commenting on the BRI generally, Amy Hawkins (2018) of Foreign Policy notes that "China's intentions go beyond providing infrastructure. It is striving to export its ideology especially around surveillance and control to African countries through the BRI initiative…"

Presence of Chinese technology and public space surveillance in Africa

In September 2019, the Carnegie Endowment for International Peace released a report titled "The Global Expansion of A.I. Surveillance". The report included an "Artificial Intelligence Global Surveillance Index" (AIGS) that aimed to sketch an "empirical picture of global AI surveillance trends". Although experts in the video surveillance field have criticised the AIGS for underestimating the prevalence of AI surveillance cameras, and conflating "conventional non-AI video surveillance with AI video surveillance", the index is still relevant to this current study. Since this review is not limited to AI surveillance, the AIGS can provide a starting point for exploring which companies are the major drivers of video surveillance equipment in SADC nations (Feldstein, 2019; Honovich & Rollet, 2019). There are 16 SADC states. They include Angola, Botswana, Comoros, the Democratic Republic of Congo (DRC), eSwatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, the Seychelles, South Africa, the United Republic of Tanzania, Zambia and Zimbabwe (SADC, 2019).

The AIGS included six of the 16 SADC nations. The six countries, as well as the companies with a significant footprint in those countries, include Botswana (Huawei), Mauritius (Huawei), Namibia (Otesa), South Africa (Huawei), Zambia (Hikvision, Huawei, Zhong Xing Telecommunication Equipment Company Limited (ZTE), and Zimbabwe (CloudWalk, Hikvision, Huawei) (Feldstein, 2019). In all these countries, the Carnegie study found Chinese manufacturers to be primary providers of AI surveillance equipment, with the exception of Namibia, which had contracted a Namibian company, Otesa Civil Engineering.

However, this current review found reports of large-scale (citywide and/or countrywide) developments of video surveillance networks driven by Chinese investments in at least three additional SADC countries: Angola, Madagascar and Mozambique. Angola is in the process of establishing a countrywide data-driven video surveillance network, and several Chinese companies are playing a role in this. Madagascar is reportedly earmarked by Huawei for smart city developments which will include video surveillance cameras – specifically its capital Antananarivo, as well as the popular island tourist destination Nosy Be (Rakotoniaina, 2015; Edjo*,* 2017; Caldeira, 2018).

It has also been reported that China's ZTE would install 450 high-definition surveillance cameras in Mozambique, specifically along the primary thoroughfares in the major cities of

Maputo and Matola. The news outlet *Verdade* reported in 2018 that the installation of the surveillance system had commenced in 2016, and was part of an extension of the country's national interception command centre designed and implemented by ZTE. The interception system was established at the behest of the Mozambican government with the express aim of intercepting all data and voice communications "between telecommunications operators and Mozambican citizens" (Caldeira, 2018).

The expansion of Chinese ICT presence to include video surveillance systems

There are a number of other reasons why Chinese companies could be considered front-runners for the supply of equipment for video surveillance network installations in the SADC nations in the future, including those countries where surveillance networks are yet to be established.

For one, China already has a very strong presence in Africa's ICT market, and surveillance cameras are increasingly a part of this market. Arguably, Chinese companies already have a foot in the door in many African countries, because they have installed the fibre Internet infrastructure on which high-definition surveillance cameras are dependent (Kwet, 2016). One source estimates Huawei's contribution to this infrastructure to comprise as much as 70% of Africa's 4G networks (MacKinnon, 2019), although China's significant ICT footprint in Africa pre-dates the 4G era. By 2010, Chinese manufacturers Huawei and ZTE were providing services to over 300 million Africans in 50 different African countries. The two companies had reportedly built over 40 3G-telecom networks in at least 30 African countries, and national fibre telecoms networks and e-government networks in over 20 African states (Zhongxiang, 2011).

The proliferation of Chinese-built network infrastructure has been attributed to the fact that China is able to offer favourable loan conditions to African governments to purchase infrastructure that those governments would not otherwise be able to afford. That infrastructure is then purchased from Chinese companies. In addition, China is not restricted by the trade regulations faced by American and European companies. It is also able to provide quality ICT infrastructure at a much lower price. Moreover, unlike Western countries, China has been a willing risk-taker in volatile and uncertain investment environments in Africa. This readiness to invest in Africa is not only true for ICT, but for a host of other infrastructure types (New

Security Learning, 2011; Moore, 2019; Executive Research Associates, 2009; Wen, 2017; The China Institute at the University of Alberta, 2019; Chen, 2009).

In line with this tendency, China's Huawei remains well-positioned to provide 5G services and infrastructure to Africa in the coming decade, despite being effectively blacklisted by the United States due to concerns that China will use Huawei's networks to conduct espionage. In May 2019, the company signed a three-year memorandum of understanding to boost ICT expertise in the African Union, and to work together on key ICT aspects. According to the MOU, Huawei will work with the AU to bolster growth in several focus areas, including the Internet of Things, cloud computing, artificial intelligence, and 5G networks (Dahir, 2019a).

The contract was signed despite news reports that the Chinese government spied on the African Union's data communications. It was alleged by multiple anonymous sources that data had been streamed from servers at the AU headquarters in Addis Ababa, Ethiopia, to servers in Shanghai, China, on a nightly basis from January 2012 to January 2017. Huawei stood accused as the main culprit since the company had provided the AU's telecommunications equipment and configured the servers. China, the African Union and Huawei denied that the hack ever occurred, and no evidence of it was ever brought forth (Solomon, 2019; Sherman, 2019).

More allegations against Huawei surfaced in August 2019 when it was reported that the Ugandan government had, with the aid of Huawei technicians, hacked into the WhatsApp chat group of opposition politician Bobi Wine. The company was accused of similarly assisting Zambian officials. In both cases, the governments and Huawei strongly denied the allegations. Once again, no evidence was ever provided (Tredger, 2018).

As worrisome as such allegations may be, observers argue that the threat of espionage is dwarfed by Africa's need for ICT infrastructure – much of which depends on Chinese funding and know-how. Africa's position is succinctly summarised in an opinion piece (published in *Quartz* in May 2019) by W. Gyude Moore, a senior policy fellow at the Center for Global Development and former Public Works Minister of Liberia:

> *In a world in which our options were again limited to Google, Pixel, Samsung, or Apple products, smartphone penetration would be abysmal. We are too poor to afford those phones. Across the continent, we log on to a fast and affordable Internet using cheap Chinese-built devices on Chinese-built networks. Africa's Internet future*

depends on components at a price that only China and Chinese companies can currently provide (Moore, 2019).

Apart from its contribution to network infrastructure required to run city- and countrywide digital video surveillance networks, China is also positioning itself in Africa to promote smart cities on the continent. This is another indicator that visual surveillance of public spaces in Africa is set to increase, since video surveillance increasingly comprises a significant component of smart city design (Ludwig Rausch, 2019; Axis Communications, 2015). In June 2018, Huawei was reported to have set up a US$1.5 billion fund to promote smart cities in Africa (Tredger, 2018; IT News Africa, 2018).

Conclusion

The purpose of this chapter was not to position China as a security threat to Africa, as this is a complex matter that is beyond the scope of this study. However, what is relevant to this research is Africa's willingness to partner with China on ICT matters despite international pressure to shun Huawei and ZTE. This type of customer loyalty indicates that these companies will retain their dominant positions in the African ICT market regardless of the obstacles they face elsewhere on the international stage. In other words, their surveillance products, which are far more affordable than any other vendors' in the world, are here to stay. The vast majority of Africa's fibre telecommunications networks are dependent on Chinese technology and funding, largely because China, unlike much of the west, has proved willing to invest in Africa.

As such, China is well-positioned to sell its video surveillance products to African countries. Notably, the companies selling such equipment on a large scale to African governments often publicly advertise this on their websites as part of their marketing strategies. These publicly announced sales could serve as an indication of the proliferation of video surveillance throughout the continent; this is a valuable indicator considering that governments, particularly authoritarian regimes, seldom publicly disclose the capabilities of their surveillance systems.

3 Video Analytics: Myths and Terrifying Realities

Introduction

Over the past decade, there has been paradigm shift in the video surveillance market from the use of analogue surveillance camera networks to digital networks. Digital cameras (more commonly referred to as IP cameras because the camera has an internet protocol (IP) address, allowing it to communicate with other devices on the network) allow for a number of convenient features making them popular, and driving market growth: these include low cost, cloud storage for footage, wireless connection allowing remote monitoring, and so-called intelligent video content analytics. This has given rise to the term “smart cameras” and “smart surveillance” (BIS Research, 2019).

With the advent of high-speed fibre Internet and big data, it is possible to use digital video surveillance cameras to capture and store petabytes of data of high-definition images continually (Rangongo, 2019; Vumacam, 2019a).

Surveillance cameras are increasingly being equipped with video analytics. Norman (2017) defines video analytics as “a technology that processes a digital video signal using a special algorithm to perform a security-related function”.

Although it is beyond the scope of this study to establish the exact capabilities of the surveillance systems in the countries reviewed in this report, it is possible to provide context for further studies. Even if exact specifications about government surveillance systems’ video analytics capabilities are not easy to establish, the analytics discussed in this chapter are those commonly used as selling points by surveillance equipment vendors. A general understanding of these types of analytics can be applied to gauge the capabilities of a surveillance system if these features are mentioned in government documentation about a specific system.

The mass surveillance systems exported by China to Africa are usually touted as "smart surveillance" systems. In 2017, China unveiled its strategy to become the global leader in AI by 2030. The Next Generation Artificial Intelligence Plan (NGAIP) endeavours to integrate AI in various spheres of human life (Yujie, 2019). The NGAIP is part of China's "Made in China 2025" plan, and the country also wants to incorporate AI into its so-called "Digital Silk Road". There are indications that China is moving away from funding large infrastructure projects (such as railways and roads) towards AI projects in the Belt and Road countries (Kariuki, 2019).

Norman (2017) distinguishes between three types of analytics: fixed algorithm analytics, artificial intelligence learning algorithms and facial recognition systems. The function of both fixed algorithm analytics and AI learning algorithms is to identify a specific type of undesirable behaviour within the camera's visual range and alert a human operator of this. Such behaviours can include a person or vehicle remaining stationary when the desired behaviour is for them to move past a certain point (Norman, 2017).

However, the two types of analytics work very differently. Whereas fixed algorithms provide a predefined set of rules, AI learning algorithms are not provided with any such rules. For fixed algorithms, the security company or government authority must have certain behaviours in mind and expressly program the software to identify these behaviours. If AI learning algorithms are employed, a surveillance camera will have to collect visual data until the AI has "learned" what usual behaviour is and what is not (Norman, 2017). It is therefore not pre-programmed by a person.

Facial recognition is used for identification purposes. It is a biometric measure, like a fingerprint, and collects data points mapping the human face. It then compares these data points to a photograph in a database in order to identify an individual (Norman, 2017).

A fourth type of analytic is licence plate recognition (LPR), also known as automatic number plate recognition (ANPR). A camera with licence plate recognition capabilities captures an image of a vehicle licence plate, then employs optical recognition software to capture the vehicle registration number (Arnold & Harris, 2013; Swart, 2018c).

It must be borne in mind that video analytics are continuously being developed for use in mass surveillance of public spaces in cities and towns. This means that the technologies have not yet been perfected: accuracy may vary for different brands and types of equipment,

and they may not perform as advertised by the vendors (Rollet, 2019a).

The fact that video analytics have not yet been perfected does not mean that citizens' right to privacy is any less endangered. On the contrary: vast amounts of personal data are required to develop these technologies (particularly where artificial intelligence is concerned) and the installation of surveillance cameras in public spaces means that this personal data will be created without the consent of the individual being filmed, and can possibly be utilised for further technology development without that individual's consent (Hawkins, 2018; Roberts, 2019).

In addition, large databases containing personal data, such as vehicle registration numbers, facial photographs, names and identity numbers, are required for LPR and facial recognition technology to work. This means that governments will need to develop such databases, and continuously collect, update and retain, perhaps indefinitely, such personal data (Arnold & Harris, 2013; Swart, 2018b).

This chapter will discuss various types of analytics, their features and limitations, and the implication of their use for individual privacy and societal freedom of movement and association.

Video analytics: Machine learning vs deep learning and artificial intelligence

In video surveillance, one of the latest evolutions of artificial intelligence is deep learning. Specifically, deep learning is a more advanced alternative to what is known as "machine learning", which makes use of fixed algorithm analytics. Deep learning makes use of artificial intelligence learning algorithms (Karas, 2017; Norman, 2017).

With machine learning and fixed algorithm analytics, a human writes algorithms that the computer software uses to identify certain predefined events in the camera's field of vision. The algorithms are set "rules" and do not change. For instance, a surveillance camera "knows" how to identify a person walking by, based on certain pre-programmed criteria that it can apply to any object appearing within its frame. The camera could be programmed to recognise that a person's height should exceed his or her width. Other parameters could include arm and leg movements, as well as the direction of movement. The algorithm will identify these parameters in a video feed, and if enough of them are present, it will "decide"

that the footage is of a person walking. The problem with machine learning is that it will at times incorrectly classify objects if they do not meet enough of the pre-programmed criteria. For example, a person crawling on the ground may be seen as a car (Karas, 2017; Norman, 2017).

Deep learning, which makes use of artificial intelligence learning algorithms, aims to overcome this limitation of fixed algorithm analytics, and refers to a computer's ability to imitate the way in which humans acquire new knowledge (Karas, 2017; Norman, 2017).

With deep learning, software uses new data, instead of preset parameters, to identify an object. The camera starts off without fixed presets generated by a human. It is essentially a blank slate at the start. As time passes, the software extracts characteristics from the visual data it collects, and teaches itself to distinguish between different object types and movement types. In other words, deep learning algorithms generate their own parameters – they are not instructed beforehand to stick to set parameters, as is the case with machine learning. In the majority of instances, a deep learning algorithm will be more effective than a human programmer and be able to learn what humans have not yet conceptualised, at a much faster rate. With so much more data at its disposal, the software can supposedly better identify objects in the footage, and update itself to improve its recognition capabilities (Karas, 2017; Norman, 2017).

A popular form of video analytics often used to punt sales of video surveillance equipment, is predictive analytics – another example of the use of deep learning. One example of predictive analytics is human activity prediction. This is an analytical function through which AI predicts what movement a person will make based on preceding movements. The aim is to identify and prevent behaviour before it occurs (Ryoo, 2011).

Object detection is a type of analytic that allows a surveillance system to identify various different objects in the camera's field of vision and to classify them (Brownlee, J. 2019). Objects may, for instance, include a human body, cars or animals. Athena Security, based in the United States, says it has developed an AI analytic that only detects guns and weapons, and touts this as a replacement for what it views as more intrusive forms of surveillance such as facial recognition (Harmon, 2020).

What this means for video surveillance in practical terms, is that analytics can be used to see if a person or vehicle is moving the way they usually do. This means that, in a typical neighbourhood security scenario, the software would be able to detect if a person in the video feed is loitering outside a home, painting the wall, or just walking by. (Machine learning algorithms can also be used for this purpose, but the assumption is that deep learning algorithms will be less likely to mistake the painter for the loiterer.) This would then send an alert to the CCTV control centre, and a security guard could then be sent to the scene (Intelligent Surveillance and Detection Systems, 2013; Stanley, 2019).

One type of AI analytic that can be used to personally identify an individual (other than facial recognition) is gait recognition. It allows a surveillance system to identify an individual based on how they walk. For example, the Chinese AI company Watrix has developed an analytic that analyses people's silhouettes. Measurements taken from a person's silhouette can be used to calculate the unique parameters of that person's gait. The analytic was developed based on pre-existing footage captured by cameras already in position. Identification of an individual is thus possible even if their face is not captured by the camera (Shepard, 2018).

Limitations on video analytics

Although terms such as "deep learning" and "artificial intelligence" are often used in marketing material to play up the effectiveness of video analytics, experts in the field are in agreement that these technologies are still developing and do not yet guarantee 100% accuracy. The following section discusses some of these limitations.

IPVM is a group of independent engineers who test IP surveillance equipment available on the international market for commercial use by businesses and governments.

In January 2020, the group published the results of a comparison of the capabilities of 15 different camera analytics from eight manufacturers. The report showed that foliage, rain, animals' shadows, and lights were factors that could cause false alerts (IPVM Team, 2020).

The IPVM group annually produces a "*Video surveillance cameras state of the market report*", which identifies market trends and product performance based on tests conducted on various manufacturers' equipment during the previous year.

In its 2019 report, it said that the artificial intelligence and deep learning products it tested "performed fairly poorly". Products varied in their quality and accuracy. The Chinese Hikvision's

DeepinMind network video recorder, for example, had several problems, including missed detections, identifying animals as people, identifying vehicles as people, and even assigning these misidentified vehicles genders (Ace, 2018; IPVM Team, 2019).

The 2019 report concluded that "the most significant potential change for surveillance cameras is when and how well deep learning will run on video surveillance cameras" (IPVM Team, 2019).

The 2020 report showed that their prediction was accurate, and that AI video analytics were improving:

> *Not only is deep learning/AI the most hyped trend for video surveillance cameras, IPVM testing shows it is significantly improving. Moreover, more AI based cameras are scheduled to be released in 2020 as the core components are maturing and being integrated into new and upcoming production cameras (IPVM Team, 2020).*

Facial recognition

Facial recognition is an identification technology, mapping data points from a person's face and comparing these to images of faces in a database until a match is found (Norman, 2017). Facial recognition analytics are used across the globe by governments in places such as police departments and border controls (Big Brother Watch, 2018; Simonite, 2019; National Institute of Standards and Technology, 2019).

At this point, it may be useful to note the distinction between facial recognition, facial detection, and facial verification. Whereas facial recognition compares an individual's face with a database of photographs of many individuals' faces, facial detection simply detects a face in an image, without comparing it to a database of facial photographs. It is therefore a form of object detection. Facial verification simply matches a newly scanned image of an individual's face (at an entrance booth to work, for example) to an existing photograph of that individual's face, in order to verify their identity. Thus there is no comparison against a database of other faces (Rollet, 2019a; Brownlee, 2019).

Increasingly, artificial intelligence is being utilised in face recognition analytics. In terms of facial recognition, the long-term goal of developers is to enable a surveillance camera to identify individuals moving in a public space, even if they are in a crowd and not facing the

camera directly. This would increase the effectiveness of tracing a person's movements, retrospectively or in real-time, by using a surveillance system continually filming public spaces, and storing the data (BIS Research, 2019; Hawkins, 2018).

Apart from identification purposes, facial recognition technology can even be used to detect mood, gender, emotion and age (Revell, 2016). China's Hikvision, the world's largest surveillance camera manufacturer, claims to have an analytic that can detect seven emotions based on facial expression, namely neutral, happy, sad, disappointed, angry, scared, and surprised (Yujie, 2019).

Limitations on facial recognition analytics

Facial recognition has been repeatedly shown to be unreliable, to the point that its usage in practical settings has been questioned by activists and professionals alike.

The IPVM group has found various vendors' facial recognition technology to render inaccurate results. Inaccuracies creep in depending on the amount of light available, the angle of the person's face, and when a subject is wearing glasses or headwear. (Rollet, 2019a; Kilpatrick, 2018; Ace, 2018; Rhodes & Rollet, 2019).

British lobby group Big Brother Watch obtained statistics about the use of facial recognition at 35 British police stations, and released a research report on their findings in May 2018. The technology incorrectly identified innocent people as suspects in over 95% of cases. For the South Wales police station, for instance, accuracy was 9%. That station had 2,451 innocent people's biometric photos in their database, and none were persons of interest or criminals (Big Brother Watch, 2018).

In July 2018, the American Civil Liberties Union reported that there were severe flaws in Amazon's facial recognition program, Rekognition. To test the software, the ACLU compared facial photographs of United States congress members to 25,000 facial photos of persons who were arrested. Twenty-eight members of congress were incorrectly matched with arrestees. Both male and female congress members were wrongly identified, but about 40% of the false identifications were people of colour. Taking into account that only 20% of congress members are people of colour, this points to extreme bias in the software (Snow, 2018).

This bias towards people of colour – particularly towards black women – remains in even top-of-the-line facial recognition algorithms. The National Institute of Standards and Technology

(NIST) of the United States Department of Commerce runs ongoing tests of facial recognition software used by government bodies internationally. The NIST evaluations are viewed as a gold standard within the field of facial recognition. When companies perform well in these tests, they use their results to market their products. Dominating NIST rankings are Chinese and Russian firms, who use the results to promote their products in local markets (Simonite, 2019).

The NIST has been publishing results evaluating the effectiveness of facial recognition on different demographics since 2017. It has consistently found that the algorithms are less accurate in identifying women than men. It is theorised that this could be due to the use of make-up (Simonite, 2019).

In July 2019, the NIST published a report titled "*Ongoing face recognition vendor test, Part 1*". Fifty companies' algorithms were put to the test. Among these were the facial recognition algorithms of the French company, Indemia, whose software is used by police services in the United States, Australia and France. In the USA, for instance, it scans millions of faces of persons on cruise ships docking in the USA for comparison against Customs and Border Protection Records (Simonite, 2019; NIST, 2019).

The NIST report found that one false match occurred for every 1,000 black female faces scanned, as opposed to 1 false match for every 10,000 white women. (An incorrect match of one in 10,000 is often used as a bench mark for testing facial recognition algorithms.) This means that black women were incorrectly matched ten times more often than white women (Simonite, 2019; NIST, 2019).

In fact, the NIST and other studies have consistently found that algorithms are less likely to correctly match people with darker skin. The July NIST report found that several of the top companies' products had error rates similar to Indemia (in terms of black and white women.) White males normally had the lowest rate of false matches, whereas black women had the highest (Simonite, 2019; NIST, 2019).

In January 2019, the United States Department of Homeland Security published an evaluation of 11 commercial face biometric systems. Results showed that skin reflectance, gender, age, eyewear and an individual's height affected accuracy. Skin reflectance was found to be the strongest predictor of inaccuracy, and it also took longer for the software to match darker skin (Cook et al., 2019).

Notwithstanding the inaccuracies, facial recognition technology is better than it has ever been. The NIST evaluated 120 algorithms from 39 software developers (which represent most of the industry) and found that, between 2014 and 2018, the software had become 20 times better at searching a database and locating a matching photograph. The NIST stated that its findings are pointing to a "rapidly advancing marketplace for face-based biometric matching algorithms" (NIST, 2018).

Licence plate recognition: Optical recognition software

LPR technology – also referred to as automatic number plate recognition (ANPR) technology – was first developed in the late 1970s, and today is employed world-wide in urban and national surveillance systems (ANPR International. n.d.; Roberts & Casanova, 2012).

A camera with licence plate recognition capabilities captures an image of a vehicle licence plate, and then employs optical recognition software to capture the vehicle registration number. Thus, the number in the image is digitised. This number can then be used for analytical purposes. It can, for instance be compared to all vehicles registered with traffic authorities in a country, region, city, or town. In this way, a person's identity can be linked to the vehicle's movements.

In addition, the system could allow for the identification of a registration number that is not in the database of registered vehicles, and automatically alert a human operator. Alternatively, the system can be linked to a database of registration numbers belonging to vehicles suspected of being used in a criminal activity. The system can also identify whether a licence plate number is attached to a vehicle of a different make and model registered in traffic or police authorities' databases. Once the camera scans the registration number of a suspicious vehicle, the system can alert the human operator (Arnold & Harris, 2013; Swart, 2018c).

Limitations on LPR

Multiple factors, human and technical, affect the accuracy and effective use of LPR systems.

Lighting, distance, and contrast factors can be controlled in a factory testing laboratory, giving marketers a basis for advertising LPR technology as almost 100% effective. However, in everyday situations, variances in light (caused, for instance, by weather conditions) can

influence image clarity. Rain, dust, dirt, customised number plates, special characters and logos on a plate can result in a camera being unable to successfully scan the plate. Obstructions, like a tow-bar, or bicycle rack make it impossible for a camera to scan a plate successfully (National Law Enforcement and Corrections Technology Center, 2010; Confidential research interview, 2018; Roberts & Casanova, 2012).

Even if an image is captured with sufficient quality, the effectiveness of LPR is ultimately determined by the sophistication of the underlying software algorithms that extract the alphanumeric characters in a readable digital format from the image (Roberts & Casanova, 2012).

The effectiveness of LPR technology in identifying vehicles is also reliant on the availability and accessibility of vehicle registration databases. Without access to, for example, a national database of registered vehicles, it will not be possible to run analytics to identify the owner of a vehicle. Similarly, an LPR system requires access to a database of vehicles of interest to law enforcement (National Law Enforcement and Corrections Technology Center, 2010; Roberts & Casanova, 2012; Gierlack et al., 2014).

Conversely, authorities may be constrained by how much of the data captured by LPR cameras they can actually store, and for how long. If there is insufficient data retention capacity, it could limit system capabilities. For instance, retrospectively mapping the movements of a stolen vehicle may become more difficult if data is not stored long enough (Gierlack et al., 2014).

Physical infrastructure also contributes to the effectiveness of LPR technology. For instance, there needs to be a reliable power supply, as well as sufficient Internet infrastructure to allow for connection between the camera, the vehicle registration databases, and the human operator in the monitoring room (Roberts & Casanova, 2012).

The human factor also bears heavily on the effectiveness of LPR. For instance, even if an LPR system is automated (meaning it can automatically scan a plate, extract a number, compare it to a database, and generate a notification for the operator if a vehicle of interest is detected), human operators still need to verify that the plate was in fact correctly scanned, and that the details connected to the registration number in the database are still relevant. That said, LPR technology scans and compares registration numbers infinitely faster and more efficiently than a human operator (Roberts & Casanova, 2012).

Staff operating the LPR system require a firm understanding of software settings, and an ability to troubleshoot and adjust the LPR system to the needs of the law enforcement body

in question. Staff administering the system also need to be able to deal with hardware and software problems, foster relationships with equipment vendors, and be capable of vetting equipment vendors. Officers must be trained to use the LPR system on a day-to-day basis (Gierlack et. al., 2014)

Systemic issues also influence the effectiveness of LPR systems. Aspects for consideration include the funding source for the LPR system, policy dictating the usage of the LPR system, and the way in which various organisations share data within the system. For instance, if it's not the policy of an organisation to access certain databases, or liaise with other role players to gain access to the necessary databases, this will hamper the effectiveness of LPR system's capability to track suspected vehicles across jurisdictions or municipal regions. If organisational leadership does not advocate for sufficient funding for the LPR system as well as for maintenance, equipment and software updates, and staff training, the system will not be put to optimal use (Gierlack et. al., 2014).

Human rights: Current signs of a dystopian future

There are many ways in which surveillance, be it LPR, facial recognition, or other video analytics, is already producing real-life snapshots of a dystopian future that may one day become the norm worldwide. Although not exclusively, China in particular has given birth to new methods of using visual surveillance to control people. Much of this is part of the country's Next Generation Artificial Intelligence Plan, published in 2017, which aims to make China the world leader in AI research and application by 2030. China plans to integrate AI in all aspects of human life (Yujie, 2019).

There are ample examples of AI video analytics being used to control citizens' behaviour on a micro level.

In March 2019, *Sixth Tone* reported that a new Class Care System is being piloted in Chinese schools that performs various functions in terms of both facial recognition and that aims to use to monitor pupils' behaviour and assess their level of engagement though a deep-learning algorithm. A surveillance camera is mounted above a classroom's blackboard and overlooks the class. It can use gestural and facial recognition, and can identify and record certain behaviours on a student's school record. These include listening, answering questions, writing, interacting with other students, or sleeping. An algorithm produces a weekly score for each student based on this data. The score can be checked via a mobile app. At the time

of the report, 28,000 students in six different schools were part of the experiment, most likely without their knowledge or consent (Yujie, 2019)

Students interviewed for the publication expressed concern that they had not been told about the surveillance system. One boy grew anxious because he thought that the system may record undesirable behaviour and prevent him from attending the university of his choice (Yujie, 2019).

Yet another type of class surveillance in Hangzhou, China, the "smart classroom behavioral management system", has been developed by Hikvision, the Chinese state-owned and world's largest IP camera manufacturer. Seven types of facial expressions of students are continuously digitally recorded and stored. These include neutral, happy, sad, disappointed, angry, scared, and surprised. Several behaviour-types are also recorded, including reading, listening, standing up, lying on the desk, raising hands and writing. As with the Class Care System, the data is used to compile a score for each student, but in this instance it is publicly displayed on a screen on the classroom wall. The Chinese public have heavily criticised the system in online forums (Yujie, 2019).

In Shenzhen, China, a company by the name of Intellifusion uses surveillance cameras to capture photos of jaywalkers. Facial recognition technology identifies them personally, and object detection technology detects unwanted movement as they cross the road. Their surname and partial government identification number is then publicly displayed on an electronic screen at the pedestrian crossing where the violation took place (Tao, 2018).

China's Hikvision has developed a technology that can distinguish between ethnicities. In both 2018 and 2019, the IPVM group found Hikvision facial recognition marketing material claiming the capability to distinguish the faces of Uyghur Muslims from those of China's majority group, Han. The Uyghurs are a persecuted minority in China's western Xingjiang province. The United Nations has estimated that at least one million Uyghurs have been detained in "re-eduction camps" (Rollet, 2019b, Nebehay, 2018).

In November 2019, the Uyghur Human Rights Project spokesperson, Louisa Greve, told IPVM:

> *"AI-enabled racial profiling for cultural extermination is the new horror brought to us by "Made in China" high tech. Through its key role in building China's 24-7 techno-surveillance state in the Uyghur Region, Hikvision is directly complicit in a crime of*

historic dimensions: Uyghurs' mass internment and torture, and a new network of permanent forced-labor factories." (Rollet, 2019b.)

Huawei is also involved in the Xingjiang region. In 2018, it signed a co-operation agreement with the Public Security Department to assist with the use of so-called smart security technology (Mu, 2018).

Although it has not been grabbing the headlines in the same way as AI and facial recognition analytics, privacy concerns about licence plate recognition technology are well established. For instance, in 2004 the Guardian reported on the installation of an LPR system at a petrol station outside Bradford in the UK. Civil groups were concerned about the collection of personal information, such as one's personal movements, and whether the data collected would be abused by authorities. There was also an expectation that the public had a right to know why their information was being collected, and how it was controlled by authorities (Oliver, 2004).

An LPR system normally scans, by default, all number plates that come into the camera's focus, even if those registration numbers are not part of a list of suspicious vehicles or vehicles of interest to law enforcement. Thus, the registration numbers of vehicles belonging to persons with no connection to crimes are recorded and stored (for periods usually determined by the authorities, since legal regulations are seldom in place to specify data retention duration) (ACLU, 2013; Swart, 2018c).

Since the scans include a data stamp, and since each camera has a fixed location, it is possible to map the movements of every road user over a period of time, depending on how long the data is stored. This leads to serious privacy and security concerns: if the databases of law enforcement authorities are not secure, either to internal or external malicious actors, it places citizens in danger. The danger can be posed by criminal actors or another state. Thus, civil society bodies have argued that the technology should be banned (Swart, 2018c; ACLU, 2013; Gierlack et al., 2014).

In September 2019, Motherboard reported on a surveillance tool developed by a private company, Digital Recognition Network, that has been passively recording licence plate numbers throughout the United States for years. Most of the plates scanned belong to innocent people. Government and businesses can buy access. The database of licence plate numbers continuously expands as hundreds of repo men, who have DRN's LPR cameras mounted on their cars, drive around the country automatically capturing the licence plate number of every car passing them (Cox, 2019).

A car's registration number can be entered into the system, which then produces a list of the times and accompanying places where the cars were photographed. Often there are details in the photograph, such as the building where a person was parked.

According to Motherboard, it has over 9 billion licence plate scans. It costs $20 to look up a licence plate number, and $70 if you want a live alert in which the DRN system will email the subscriber live updates every time a camera in the network spots the number plate in question (Cox, 2019).

Conclusion

Video surveillance technology is not perfect, but technology in general and AI video analytics in particular are rapidly improving, and innovative and draconian uses are already being demonstrated globally. Governments with vastly different political ideologies are all increasingly employing this technology, be they liberal democracies or communist autocracies. In the process, petabytes of new personal data is being created without the consent or consultation of the individuals being captured on surveillance cameras in public spaces.

China's role in the proliferation of video analytics in video surveillance cannot be overstated. Although China is by no means the only country that makes and sells this equipment, it is unique in its singular drive to establish itself as the world's dominant AI provider. In doing so, it plans not only do develop these technologies domestically, but is also determined to export it on a massive scale to other countries, particularly those signed up for the Belt and Road Initiative. Thus far, only 14 out of Africa's 55 states have not signed up for the Belt and Road Initiative (Dahir, 2019b).

It is therefore safe to assume that, in future, the installation of video surveillance networks are highly likely to include AI-powered analytics that are forever improving in accuracy.

Huawei has publicly stated that, as long as it obeys the laws of a country, it will continue business there. While giving oral evidence before the UK's Science and Technology Committee in the House of Commons in 2019, John Suffolk, Huawei's Global Cyber Security and Privacy Officer, stated:

> *"Our starting point in the 170 countries in which we operate is: what is the law, and what does the law define as acceptable and unacceptable? I think it is right for Governments to determine, in essence, their objectives and enshrine that in law."*

In response to this, the Chair of the Committee asked Suffolk, “So, if it is a dodgy regime, you will go with it?” To this Suffolk replied: “I don’t think it matters whether it is a dodgy regime; it matters what is in the law. We do not create any moral judgments on what we think is right or wrong. That is for lawmakers to do. We execute within the law in 170 countries.” (Science and Technology Committee, 2019.)

Huawei’s policy of not placing moral judgments on other countries’ local laws very much echoes China’s policy of non-interference with other regimes. It also means that Huawei will empower any government to use video surveillance on its citizens, regardless of the extent to which this erodes their human rights.

Another tool is the tried and tested licence plate recognition technology, which has quietly been developed into a mass surveillance system in the United States. This technology allows for the real-time tracking of millions of individuals by those who can pay the price. With security forces in Africa ever searching for ways to track populations, LPR offers a reliable method for governments to keep tabs on activists, political opponents, and dissidents, without the need to jump through legal hoops as the case may be with cell phone metadata. Thus, unregulated and unfettered access to personal data becomes instantly available, and the owners of that data have no control over its collection, storage, or use.

In the next chapters, this review will take stock of the proliferation of some of these technologies in selected African countries.

4 Country Case Studies

The Case of Angola

Governance

According to Freedom House (2019), Angola is not a free country. On a scale of nought to 100, where 100 is completely free, the country is ranked at 31. A single party, the Popular Movement for the Liberation of Angola, has been in power since its independence from Portuguese colonial rule in 1975.

The previous president of the country, José Eduardo dos Santos, had been in the presidential seat since 1979, and only stepped down in 2017. Journalistic, academic, and civil society movements opposing the government are known to have been placed under surveillance by security forces. Internet use is also subject to monitoring (Freedom House, 2019).

According to the Human Rights Watch's 2019 World Report, Angola's civil rights and political environments had become less restrictive during 2018, but security forces were implicated in grave human rights abuses, including extrajudicial killings of criminal suspects. In addition, HRW reported, Angolan police were still "arbitrarily arresting peaceful protesters and activists" (Human Rights Watch, 2019).

Chinese involvement in communications infrastructure development

In the early 2000s, China was prepared to invest in Angola despite the country's recent emergence from a devastating civil war that lasted from 1975 until 2002. China's Ex-Im Bank extended $2 billion credit to Angola in 2004. In return, Angola agreed to supply China with 10,000 barrels of crude oil per day as part of the long-term loan repayment. The Chinese took this opportunity following the failure of negotiations between Angola and the International Monetary Fund. Angola also participates in China's Belt and Road Initiative.

Just how much this benefits the wider population is unclear; according to Freedom House, "Public oil revenues are not equitably distributed or used to benefit the entire population. Rural regions in particular have inadequate infrastructure and access to services, leading to inequities in economic opportunity" (Hon et al., 2010; Breuer, 2017).

China's influence also extends to the country's Internet infrastructure. In 2004, the Zhong Xing Telecommunication Equipment Corporation (ZTE), of which the Chinese government is the controlling shareholder, entered into an agreement with Mundo Startel, Angola's fixed-line operator. In 2008, ZTE took over the operations of Movicel, the Angolan state-owned mobile operator (New Security Learning, 2011).

Huawei was responsible for building Angola's national backbone wireless infrastructure, and also established the fourth-generation network, bankrolled by China Ex-Im Bank. Huawei further invested US$7 million in Angola's University of Telecommunications (Universidade de Telecomunicações) and built a Telecom Technical Training Centre (New Security Learning, 2011).

Video surveillance infrastructure

Over the last the past two years, the Angolan government has been constructing a countrywide surveillance apparatus to place personal data pertaining to its entire population within a platform that can be analysed, mined, and augmented by government officials. Personal data to be collected and stored include official records (e.g. birth registration certificates, criminal records) and biometric data (fingerprints, facial photographs) for all citizens. In addition, this system is also linked to a countrywide video surveillance network that monitors public spaces.

In October 2016, the Chinese state-owned China National Electronics Import and Export Corporation (CEIEC) announced on its website that it would construct Angola's Integrated Public Security Center (Centro Integrado de Segurança Pública – CISP), the headquarters of which would be located in Ho Chi Minh Road in the Angolan capital of Luanda, and which would be "the central hub of Angolan national public security". The statement referred to it as "the first comprehensive support system for social security in the African continent", saying that the aim of the new system would be to "integrate the resources of seven functional departments", including police, transportation, fire-fighting and medical services. The system would also be employed to coordinate emergency response services at "country, province,

and city level". As part of this system, video monitoring was to be set up in a countrywide network (CEIEC (Guangdong) Fullgain Industrial & Trading Co. Ltd, 2017).

In January 2017, according to the Forum for Economic and Trade Co-operation between China and Portuguese-speaking Countries (also known as Forum Macao), Angola's government had struck a deal with CEIEC for US$243 million to "manage the country's identification card system". The platform was intended to manage Angola's civil and criminal records database, as well as the issuance of identity cards and birth certificates. The article stated that Angola had a total of 96 registration offices where identity cards were issued, but that the "flawed process leaves thousands of Angolans without any identification documents" (Forum for Economic and Trade Co-operation between China and Portuguese-speaking Countries, 2017).

In March 2017, the Angolan court approved a contract between the Angolan government and CEIEC to develop the Integrated Public Security Center (CISP) for Angola. According to the court ruling, the centre would be constructed in two phases. Phase 1 would cost the Angolan government US$243 million, to be implemented over 24 months. Phase 2 would cost US$443 million, also to be implemented over 24 months. According to the ruling, the system would serve the entire country (República de Angola Tribunal de Contas, n.d.).

In June 2017, in a report about Angola's new Integrated Public Security Management System, the news site *Macauhub* reported that earlier that month the Chinese company Beijing Global Safety Technology had announced signing a contract with the Angolan government to install an integrated public safety system. The contract, spanning 24 months at a cost of US$62.6 million to the Angolan government, would include the supply of computer applications (Macauhub, 2017). It is not clear if this amount was allocated in addition to the amounts agreed upon between the Angolan government and CEIEC, or if it was allocated through a subcontract between CEIEC and Beijing Global Safety.

Whatever the case may be, this will not have been the first partnership between the two companies. According to a November 2016 report in *The China Daily*, Beijing Global Safety and CEIEC had worked together to establish Ecuador's national response centre, Ecu911 (China Daily, 2016). In April 2019, the New York Times reported that police in Ecuador were sending footage recorded by 4,300 high powered surveillance cameras around the country to that country's domestic intelligence agency. The agency has a history of intimidating and attacking political rivals during the reign of former President Rafael Correa, the Times reported.

The footage was allegedly being shared with the agency despite the fact that they were still under investigation by the new political administration (Mozur, Kessel, & Chan, 2019).

The Ecuadorian surveillance system was built in 2011 primarily by two Chinese companies, CEIEC, and private entity Huawei, the Times reported. According to the publication, Chinese news outlets have said that a replica of the system was also built in Angola. The Ecuadorian system reportedly has 16 monitoring offices, and a staff of 3,000 monitoring the footage. The cameras have zooming capabilities which can be controlled with a joystick controller from individual monitoring stations (Mozur, Kessel, & Chan, 2019). This is typical of so-called PTZ (pan, tilt, zoom) cameras, which allow an operator to actively move the camera lens around to get more detailed footage of a specific area or event.

Like the Angolan system, the Ecuadorian system is said to connect an array of security and disaster relief services, which include the police, transportation, fire departments and medical services. The emergency number in Ecuador is 911. In Angola it is 111. This is according to the November 2016 report by the Chinese media outlet, the *China Daily*. The Chinese ambassador to Ecuador, Wang Yulin, reportedly said that since the launch of the Ecu911 centre, the crime rate in the country had fallen by 30%, although the source of this information was not identified in the article. The article also stated that Beijing Global Safety had installed its emergency platform software and equipment in "80% of Chinese cities, provinces and regions" (China Daily, 2016).

The Angolan Ministry of the Interior is also looking to Huawei for assistance with the CISP's surveillance functions. To this end the Angolan Minister of the Interior, Eugénio Laborinho, travelled to China to visit CEIEC headquarters and Huawei's headquarters in Shenzen in November 2019. This is according to an official news report from the Angolan government, which also stated that the Angolan delegation looked at using Huawei equipment and technological solutions to improve the capacity of CISP staff to respond to crime fighting and prevention (Angolan Ministry of the Interior, 2019).

Very few specifics about Huawei's contribution to the CISP were mentioned, with Mr Laborinho simply stating that "They [Huawei] maintain and develop a strategic partnership with the Ministry of the Interior, in the construction and implementation of technological solutions that will complement the systems of the integrated public security center" (Angolan Ministry of the Interior, 2019).

According to another report published in 2018 by the People's Daily Online (a Chinese state-owned news website), the Percent Corporation (a Chinese big data and artificial intelligence service provider) had constructed an intelligent system used for information visualization and data analysis. Its aim was to aid the Angolan government in resource allocation (such as allocating social grants, determining staff requirements at hospitals, and establishing schools in certain areas based on population data) and to "manage the national population information". Such information was, at that stage, managed with a paper-based system (People's Daily, 2018).

According to the news site, the new platform was to be used for data collection pertaining to the full life cycle of birth, education, marriage and social security as well as biometric information (including fingerprints, facial images) of the local population, thus "laying a foundation for smart governance". Angolan government staff were said to be trained to use the system in China (People's Daily, 2018). The People's Daily Online did not specifically state that this system was part of the CISP system. However, the Percent Corporation company profile does show that it operates the "Big Data Joint Lab" in partnership with CEIEC. The Percent Corporation has also received investment funds from China's state-owned Capital Venture Investment Fund (Beijing Percent Information Technology Co., Ltd, 2018).

In August 2017, *Agência Angola Press* (2017) reported on a ceremony for the laying of the CISP main centre's foundation stone in the capital of Luanda. The stone was laid by then head of state, José Eduardo dos Santos, since the CISP is a presidential initiative. The lead government department in the project – the Ministry of the Interior – was present at the ceremony, as were top officials of the Justice Ministry and the National Police. At the time, the Minister of the Interior, Ângelo da Veiga Tavares, reportedly told the press that the new centre would handle electronic passports, identity cards, and a more advanced system of criminal record keeping. Another article about the ceremony appeared in August 2017 on the Angolan tech-centred news site, *Menosfios*. It stated that the CISP centre in Luanda would be connected to provincial centres via "fibre optic networks, satellite communications and microwave" (Massala, 2017; Sena, 2018; Jornal de Angola, 2019a).

More detail about the project was made public by a government official through the television news site of TV Livre Angola (Free Television Angola) in October 2018. According to the report, another centre, the Huila Integrated Centre for Public Security (CISP) was to be built in the city of Lubango in the province of Huila during the first quarter of 2019. While the country's primary centre was being established in Luanda, a total of 18 centres would be

constructed countrywide. The Luanda centre would be built in an area the size of 8,000 square metres. Two types of centres for the countrywide system were envisioned; type A would be constructed in the provinces of Huila, Huambo, Cuanza Sul and Cabinda and would have greater capacity since they would serve a higher population with a higher crime rate. Type B, serving smaller populations, would have less capacity. The article did not elaborate on additional indicators of such capacity (Sena, 2018; Jornal de Angola, 2019a).

Several aims of the CISP were mentioned, including "improving citizen services, enabl(ing) citizens to access emergency services anywhere in the country ... as soon as possible, public order, and citizen control". Notably, the official stated that all security forces of the country would be connected through the system. Whereas previous articles had placed an emphasis on emergency services, the official stated on this occasion that, apart from the National Police and the fire-fighting services, the Angolan Armed Forces, the intelligence services (external and internal), as well as all the organs of the interior ministry would be integrated through this system. A key element for citizen control, according to the official, was a microchip that allowed the state to access citizens' real-time data in order to verify the veracity of a person's nationality as well as call up details of the individual's criminal record.

The Angolan government has demonstrated a keen interest in identifying foreign nationals. In October 2018, according to HRW, Angola deported over 400,000 migrants, the majority Congolese. Angola has seen large numbers of refugees fleeing the violence in the Democratic Republic of the Congo (DRC). The expulsion of nearly half-a-million people was part of "Operation Transparency", HRW said, a drive aimed at eradicating diamond smuggling and diversifying the economy. The Angolan government has said that illegal mining and diamond smuggling were being carried out by "irregular migrants", but HRW say the authorities have yet to provide evidence of such criminal networks. Several migrants affected by Operation Transparency have said that the Angolan forces have killed "dozens of people", torched homes, and stolen property. Migrants said they continued to be subjected to fear and intimidation, even after the closure of the operation (Human Rights Watch, 2019).

In August 2019, local news outlet *Jornal de Angola* reported that, as part of CISP, a network of 700 surveillance cameras had been installed in Luanda Province, and a few dozen in Benguela Province. The cameras were said to have been installed as part of the first phase in establishing a surveillance network, but the article did not elaborate on further phases, nor did it mention the company responsible for installing the camera network. Apart from mentioning that the cameras would allow Angolan police to monitor cities in "real-time", and that the

infrastructure utilised the most modern information and communication technology platforms the market had to offer, there were no further details about the system's capabilities. Details about the system's installers were not mentioned in the article (Jornal de Angola, 2019b).

Legal aspects

According to Agência Angola Press, the Angolan cabinet (Council of Ministers) reviewed a proposed Video Surveillance Bill in May 2019. The bill aimed to regulate "the installation and use of surveillance cameras at critical points previously identified by police authorities", according to the article (Agência Angola Press, 2019).

The Cabinet's final communiqué on the meeting reportedly stated that the purpose of the bill was to "ensure greater security for people and goods and assist the Defence and Security forces in clarifying crimes and identifying their perpetrators". In August 2019, TechQoon, a global news site dedicated to matters related to technology, compliance and privacy industry news, reported that the Angolan Parliament had approved the Bill. Parliamentary discussions reportedly stated that the aim of the bill would be to allow government security bodies to combat domestic terror threats, which it said had increased globally (TechQoon, 2019).

The above media reports about the new bill did not mention anything about how the impact of surveillance on personal privacy will be regulated.

Currently, several laws in Angola regulate data protection privacy in Angola. These include:

- the Data Protection Law (Law no. 22/11, 17 June 2011),
- the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011)
- the Protection of Information Systems and Networks Law (Law no. 7/17, 16 February 2017).

While the Data Protection Law of 2011 pertains to the processing of personal data and provides for the role of a Data Protection Agency (Agência de Proteção de Dados (APD)), this oversight agency has not yet been established (TechQoon, 2019).

Conclusion

Angola is seeing the rapid deployment of city-wide public surveillance networks, made possible by Chinese government loans and comprised of Chinese technology. The CISP is aiming for the large-scale (i.e. country-wide, and inclusive of the entire population) integration of several data sets (age, gender, nationality, biometrics, and so forth) and video surveillance into one centralised system. This system is in turn connected to virtually all government sectors.

Four alarming issues were identified in this review.

Firstly, it appears that the country's intelligence forces will also have access to the system's information. This would be in contrast to the case in Ecuador, where this practice seems to be regarded as an irregularity (Sena, 2018). Although further details on the role of intelligence services and their use of the surveillance systems were not provided, this raises an important question: Could these agencies readily have access to the CISP's data and surveillance footage? Could it be possible for data to be routinely sent to intelligence services as part of normal protocol?

Secondly, as far as video analytics are concerned, indications are that AI analytics will become a feature of the system if companies like Huawei and the Percent Corporation are involved. This means that the Angolan public may, without their knowledge or permission, have their personal data used by Chinese technology firms for the further development of AI analytics. (For instance, using photographs of faces taken by public space surveillance cameras to develop AI algorithms for facial recognition.) These very analytics can then be sold back to the Angolan government, and used against the people whose data was used to develop these analytics.

Third, the Angolan government has all but openly stated that the CISP will be used to identify refugees. This means it is probable that the CISP could be employed to crack down on refugees and facilitate mass deportations.

Finally, the one law that can assist Angolans to protest the abuse of the CISP system, the Data Protection Law (Law no. 22/11, 17 June 2011), remains toothless as its implementing body, the Data Protection Agency, has yet to be established. Furthermore, the government does not appear to have shown much concern for individual privacy during their discussion of the Video Surveillance Bill. Rather, their focus appeared to be on how the law could empower government authorities to more effectively police citizens.

Given these four factors, and Angolan security forces' history of human rights abuses, the stage seems set for the violation of individual rights to privacy, and freedom of association, expression, and movement. The majority of the population will be placed under increasing control through further deployment of the CISP, and people will have little recourse should authorities abuse the CISP for personal of political gain.

The Case of Botswana

Governance

Botswana became the Independent Republic of Botswana on 1966 after it gained full independence from British colonial rule. Since then, the country has had five presidents, with Mokgweetsi Masisi serving as the current head of state. The Botswana Democratic Party (BDP) has been in charge since the country's first democratic elections in 1966. Botswana's last general elections took place in 2014. Of 57 constituencies, the BDP won 37. Regional and international monitoring agencies declared the elections credible. Botswana held general elections again on 23 October 2019, and the BDP won 38 seats out of the 57 constituencies. The opposition leader, Duma Boko, said that they would take legal action to challenge the results (Embassy of the Republic of Botswana, n.d.; Freedom House, 2019; Dube, 2019).

Freedom House's 2019 report rated the country as "Free", with a score of 72 out of 100, where zero indicates the least amount of freedom, and 100 indicates the highest level thereof. However, scholars have argued that, despite Botswana being widely considered as a successful model of democracy in Africa, the country is actually a liberal autocracy, and intolerance of political dissent is on the rise (Freedom House, 2019; Botlhomilwe, Sebudubudu, & Maripe, 2011). Civic society groups and human rights activists generally do not face restrictions. However, in May 2018 President Masisi banned a well-known South African human rights lawyer, Joao Carlos Salbany, from entering the country. He withdrew the ban after being criticised by human rights activists and the Media Institute of Southern Africa (MISA) (Freedom House, 2019; CIVICUS, 2018).

Freedom of assembly is enshrined in Botswana's constitution, but in terms of the Public Order Act police permission must be granted for a public gathering. The police have reportedly at times denied such permissions without legal grounds, and the constitutionality of the law has been called into question (Freedom House, 2019; Lekgowe, 2014).

Despite freedom of expression being a constitutional right, punishable restrictions can lead to self-censorship by citizens, including academics. For instance, insulting a public official, including a lawmaker or the President, can be punished with a fine (Freedom House, 2019; Constitution of the Republic of Botswana, 1966).

Botswana's primary national security agency, the Directorate of Intelligence and Security Services (DISS), stands accused of human rights violations and corruption under the rule of the country's former president, Ian Khama. In May 2019, caretaker President Mokgweetsi Masisi dismissed the head of the DISS, Colonel Isaac Seabelo Kgosi. Masisi also transferred both the DISS and the Financial Intelligence Agency (FIA) from the care of the Justice Ministry and the Finance Ministry (respectively) to that of the presidential office, sparking concern about the centralisation of power. The DISS has reportedly been acquiring technology to enable the surveillance of citizens' private online communications (Freedom House, 2019; Komane, 2019).

The DISS can arrest any citizens without a warrant should an agent suspect them of a crime, or the intention to commit a crime. The agency faces a slew of accusations, including corruption, unlawful arrests, and extrajudicial killings (Freedom House, 2019). The National Police have also faced allegations of large-scale corruption, with a 2019 survey by Transparency International finding that 39% of respondents believed the police to be corrupt (Sunday Standard, 2019; Transparency International, 2019).

Chinese involvement in communications infrastructure development

China first established diplomatic relations with Botswana in 1975, and since then China has invested billions of dollars in infrastructure in Botswana, and Chinese companies have a significant stake in Botswana's construction sector. Botswana is a partner in China's Belt and Road initiative, and is also part of the Forum on China-Africa Cooperation (FOCAC). By the end of 2017, according to China's state-owned China Global Television Network, China's investment in projects in Botswana exceeded US$101 billion. According to a November 2018 report in China Daily Africa, Botswana imported over US$100 million worth of electronics and textiles from China annually (China Global Television Network, 2018; Chen, 2009; Segaetsho, 2018).

China is a major importer of Botswana's primary mineral export and mainstay of the Botswana economy, diamonds. Unfortunately, formal figures about the value of the diamond trade between the two countries could not be sourced for this report. However, in August 2018, China Daily Africa reported that China imports US$30 million in diamonds from Zimbabwe each year (Segaetsho, 2018). In 2018, China was the world's fifth largest importer of diamonds in terms of dollar value, with a share of 7% of diamond imports valued at US$8.9 (Workman, 2019a). Conversely, Botswana exported US$5.9 billion in 2018 (Workman, 2019b). Botswana

is the leading diamond producer in value worldwide. At the China International Import Expo held in Shanghai, China, in November 2018, a Botswana government official announced that Botswana was "earmarking to export more diamonds to China" (Xinhua News Agency, 2018).

It is common practice for resource-rich African countries to include such natural resources as part of payment to China for infrastructure construction and financial contributions to parastatals (often referred to as Angola-mode) (Chen, 2009; New Security Learning, 2011).

The case of Botswana, however, does not necessarily fit this mode. A strict regulatory environment and commitment to accountability and transparency, demonstrates the challenges China faces in Africa's infrastructure sector. In this regard, Botswana has avoided the so-called "resource curse" – a phenomenon in which countries rich in mineral and energy resources have a slower rate of growth, weak democratic structures, and more socioeconomic and political problems than countries who are resource-poor (Jefferis, 2009).

In an article in which he reviews the involvement of transnational corporations (TNCs) in the extractive industry, former deputy governor of the bank of Botswana, Keith Jefferis, observes:

> *Botswana's record of mineral-led development is remarkable not just for its rapid growth, but for apparently avoiding most other aspects of the resource curse. The country is relatively free of the corruption and environmental damage that is often associated with mining industries. Public finances are strong, debt is minimal, and the country enjoys investment-grade credit ratings.* (Jefferis, 2009)

In Botswana, Chinese contractors are by no means guaranteed business, and government oversight mechanisms as well as press freedom means that contractors come under scrutiny should they not fulfil their obligations to government. In 2013, for instance, when the Chinese National Electric Equipment Corporation (CNEEC) failed to keep its schedule in the establishment of a major power plant, then President Ian Khama openly blamed the Chinese for the delay. The Botswana government did not renew the Chinese contract for maintenance and operation of the power plant; instead they awarded it to Germany's STEAG Energy Services (New Security Learning, 2011).

China has participated significantly in the development of information and communications technology (ICT) infrastructure in Botswana, with Huawei operating in the ICT infrastructure field there since 1998. It has contracts to develop ICT infrastructure with major service

providers in Botswana, although it by no means holds a monopoly. For instance, KT Corporation – a South Korean telecommunications equipment manufacturer – won major contracts with Botswana Fibre Networks (BoFiNet) in both 2014 and 2018 for fibre upgrades to the country's copper-based Internet backbone (Pulse, 2018).

Botswana is, however, still heavily dependent on Chinese ICT technology and infrastructure for its Internet access. From 2018 to 2019, Huawei Marine Networks upgraded the West Africa Cable System. The upgraded section of the 100 Gbps fibre-optic undersea cable spans a distance of 11,500 km from Portugal to South Africa. It has 12 landing points in as many countries along the western coast of the African continent. The landing point in Namibia also provides an Internet connection for Botswana, Zambia, Zimbabwe and Malawi (Huawei, 2019a; Ogundeji, 2015).

National infrastructure is also dependent on Chinese infrastructure and technology. BoFiNet is a state-owned corporation created in 2012 by Botswana's cabinet to provide and operate the country's national communications network infrastructure, in particular the national backbone fibre network. Huawei is a major partner of BoFiNet in establishing this network. All Internet service providers are dependent on BoFiNet for fibre Internet access (Botswana Fibre Networks, 2018; Botswana Fibre Networks, 2017; Churu, 2016).

Huawei has also partnered with mobile service providers Mascom (to provide 4G broadband network services) and Botswana Telecommunications Limited (BTCL) to develop rural mobile networks (Churu, 2016; Setswalo, 2015).

Video surveillance infrastructure in Botswana

Botswana's video surveillance infrastructure is in the early stages of development, and thus far a diverse group of service providers have been involved. However, Huawei remains the main contractor for the development and establishment of the country's large-scale surveillance networks. In November 2017, Botswana's National Police concluded an agreement with Huawei Botswana for a two-year contract to start Gaborone's Safer City Project. At the signing ceremony, Police Commissioner Keabetswe Makgophe stated that the project would allow the police to deliver effective police services by using surveillance cameras. At the time, Gaborone had reportedly suffered a spate of armed robberies and had generally experienced escalating crime rates (Ramaphane, 2017).

The project was set to establish a network of cameras in Gaborone and Francistown, the two cities considered to be the country's major economic centres. Construction costs were not specified, other than it being a "multi-million pula" undertaking. (One US Dollar is worth almost 11 Botswana Pula (Republic of Botswana, 2017). Commissioner of Police Keabetswe Makgophe stated in a press release in November 2017 that the project would be rolled out to "other parts of the country in future if it proves to be sustainable and effective as well as if funds permit" (Republic of Botswana, 2017; Ramaphane, 2017).

Although exact technical specifications could not be sourced for this study, the news site Privacy in Africa reported in December 2017 that Botswana Police Services (BPS) did reveal some details about the network. The surveillance network would meet "international standards" and would include "high definition cameras" and "intelligence lenses". Cameras would primarily be placed at busy intersections and "strategic corporate enclaves of high economic value". The surveillance system would reportedly also include "software packages and monitoring computers with secured database and other world-class security surveillance gadgets used globally around international premier cities" (Republic of Botswana, 2017).

In a press release in September 2018, BPS's Senior Superintendent, Near Bagali, stated that the cameras would allow police to observe events in the city in real-time, and that the cameras would be controlled and monitored from a central point. Cameras were also to be installed at traffic lights to monitor traffic offenders in an attempt to reduce road accidents and deaths. It would also assist police to apprehend motorists who knock down traffic lights and "provide evidence in cases of hit and run of pedestrians, motorists and road infrastructure vandalism". Bagali added that at the time of the statement's release, the police were still running trials with the cameras in selected locations, and that the police were satisfied with progress at that stage. The project was scheduled for completion in November 2018 (Republic of Botswana, 2018; Adepoju, 2019).

In June 2019, news site Mmegi Online reported on additional aspects of the networks in an article related to the instalment of cameras in Francistown. Senior assistant commissioner of the BPS, Gaboletswe Dimeko, stated that there would be over 500 cameras with facial recognition capabilities installed in 195 locations around the city. The system would run on a fibre optic data network. At the time, the refurbishment of Kutlwano Police Station had commenced in order to prepare it as the control and command centre for the city. Two mobile command vehicles with satellite camera equipment would also be in place by the end of the project (Kebotse, 2019; Mmolawa, 2019).

Dimeko further stated that Huawei would work with two local companies to build the Francistown network, which would cost more than BWP 200 million (US$18.4 million). He appealed to the Francistown City Council to assist with funding (Kebotse, 2019; Mmolawa, 2019). In August 2019, the installation of surveillance cameras as part of the Safer City project reportedly also commenced in Francistown, the country's second largest city. That phase of the project was scheduled for completion in December 2019 (Xinhua News Agency, 2019). At the time of writing this report, there had been no official announcement about the progress of the network installation in either city.

Legal aspects

The Data Protection Act (Act number 32 of 2018) of Botswana was passed by parliament in August 2018, the main aim being to protect personal data and the privacy rights of individuals (OneTrust Data Guidance, 2018; Mokwena, 2018; Data Protection Act of Botswana, 2018). The Act defines personal data as "*information relating to an identified or identifiable individual*" which can be used to identify that individual "*directly or indirectly, in particular by reference to an identification number or to one or more factor specific to the individual's physical, physiological, mental, economic, cultural or social identity*" (Data Protection Act of Botswana, 2018).

The Act sets out a range of principles governing the processing of personal data, such as fairness, lawfulness, adequacy, necessity and accuracy. Processing cannot occur without a legitimate purpose and establishing data security measures. Data cannot be processed without the consent of the data subject (OneTrust Data Guidance, 2018; Mokwena, 2018; Data Protection Act of Botswana, 2018).

The Act makes provision for a Data Protection Commissioner to enforce its regulations. Commissioners can take steps (for example, issuing fines) should the act be breached. The Commissioner's office has not yet been established, and the law is not yet being enforced (OneTrust Data Guidance, 2018; Mokwena, 2018; Data Protection Act of Botswana, 2018).

Conclusion

Botswana may have escaped the so-called resource curse, but it has not escaped the proliferation of public video surveillance networks. Authorities appear to have bought into the concept of digital surveillance, and the accompanying modern features. Authorities'

revelations about the capabilities of the new surveillance system (with phrases like “high definition cameras”, “world class security surveillance” and “facial recognition”) as well as the involvement of Huawei, suggests that Botswana will look to increasingly use artificial intelligence and video analytics in public video surveillance. At the very least, the stage is being set for that.

As is the case with the rest of Africa, legislation protecting individual privacy and private data is yet to be fully implemented, and the population will have little recourse should this new technology be abused by the state.

Although Botswana’s press and civil rights activists face few restrictions, some scholars have argued that intolerance of political dissent is on the rise. It is yet to be seen, however, whether or not the installation of these new public video surveillance networks are a result of this increased intolerance, or if it will contribute to increased intolerance, or both.

The Case of South Africa

Governance

From 1948 to 1994, South Africa was under the rule of a white Afrikaner National Party government that enforced the policy of apartheid on its population. Black South Africans were stripped of their most basic human rights during this period of brutal nationalist government rule. After nearly five decades of pressure on the National Party from various civic groups in and outside of South Africa, as well as international sanctions, apartheid came to an end. In April 1994, the African National Congress (ANC) won the country's first democratic election with a 62% majority. Nelson Mandela became the country's first black president (Government of the Republic of South Africa, 2019). In December 1996, South Africa's new constitution was signed into law. The drawing up of the Constitution has been labelled the largest public participation process ever to be implemented in South Africa. The process took two years, and included consultations with civic organisations, political groups, and citizens, as well as negotiations between the representatives of different political parties to settle upon a final formulation. It also had to be approved by the Constitutional Court (South African History Online, 2019).

South Africa has national, provincial, and municipal elections every five years. Each president may serve a maximum of two five-year terms. Thus far, no South African president has overstayed his term. Elections are overseen by the Independent Electoral Commission, and elections have to date always been declared free and fair. Freedom House classified South Africa as "Free" in its 2019 Freedom in the World report, with a score of 79 out of 100, where 100 represents the highest level of freedom, and zero the lowest (Freedom House, 2019). South Africa's Constitution guarantees its citizens' rights to protest against government. The Constitution has various provisions to this end, including the right to freedom of expression, press freedom, the right to assemble, demonstrate, picket and petition, the right to freedom of association, and constitutionally guaranteed political rights such as forming a political party or campaigning for a cause (Constitution of the Republic of South Africa, 1996).

Despite this, South Africa's primary government national security organisation, the State Security Agency, as well as the national police's Crime Intelligence Unit, have repeatedly been reported to conduct surveillance on and harass journalists, activists, and academics (Swart, 2019a; Mail and Guardian, 2011). In 2018, President Cyril Ramaphosa ordered a panel of experts to review the activities of the State Security Agency during the rule of former

president Jacob Zuma. The panel found that there had been political malpurposing and factionalisation of the intelligence community over the past decade or more that has resulted in an almost complete disregard for the Constitution, policy, legislation and other prescripts (The South African Presidency, 2019).

Chinese involvement in communications infrastructure development

Following the rift between the two countries during apartheid, China and South Africa established diplomatic ties in 1998 for the first time. Today, South Africa is China's biggest African trading partner, and China is South Africa's biggest trading partner. In 2018, the joint trade balance reportedly stood at R627 million (Chen, 2018; West, 2019).

South Africa is a primary centre of operations in Africa for both ZTE and Huawei. China has selected South Africa as one of its hubs from which to roll out its telecommunication strategy on the continent (along with Egypt, Algeria, Tunisia, Kenya, and Nigeria). MTN (South Africa's second largest mobile operator) and Huawei became global strategic partners in 2005 when Huawei signed a three-year contract for US$600 million with the mobile operator to provide communications equipment and services. MTN used Huawei's GSM base station sub-system for expansion of its GSM networks (Executive Research Associates Pty Ltd., 2009).

Huawei has been operating in South Africa since 1998, and by 2009 was the sole strategic partner of Telkom's 21CN integrated access network. The South African government today owns 39% of Telkom, a semi-privatised company. Huawei provided Telkom with an access platform to integrate voice, IP, and video. Also, by 2009, Huawei was providing Vodacom, South Africa's biggest mobile network service provider, with the latest 3G terminals, and another major provider, Cell C, with IP networks (Executive Research Associates Pty Ltd., 2009). Currently Huawei, ZTE, China Telecom, China Unicom and China Mobile have all co-operated extensively with South Africa's main telecom operators. At the end of 2017, 1,100 kilometres of fibre optic cable had been laid in South Africa by China Telecom (Jing, 2019). In September 2019, Huawei announced that it would team up with South African mobile data network operator Rain to establish South Africa's first commercial 5G network (Huawei, 2019b).

On October 2019 it was reported that Cell C mobile's sale to the China's state-owned China mobile was "imminent". Cell C has been in financial distress this past year. If the sale took place, it could have major consequences for the telecommunications market in South Africa,

because the company has vast resources that would allow it to "outspend" the competition, according to Eric Orlander of the China-Africa Project, a think tank specialising in Sino-African relations. According to Orlander, this is of major significance (Orlander, 2019b). "This would be the first time that Chinese companies would effectively control the entire communications ecosystem in an African country: from the data lines (China Mobile/Huawei) to the networking gear (Huawei/ZTE) to the consumer hardware (Tecno/Oppo/Innix) to the customer relationship through Cell C (China Mobile)" (Orlander, 2019b).

Video surveillance infrastructure

The development of public video surveillance infrastructure in South Africa has taken a different path than most other African countries. Although Chinese telecommunications equipment dominates the South African mobile network industry, there hasn't been an explosion of large government-driven surveillance projects featuring Chinese technology (as is seen in countries like Angola, for instance). One reason for this, is that South Africa's surveillance networks started developing as early as the mid-90s, long before Chinese surveillance products from the likes of Huawei, Hikvision, ZTE and Dahua became competitive brands. Although there are city-wide government camera surveillance networks, some are also privately owned, funded and operated.

However, large government-led roll-outs of public surveillance camera networks equipped with AI capabilities seem to be on the horizon, courtesy of Huawei. The company hopes to provide equipment for smart cities, and has already earmarked eKhuruleni for the pilot project of its trademark smart city brand, "Safe City Solutions". Huawei has already laid the foundation for this, having worked with the city to deploy wired and wireless networks throughout the city, as well as building cloud data centres and designing customised smart phone apps for the city. (Huawei, n.d.)

Artificial intelligence is part and parcel of Huawei's smart city technology, and the company hopes to provide South Africa with AI powered facial recognition software as part of the package. Huawei says it has already installed its Safe City Solutions in over 700 cities in 100 countries (Prior, 2019).

However, Huawei's smart city dreams for South Africa are yet to be realised.

Below follows a summary of the current state of public video surveillance in South Africa's first and second most populous cities respectively, Johannesburg and Cape Town. For each city, government-funded networks will be discussed separately from private networks, since they have distinct histories and characteristics. Although there are also video surveillance networks in other major cities and towns in South Africa, the networks in Johannesburg and Cape Town are the most extensive. In addition, these two cities have the most data publicly available about their surveillance systems. This allows for a sensible thematic presentation. For these reasons, only these two major cities are discussed in this review.

A separate section will be dedicated to the South African National Roads Agency's e-tolling system. Although this was not set up as a surveillance system, but as a billing system for drivers using the agency's toll roads, it collects and stores visual data of licence plate registration numbers through its e-toll cameras. It therefore necessarily provides a surveillance function. Since the e-toll network covers around 187 km of toll roads in Gauteng, it was deemed adequately extensive for inclusion in this review.

(i) Cape Town

Government funded surveillance networks

The first CCTV camera installations in the City of Cape Town were initially driven by the South African Police Services (SAPS), following a visit by SAPS officers to a conference in Johannesburg where they learnt about surveillance in British cities. At the time, there had been a serious spate of crime in the city's central business district from 1995 to 1997. In 1998, a pilot project consisting of a 12-camera network was launched in the city's CBD. The pilot was a joint effort between the City of Cape Town municipality and the local private non-governmental business coalition Business Against Crime. A Finnish company, Teleste, provided the network equipment (City of Cape Town, 2017; Teleste, 2011; City of Cape Town, 2012).

Following this, the City of Cape Town municipality footed the bill of close to R8.5 million for a 72-camera network, the installation of which was completed by 1999. The City of Cape Town took control of the network in June 2000. The system was digitised by Teleste in 2001. In 2009, the project was further expanded, with its STM1 ATM network being upgraded to 10Gb ethernet. Teleste worked with a second company, South Africa's Fibre-Based Integrations, to upgrade the system (City of Cape Town, 2017; Teleste, 2011; City of Cape Town, 2012; Teleste, 2013).

Today, the system monitors large parts of Cape Town's surrounding suburbs, as well as the city's highways. The system is controlled from two main control centres. Feeds can be switched and shared between the control centres, and each centre can operate independently. The first centre to be established was the Communicare Control Room of the Metro Police Department in the CBD. The second control room is located at the city's Transport Management Centre (City of Cape Town, 2017; Teleste, 2011; City of Cape Town, 2012; Teleste, 2013). In 2010, a South African company, Transport Telematics Africa, installed an additional 32 cameras in the CBD (Transport Telematics Africa Pty Ltd., 2010). By the end of 2018, the city had a total of 1,578 cameras in its entire network. The networks consists of sub-networks (Researcher's correspondence with the City of Cape Town, 2018).

The city's Integrated Rapid Transit System (the city's public transport network which includes the MyCiti Bus Routes and bus stations) has 713 surveillance cameras (Researcher's correspondence with the City of Cape Town, 2018). The city's Freeway Management System has an additional 239 cameras used primarily to monitor traffic on the city's main roads and highways. It allows the city to send concise messages to "overhead variable message signs" along the road to inform road users about accidents, emergencies, maintenance issues, or adverse weather conditions along the route (Researcher's correspondence with the City of Cape Town, 2018).

The Metro Police Strategic Surveillance Unit network is dedicated to crime surveillance. Of its 626 cameras, about 514 have pan, tilt and zoom (PTZ) capabilities (Researcher's correspondence with the City of Cape Town, 2018). About 514 of these are equipped with both PTZ capabilities as well as licence plate recognition technology, or LPR (Researcher's correspondence with the City of Cape Town, 2018). PTZ keyboards allow an operator to move the camera lens upward, downward, or sideways, and focus on a specific angle. Thus, it is possible for the camera's lens to maintain focus on a fleeing suspect. As long as the suspect remains within the network's parameters, his or her movements can be tracked in real-time. (Transport Telematics Africa Pty Ltd., 2010; Researcher's correspondence with the City of Cape Town, 2018).

The licence plate recognition system digitally captures a car's registration number. The car and number plate are photographed, and optical recognition software allows the system to identify the car's registration number on the number plate. The registration number can then be compared to a database of number plates. The data is stored and can be analysed later to retrospectively map an individual's driving patterns. In addition, although it is not a

clear or high-definition photograph, it is at times possible to identify the driver and front-seat passenger in the photograph (Demonstration attended by researcher, 2014; iTrackLPR, n.d.).

A registration number can be entered into a database in order to retrieve data that has been gathered about that number by the surveillance system. These typically include the series of photographs of the front of the vehicle, the location of each camera that took each photo, and the time when each photo was taken. The network is connected to eNatis, South Africa's official electronic National Traffic Information System, allowing a network operator to access the vehicle owner's personal details attached to the vehicle registration number. The system can also be programmed to alert authorities when a suspicious vehicle is detected. LPR cameras are also used at roadblocks to flag motorists with outstanding fines. They are also utilised to enforce speed-over-distance traffic fines, and to capture licence plates of vehicles illegally driving in the city's dedicated "bus lanes" during restricted periods (Demonstration attended by researcher, 2014; iTrackLPR, 2014; Mzekandaba, 2016a).

The surveillance network is operational 24 hours a day. Footage is recorded and stored for 30 days, and the system has a storage capacity of 1.4 petabytes (Researcher's correspondence with the City of Cape Town, 2018). By the end of 2019, the City of Cape Town planned to have an additional 44 cameras added to this subnetwork. Cameras would be equipped with LPR capabilities. The extension was made possible by funding from wards – areas demarcated by the municipality in which communities are represented by a dedicated ward councillor (Independent Online, 2019).

Privately funded surveillance networks

A total of 513 private cameras were registered with the city at the end of 2018, as is required by its by-laws. The City has however stated that it is not incorporating these feeds into its system (researcher's correspondence with the City of Cape Town, 2018). The Cape Town network does not have analytical capabilities such as facial recognition, or any other form of biometric measurements. It completely relies on human operators to interpret data feed (Researcher's correspondence with the City of Cape Town, 2018).

The majority of middle- to high-income neighbourhoods in Cape Town have LPR cameras installed at major intersections, and are controlled from control centres within those neighbourhoods. These more affluent suburbs have funded the system by private contributions from residents. The various sub-networks are connected, and it is possible for different control rooms to share information with each other (iTrackLPR, n.d.; Independent

Online, 2019; Seldon, 2015; interview with representative of Cape Town LPR User Group, 2018).

A significant part of the system is cloud-based and can be accessed in real-time through various types of devices connected to the Internet, including laptops and cell phones. This platform was created by a South African company called iTrack (iTrackLPR, n.d.).

There is currently no government regulation in place controlling these private systems, and the data is controlled, analysed and managed primarily by private neighbourhood organisations. Information is shared with law enforcement organisations and private security companies for crime prevention services. Those with access to the system are strictly vetted by police (Interview with representative of Cape Town LPR User Group, 2018).

Very little open-source information about equipment brands could be sourced for this report. However, the information available indicates that a May 2015 press release on Hikvision's website stated that 42 Hikvision cameras with day/night capabilities were installed in the suburb of Sea Point, Cape Town. A CCTV specialist who was involved in the installation of Cape Town's first CCTV installations told this researcher off the record in October 2018 that Cape Town's original system was built with cameras from Geutebrück, a German surveillance camera manufacturer (Industry source interview, 2018).

(ii) Johannesburg

As is the case with Cape Town, Johannesburg's CCTV surveillance network is a hybrid of privately funded and state-sponsored cameras.

Government funded surveillance networks

The Johannesburg central business district was first outfitted with a surveillance camera network in 1999. The contract was awarded by the City of Johannesburg to South African company Cueincident. (Cueincident was a company formed by the Business Against Crime initiative. The BAC worked with the City of Cape Town to establish that city's first surveillance network in 1998. Cueincident would later establish Pretoria's first surveillance network in 2004.) (Larsen, 2006; Czernowalow, 2005; Intelligent Transport Society South Africa, 2013).

In 2008, a Mauritian company, Omega Risk Solutions, won a tender from the City of Johannesburg to install additional cameras in the existing network of 109 cameras and to take

over operations and maintenance of the system, thereby replacing Cueincident. Omega Risk Solutions has implemented surveillance projects in Angola, Ghana, Namibia, Mozambique, Nigeria, Zambia and Iraq (Swart, 2018b; Businesstech, 2018). The City of Johannesburg did not renew Omega Risk Solutions' contract after it expired in April 2017. Instead, the city itself took over the operation and maintenance of the network and the control centre. Following this, there have been news reports about witness accounts that the CCTV system in Johannesburg is not fully functional, although the city has denied this (Slabbert, 2017; Swart, 2018a).

In July 2018, the Johannesburg Metropolitan Police Department (JMPD) added an additional 50 cameras to the 450 already in place in its inner-city surveillance network. (Of these 450, at least 318 have PTZ capabilities. The cameras could reportedly have a range of up to 3 km within which they could zoom in and capture accurate images.) The City stated that the new cameras would have facial recognition features and movement prediction (an analytic feature through which software identifies motion that is "suspicious" and then sends an alert to the human operator). The additional 50 cameras were said be capable of a 360 degree rotation, thus solving the problem of so-called "blind spots" – patches that fall outside of the camera's view. At the time, the police spokesperson said that the new cameras had a visual range of up to a kilometre, although specific details about camera range and resolution were not provided (Businesstech, 2018; Johannesburg Metropolitan Police Department, 2015; Defence Web, 2009).

The data feeds from the CCTV camera network are connected to the city's Integrated Intelligence Operation Centre (IIOC). The IIOC is part of Johannesburg's transformation to become a "smart city". The centre was launched in May 2019. The IIOC serves to improve coordination of the city's emergency and law enforcement resources by integrating all municipal data. The network operates on a 900 km fibre broadband network. The city reportedly paid over R1.3 billion for its installation in order to serve its internal communication needs. The city plans to have data from all city-owned agencies to feed into the IIOC data centre to allow better service integration, including emergency response services and health services. In May 2019, the JMPD launched a special unit of 80 undercover police officers dedicated to emergency responses to crimes detected by the CCTV network (Moyo, 2019; Mzekandaba, 2016b).

Privately funded surveillance networks

Johannesburg has become a notorious hotbed of crime in the CBD, townships and suburbs. Burglaries and hijackings are a common concern for residents (Businesstech, 2019; Radio 702, 2018; South African Police Service, n.d.). In 2015, residents of the affluent Johannesburg suburb, Parkhurst, started up a privately funded initiative to bring fibre-to-home Internet to their neighbourhood with the express aim of installing digital surveillance that would only be possible with high-speed Internet. At the time, an employee of the fibre network provider, Vumatel, said that the camera feed would be transmitted to a control room and remotely monitored. Here, analytics such as number plate recognition and facial recognition could be applied to the video feed. There were also plans to install infrared and heat-source cameras with GPS technology to map incidents and so-called abnormal movements (VPRO Documentary, 2015; Kwet, 2016).

In February 2019, Vumacam, a subsidiary of Vumatel focusing exclusively on high-definition video surveillance, announced its intention of installing 15,000 high-definition surveillance cameras. This was made possible because the Johannesburg area had sufficient fibre Internet infrastructure in place with capacity to accommodate the video feed (Kwet, 2016; Intelligent Surveillance and Detection Systems (Pty) Ltd (ISDS), 2013; Vumacam, 2019a). In a press conference held in February 2019, Vumacam representatives told reporters that their cameras would not provide facial recognition analytics, since this technology was still in the development phase and not ready to be employed in the field (Vumacam press conference, 2019).

During the same press conference, Vumacam stated that the cameras would be developed and manufactured by China's state-owned Hikvision. Vumacam stated that it had a special relationship with Hikvision, and that Hikvision was developing equipment tailored to Vumacam's needs. Although Hikvision already has a significant footprint in the private security industry and established a South African branch in 2015, the Vumacam project is the first large-scale roll-out of its kind in South African suburbs. Vumacam hopes to take its network to other South African cities. (Vumacam press conference, 2019; Swart, 2019b).

Hikvision has a poor cybersecurity track record and has been accused of building back doors into their camera equipment. There are also concerns in the industry that the company does not sufficiently ensure that customers are made aware of vulnerabilities and upgrades to address the vulnerabilities. This has created concern that their cameras can be easily

hacked. When asked about the security of their network, Vumacam said that it had tested the vulnerability of Hikvision products to ensure they could not be hacked (Swart, 2019b).

Vumacam's network is essentially funded by local residents in Johannesburg. Residents' Associations rent Vumacam's video feed for R730 a month per camera. Vumacam owns the cameras. Private security companies hired by residents' associations monitor the camera feeds from neighbourhood control rooms. Security staff can only monitor the feed from the neighbourhood they are guarding (Swart, 2018c). Vumacam's cameras, according to the company's website, have licence plate recognition (LPR) capabilities. The licence plate of every vehicle passing within range of a camera, whether on a list of suspicious vehicles or not, is captured and compared to "multiple databases of verified Vehicles of Interest (VOI)", according to the company's website. The database includes the South African Police Services' database of stolen vehicles, forged number plates and wanted criminals. The cameras reportedly register an average of around 500 registration numbers per minute (Vumacam, 2019a; Rangongo, 2019; PWP Neighbourhood Watch. 2017).

During Vumacam's press conference in February 2019, the company demonstrated various analytical tools that could be used with their video feed. There is some indication that surveillance companies are paying heed to activists' pleas for personal privacy. In a news report on Vumacam's surveillance in March 2019, a demonstration of one private security company's use of Vumacam's video feed showed that a security guard did not monitor the video feed constantly. Instead, the system employs "black screen" technology. This means that analytical software detects "suspicious" movements (Unusual or suspicious behaviours or actions picked up by the software included a car reversing on the wrong side of the road, and three people standing too close to a resident's perimeter fencing.) and then alerts the operator. Only then is the image shown on the screen (Carte Blanche, 2019).

However, except for LPR analytics, all other analytical software for use with Vumacam's video feed would have to be provided by the customer. It is therefore up to the entity monitoring the video feed to choose their own analytical tools (Vumacam press conference, 2019). This makes it difficult to assess the system's capabilities as a whole, since system capabilities will vary depending on which analtyics residents associations or neighbourhood watch organisations choose to employ.

Vumacam says that its cameras operate 24 hours a day, seven days a week, with 96% "uptime". The cameras are capable of producing clear images during both day and night.

Data is recorded and stored for about 14 days. The data is not compressed, and the latest statements from Vumacam say that the cameras generate around 30 petabytes of data per month. Data is stored at a third party data centre hosted by private company Teraco (Vumacam, 2019b). At the time of writing this report, Vumacam's website stated that it had installed 1,500 cameras in Johannesburg, covering an area of close to 500 square kilometres (Vumacam, 2019a).

Vumacam has stated that it complies with the Protection of Personal Information Act in its management of the data, despite the Act not yet being in effect. It has stated that it vets every security company that purchases access to its data feed and signs an agreement with the company to be periodically audited by an independent external company to ensure adherence to the terms. However, legal experts have warned that once the Act is implemented, the company may struggle to justify its collection and creation of such massive amounts of personal information without the consent of individuals filmed by their cameras (Vumacam, 2019b; Rabkin, 2019; Moubray, 2019).

(iii) The case of SANRAL and e-tolls

In 2011, the South African National Roads Agency Limited (SANRAL) started the process of motorist registration with their electronic tolling system (e-toll system) that would be used to bill motorists for using specific roads (Finance24, 2013). A so-called Intelligent Transportation System (ITS), Gauteng Open Road Tolling uses licence plate recognition technology to register each time a vehicle passes through an electronic toll gantry (unless a vehicle is outfitted with a special e-toll tag that is registered by an e-toll gantry every time that vehicle passes under it). Images used for LPR are captured by cameras mounted on the gantry (Finance24, 2013; Daniel, 2018; Clarke, 2014). A company by the name Electronic Toll Collection (Pty) Ltd (ETC), which is a subsidiary of Austria's Kapsch Group, designed, constructed and still manages the e-toll system (Samuels, 2014).

The e-tolls cover around 187 km of roads in the Gauteng province (Daniel, 2018; Toll Infrastructure Services, 2015).

The network operates on a fibre optic communications backbone specifically constructed for this purpose. There are a total of 42 gantries, with a central operations centre located in Midrand, Gauteng. The SANRAL head office is linked to the fibre optic communications backbone, and traffic data is uploaded to SANRAL's system from "traffic data loggers"

placed along roads (Toll Infrastructure Services, 2015). Gauteng Open Road Tolling has met with staunch public opposition, albeit not due to privacy issues. Road users refusing to pay tolls had a collective debt of R11 billion in 2018. SANRAL has been accused of ignoring the public's input collected during the public consultation period prior to construction of the system (Finance24, 2013; Daniel, 2018).

Legal aspects

The South African Constitution guarantees an individual's right to privacy. There are, however, no laws governing any form of visual surveillance (electronic or otherwise) in South Africa (Constitution of the Republic of South Africa, 1996). The Protection of Personal Information Act (POPIA), designed to regulate the collection and processing of personal data, was signed into law in 2013. However, at the time of writing this report, only the sections of the act allowing for the appointment of an Information Regulator have been enforced. Despite those executives' appointments four years ago, the body is not yet fully functional. Thus, personal data is as yet not being protected by the Act (Moubray, 2019). There are no laws explicitly governing video surveillance in public spaces in South Africa.

Conclusion

South Africa's public video surveillance systems are a hybrid of privately and state-funded networks. Thus far, public fear of crime seems to have been the major driving force behind the proliferation of surveillance systems, and the public funds large parts of these networks in suburban areas in both Johannesburg and Cape Town. In contrast to other African countries, Chinese tech companies' ambitions to dominate the global surveillance market, and the AI market in particular, have not yet fully impacted the South African market; the presence of China's Hikvision in Vumacam's private networks seems to have largely been motivated by their competitive pricing above all else. Vumacam has, however, confirmed that they are open to using other companies' products as and when it becomes necessary.

As Huawei increasingly lobbies for the deployment of its Safe City Solutions package in South African cities, the surveillance camera networks that accompany these "solutions" are likely to grow, and South Africa will increasingly move in the direction of other African countries with regard to surveillance, namely AI-based Chinese technology.

As it stands, South Africa's video surveillance networks are effectively unregulated. If safe cities, driven by Huawei, are added to the list of unregulated government surveillance facilities, data privacy will become even more difficult to regulate, and the gap between surveillance and privacy regulations could even become insurmountable.

The Case of Zimbabwe

Governance

In 2019, Freedom House ranked Zimbabwe as partly free, with a score of 29 out of 100 (Freedom House, 2019).

The Zimbabwe African National Union-Patriotic Front (ZANU-PF) has governed Zimbabwe since the country formally became independent from the United Kingdom in 1980. Canaan Banana served as the country's first President from March 1980 to December 1987, after which Robert Mugabe, who had served as Prime Minister during that period, became President. Mugabe was in power until 2017 when he was ousted by a military coup and replaced by his vice-president, Emmerson Mnangagwa (The Irish Times, 2003; Smith, 2019).

During his tenure, Mugabe led the country to become one of the most prosperous in Africa, but starting in the mid-1990s and accelerating post-2000, the country went into decline under his rule. The economy shrank, and Zimbabwe needed foreign food aid as the population faced food shortages, and extreme poverty. Schools and healthcare services went into decline, and hyperinflation left the Zimbabwean dollar virtually worthless. With this, the political environment became increasingly hostile, with activists, journalist, and perceived dissidents facing persecution, including imprisonment, violent assault, and murder. The Movement for Democratic Change, ZANU-PF's main political opposition, claimed that during the 2008 elections, 253 people were killed as a result of political violence (Freedom House 2019; Smith, 2019; Sanger & Bradley, 2020).

In 2018, Emmerson Mnangagwa was formally elected president. The election was promptly followed by a violent crackdown by security forces on opponents. Under the rule of Mnangagwa, Zimbabwe's infamous government security agency, the Central Intelligence Organisation, has remained largely unaltered and unchallenged. In fact, the police and security services have ramped up repression in order to maintain power. In January 2019, Mnangagwa announced petrol prices would be increased by 150%. This further fuelled citizen's anger about the country's weak economic state, and large protests broke out. Protesters were met with a lethal pushback from police and the military, and faced gun violence, arrest and torture. To further stifle dissent, there was an Internet shutdown that lasted seven days. (Freedom House, 2019; Human Rights Watch, 2019).

On 15 January 2019, the government ordered all telecoms operators to block WhatsApp, Twitter and Facebook. Later that day, all access to the Internet was blocked. There was an outcry from civil society, and the High Court in Harare ruled the Internet shutdown illegal on 21 January 2019. The Minister of State Security had invoked the Interception of Communications Act to order the shutdown. The court said it was illegal, since only the President had the power to issue the order. But observers argued that the Act did not make provision for such a shutdown in the first place, and warned that another shutdown could be implemented, despite the ruling (Independent Online, 2019; Nyahasha, 2019).

Journalists also face intimidation and persecution. During 2019, state security agents and police detained and harrassed at least four journalists. In September 2019, a group of journalists, editors and publishers held a meeting with senior ZANU-PF officials to lay complaints about intimidation of journalists by party members (Human Rights Watch, 2019).

Chinese involvement in communications infrastructure development

After 2000, Mugabe's actions increasingly isolated Zimbabwe from the West, and the country was cut off from the aid of financial bodies like the International Monetary Fund and the World Bank. China stepped into this vacuum, and has since established strong trading ties with Zimbabwe and invested millions of US dollars in infrastructure projects (Bhoroma, 2018).

For instance, in 2013, China spent US$200 million for China's Anhui Foreign Economic Construction Corporation (AFECC) to build the Long Chen Plaza. In 2018, China Exim Bank made available the first tranche of the US$1.4 billion committed to expand the Hwange Power Station, and also backed the expansion of the Victoria Falls International Airport in 2016 for US$150 million. In each case, the projects were undertaken by Chinese companies. These are just a few examples of the many infrastructure projects China has undertaken in the country over the past two decades (Bhoroma, 2018).

China is a major contributor of state-backed credit facilities for the purchase of mobile network equipment in Zimbabwe. All of Zimbabwe's major mobile network operators have made use of Chinese loan facilities to build, expand, and upgrade their networks (Technology Zimbabwe, 2015).

There are numerous examples of the Chinese state providing financial backing for Huawei and ZTE infrastructure projects.

By 2015, the state-owned mobile network operator NetOne had started rolling out an LTE network upgrade led by Huawei with a loan facility of $218 million from the China Exim Bank (Link, 2019; Technology Zimbabwe, 2015). In December 2017, NetOne closed a US$71 million financing agreement with China Exim Bank for Huawei to expand and upgrade its networks (Mawonde, 2018).

In February 2010, Zimbabwe's privately owned Econet Wireless announced it would build links to the SEACOM and EASSy submarine fibre optic cable systems, as well as a 7,500 km fibre network connecting all major cities in Zimbabwe. In addition, it also planned to build an international fibre network linking Botswana, South Africa, Zambia, Namibia, Mozambique, Malawi, Angola, the Democratic Republic of the Congo. Fibre networks for Harare and Bulawayo were also announced. The contracts went to Huawei. (Liquid Telecom, 2010).

In 2015, Econet Wireless announced a $500 million loan from the China Development Bank and Huawei's Chinese state-owned competitor in the telecommunications equipment market, ZTE (Technology Zimbabwe, 2015).

In April 2019, the Zimbabwe Independent reported that Econet Wireless would team up with ZTE to replace redundant core network components, originally from Ericsson (Chikono, 2019; Techzim, 2019).

In March 2019, the TelOne's National Backbone Fibre Link went into commission. The US$23,6 million was funded by the China Exim Bank, and built by TelOne and Huawei (The Herald, 2019).

Video surveillance infrastructure

A notable feature of Zimbabwe's growing surveillance architecture, is the increasing involvement of China.

In the most recent development in March 2020, it was reported that Huawei had allegedly already received US$20 million to start the installation of a grid of public surveillance cameras, as part of a larger Smart City Project (presumably in the capital of Harare) with a budget of US$100 over the next five years. It was further alleged that Hikvision and CloudWalk Technology would supply facial recognition software for the project. Huawei has denied the reports (Mabaya & Motsi, 2020).

Chinese companies like Huawei, Hikvision, Dahua and ZTE have been significant drivers of the spread of video surveillance technologies in Zimbabwe. Like many African countries, Zimbabwe has benefitted from China's surveillance technologies under China's Belt and Road Initiative (BRI). However, Zimbabwe's accumulation of expensive surveillance technology in the midst of economic disaster is notable.

Hawkins (2018) notes that "Zimbabwe is signing up for China's surveillance state, but its citizens will have to pay the price..." Commenting on the BRI generally, Hawkins (2018) said,

> *China's intentions go beyond providing infrastructure. It is striving to export its ideology especially around surveillance and control to African countries through the BRI initiative ... as part of China's Belt and Road Initiative (BRI), aimed at making China a "cyber-superpower", Chinese companies offer African governments artificial intelligence and facial recognition systems. While the ostensible purpose is to battle crime, some Africans are concerned that the systems may make it easier to stifle legitimate dissent.*

In 2016, China's surveillance technology giant CloudWalk signed a deal with the Zimbabwe government to supply mass facial recognition software and devices. Commenting on the deal with CloudWalk, a weekly online newspaper reported then:

> *The Zimbabwean government did not come to Guangzhou purely for AI or facial ID technology, rather it had a comprehensive package plan for such areas as infrastructure, technology and biology (The Global Times, 2018:12).*

Yao Zhiqiang, strategic director of CloudWalk's research and development centre in Chongqing told the Global Times: "With the knowledge that Chinese facial ID technology has made rapid progress over recent years, the Zimbabwean government hopes to introduce it to the country to help accelerate its modernization by partnering with leading Chinese enterprises in the IT sector." (The Global Times, 2018:12). However, the deal with CloudWalk has provided a double advantage to the company. Cook (2019) notes that the company now has a "training ground" on which it can test facial recognition devices on black faces. Cook notes:

> *In the realm of surveillance, the western region of Xinjiang has become a laboratory for testing big-data, facial-recognition, and smartphone-scanner technologies that can eventually be deployed across China … under a new deal with Zimbabwe's*

> *government – sub-Saharan Africans could collectively enable developers to correct common race-related errors in facial-recognition software and gain market share in other parts of the world … (Cook 2019: n.p).*

There is more recent interview data[1] that points to the fact that soon after the military coup that toppled Robert Mugabe the military became more active in the installation of public space surveillance infrastructure. The role of China has been noted in many of the interviews.

The military, according to respondents, has seized much of this initiative from the police and, from the councils who were, to a very limited extent, involved. The military's signals department has been at the centre of this roll-out. One respondent pointed out, "The signals department has been central because it possesses the capabilities to roll this out. There is no other department in the whole Zimbabwe Defence Forces which can do this except them…"[2]

The growth of military-driven surveillance in the Zimbabwean context has been noted in emerging research (see Dhlela, 2020), in this field. The increasing involvement of the military in political issues should be understood as part of the post-coup power dynamics (Tendi, 2020) within the state of Zimbabwe. The coup was led by the military, and after the coup, other state security agencies were attenuated as the military became stronger, not as a state institution but as a political institution (Ruhanya, 2018). The gradual attenuation of other security agencies conversely gave much power to the military. A respondent noted that,

Even before the coup, the signals unity of the military had gained lethal powers of surveillance. Everybody close to power knew this. And those who worked within this department also knew this … the coup only meant that the military was a preferred institution of surveillance, rather than the police and the CIO as had been the case during the Mugabe era.[3]

Who are the enablers of this kind of surveillance in the military? The growing role of China has been noted in many of the interviews. The Zimbabwean authorities have received financial aid from China, which enabled them to purchase CCTV equipment from Chinese technology companies like Hikvision and CloudWalk. Beside financial aid from China, these technology companies have had direct access to the ruling elites in Zimbabwe and have negotiated their own deals to supply the authorities with surveillance technology (The Herald, 2019).

The justification for the rapid roll-out of CCTV in Zimbabwe's big cities has always centred on

1 Interviews in Masvingo with retired senior officer 28 February 2020.
2 Interview with retired signal officer of the ZNA in Masvingo 12 February 2020.
3 Interview in Masvingo with retired ZNA officer, 12 February 2020.

fighting crime. The Zimbabwe Republic Police (ZRP) had led the exercise of installing CCTV in Harare and Bulawayo (Bulawayo News, 24 March 2017). The authorities insist that CCTV will help eliminate, or, at the least, reduce crime rates in Harare and Bulawayo's streets. But there are problems with this justification of the deployment. The first problem is that crime statistics (Nation Master 2016) in Zimbabwe do not point to crime in the city centres of Bulawayo and Harare much higher than in other urban locations. Ironically, the CCTV cameras in both cities are concentrated in the major streets of both towns. For example, in Harare, the ZRP installed cameras in Julius Nyerere and Jason Moyo Avenues. It also installed cameras at Africa Unity Square opposite the National Assembly building of Zimbabwe (commonly known as Parliament Building). Second, these places are well known as the spaces in which anti-regime demonstrations have been held. For instance, the National Electoral Reform Agenda (NERA), which was demonstrating for electoral reforms, did so at Africa Unity Square. Also, anti-regime demonstrators had, since the Mugabe era, flooded the major streets of Harare mainly Julius Nyerere and Jason Moyo.

Public spaces, like Africa Unity Square in Harare, have become hotbeds of political activism. In the "construction" of public space surveillance infrastructure, both the central government and, to a very lesser extent, local government have been active participants. In the city of Harare, for example, the city council has admittedly started a process of installing cameras in public spaces like Africa Unity Square. Their efforts have been augmented by the central government which seems determined to ensure potential "opposition hotbed spaces" are put under camera surveillance. In August 2018, the Chinese company Hikvision was awarded a contract by the government to install CCTV cameras in the streets of the capital city, Harare to fight crime (The Herald, 2018). These cameras have the capability of capturing faces, movements, actions and, depending on location, even voices and utterances.

This confirms that there is more of a political dimension, than a public safety one in the roll-out of CCTV in Zimbabwe. The intention is to police anti-regime activists by intimidation. More so, there is no known public conviction of criminals, or even a single criminal in the Zimbabwe court records, based in CCTV information despite the fact that CCTV cameras have been there for more than five years now, and they continue to expand them in terms of installation. If, then, the intention of CCTV was crime fighting, there could have been an evaluation of their efficacy in this regard.

For example, large administration buildings in Harare, like Mukwati Building, and Kaguvi Building now have cameras inside. And in many occasions, the justification has been the same – to fight crime. Even the reasoning that surveillance cameras inside public buildings to fight crime has on many occasions, proved to be more fictitious than factual. For example, despite the presence of many surveillance cameras in government buildings, high profile person's offices are still broken into. In the year 2016 alone, for example, the offices of Emmerson Mnangagwa who was then Vice President to Mugabe were broken into four times. This is despite the heavy presence of surveillance cameras at New Government Complex where the offices are situated. On 23 September 2014, the offices of the then Chief Justice, Godfrey Chidyausiku, at Benjamin Burombo House, were broken into despite surveillance cameras being visible all over the building. The question becomes: If high-profile figures cannot be saved by surveillance cameras, how can they be trusted to fight crime in public spaces?

Legal aspects

There is a legal vacuum in the deployment of CCTV in Zimbabwe. Urban areas like Harare and Bulawayo are governed under the Urban Councils Act of 2015 (Chapter 29:15). The act is specific that local boards and municipalities are administered by local government, municipal and town councils. This means the councils of both cities would be expected to be at the forefront of the CCTV roll-out. Yet evidence shows that in most instances, the city authorities have had no say in the installation of these surveillance devices in areas where they, legally should have jurisdiction. A former Signals intelligence officer with Zimbabwe National Army (ZNA), noted,

> *The Joint Operations Command (JOC) (which includes the Central Intelligence Organisation (CIO), the ZRP and the ZNA), issues instructions without necessarily consulting anyone. The deployment of CCTVs around cities and towns is a national security issue and it requires presidential permission, not anyone else's.*[4]

But the Urban Councils Act Section 8 (v) is inconsistent with this thinking as it stipulates that urban councils

> *… shall direct and authorize the existing council to provide, at cost, the services of such of its own employees, security and welfare to the new authority as may*

4 About 8 interviews held in between December 2019 and early March 2020 in Zimbabwe and South Africa have pointed out this. These interviews are not particularly for this research, but yielded information that relates to this research, and can be used here.

be necessary for the proper administration, control and management of the first-mentioned area or for the proper operation of any service and any extension thereto directed to be provided in terms of subparagraph" (The Zimbabwe Urban Councils' Act, 2015:12).

Public space surveillance legislation vacuum

There is an absence of legislation governing the installation and application of public space surveillance technologies in public spaces. The major surveillance legislation in existence in the country falls far short of addressing this subject. The Information and Communication Act (ICA) does not address public space surveillance. This, perhaps, underlines the extent to which the authorities malign this kind of surveillance as a trivial issue not worth legislating, or as an important part of their political strategy allowing them, in the absence of strong legal checks and balances, to mine metadata from their target groups without fear of being limited by the law.

The absence of a legal framework governing public space surveillance in Zimbabwe is worrying on many fronts, chief amongst them being the fact that there is a growing number of private players that have started installing surveillance cameras on their premises. In the absence of a legal framework, there is a danger that people's data can be exploited for private corporates' ends. In the absence of an enabling legislation, the state cannot seek accountability from these companies and organisations since it has no "legal teeth" on which to base the request. This raises the question: what happens to data collected via publicly installed cameras and even CCTV installations within buildings and other premises? Thus, the absence of a law in this regard has consequences for the public which is unaware (in the Zimbabwean context) of the huge amounts of data that both the state and the private sector organisations have about them.

This legal vacuum is not likely to be closed any time soon. A Media Policy and Democracy Report (2019) notes that the Zimbabwean state has huge ambitions to achieve blanket surveillance. Legislation that governs this objective is not the best ally at this particular moment. Privacy International (2019) notes, particularly: "That cyber-surveillance is growing in Zimbabwe is now beyond doubt. The state is evidently determined to achieve mass surveillance/blanket on the Chinese level" (Gough, 2016).

Currently, there is no law providing for mass surveillance in Zimbabwe. However, such a law would not be difficult to pass. This is because the dominant player in the state, ZANU PF has a majority in parliament. It will, hence, be easy to railroad the law. Of course, there will be protests by activists and CSOs. But, ZANU-PF has no history of compromising on its interests, consultation or even log-rolling practices in parliament. Add to this the absence of powerful lobbying groups in Zimbabwe's parliamentary practices, and it is easy to see how such laws would be easy to bypass.

Therefore, without much civil society activism around legislation, the researcher does not expect any movement towards a rule of law based surveillance approach by the state in Zimbabwe. Private organisations are also likely to exploit this silence to "harvest" as much data as they can in the absence of a law to stop or regulate what they can and cannot keep.

CCTV Cameras, consent and data retention issues

As a result of the legal vacuum surrounding the installation of CCTV and other cameras in Zimbabwe, there a number of issues that need red flagging. The haphazard nature of CCTV camera installation in Zimbabwe's major cities, the question of public consent, which is an important standard (Gras, 2004), of their deployment, come to the fore. There are many countries the world over that value public consent in the installation of CCTV to ensure transparency and also, to an extent, to gain public legitimacy for such installations. The public ought to know that they are entering such a zone, and it should be marked as such. In other jurisdictions, legislation has developed further to include "requisition clauses" (Loch, 2017, n.p.). These are legal clauses which allow the public or employees, subjected to CCTV to make a legally protected request to access those recording themselves. The Zimbabwe case lacks such protective clauses. Though the absence of such clauses may be common in the region, it still does not hide the fact that such a lack of protection makes CCTV surveillance arbitrary and penetrative. In addition to this, there is the absence of notices wherever CCTV cameras are installed. This is yet another important requirement absent in the Zimbabwean context. Actually, it seems there is a deliberate effort to hide them from public view, perhaps in the belief that they may generate much more "incriminating" data if hidden from an unsuspecting public. The fact that there have not been known and documented public consultations around CCTV roll-out means that it was never meant to be an inclusive process altogether, and hence, it is difficult not to see nefarious intentions in the whole programme.

Conclusion

The case of Zimbabwe provides a detailed example of how Chinese companies like Huawei have extended their business in Zimbabwe, from telecommunications equipment, handsets, and business solutions to public video surveillance infrastructure.

The observation in the Global Times (2016) that "the Zimbabwean government did not come to Guangzhou purely for AI or facial ID technology", but rather accepted a "comprehensive package plan for such areas as infrastructure, technology and biology" speaks volumes: It is a clear illustration of the dynamic between China's larger infrastructure projects and the construction of surveillance networks and technology. The latter flows naturally from the former, and is simply part of a basket of services made available to African countries by China as a packaged offering.

Cook's (2019) observation that CloudWalk could use the people of Zimbabwe to train their AI facial recognition systems demonstrates how China and Chinese technology companies reap multiple benefits from the proliferating Chinese surveillance culture. It is a business: Chinese banks earn interest on loans to African governments. African governments use this money to purchase surveillance technology from Chinese companies. Then, Chinese tech companies utilise the data obtained from private citizens – like their faces – to develop their AI facial recognition even further. This can later be sold to African governments as an upgrade, or replacement, of their existing facial recognition systems.

There is need to further this research on public space surveillance to other towns and cities which have become hotbeds of public dissension against the economic crisis engulfing the country at the moment. It is also important to note that public space surveillance in Zimbabwe is gradually expanding to include the installation of cameras on government buildings. There is need to further interrogate the growing capabilities of state-driven public spaces surveillance. A thorough research study would go a long way to establish how this new threat to privacy is unfolding in other smaller towns of Zimbabwe outside the capital city Harare and the second largest city Bulawayo. At the same time, the growing involvement of private and commercial companies in public space surveillance needs further research and interrogation. In terms of surveillance research, Zimbabwe should be viewed as an on-going case as the state continues to consolidate its surveillance capabilities with the help of China.

5 Conclusions and Recommendations

The urgency of curbing the rise of artificial intelligence in public space surveillance

China's role in the proliferation of public space surveillance throughout Africa is unquestionable. Although they are by no means the only country selling video surveillance equipment to certain African regimes (with total disregard of these regimes' human rights track record) their drive to monetise AI surveillance is unprecedented. China's Next Generation Artificial Intelligence Plan (NGAIP), a part of China's Made in China 2025 strategy, aims to make China the world's leading power in AI research by 2030. AI surveillance technology is very likely destined for African countries signed up to the Belt and Road Initiative.

The four countries surveyed in this research, namely Angola, Botswana, South Africa and Zimbabwe, have very different histories, governance systems, and levels of infrastructure development. Their public surveillance infrastructure also has not been expanded at the same rate. However, every one of these countries are headed in the same direction: AI-powered surveillance, with features like facial recognition and a variety of other video analytics.

These analytics make it possible for governments to track and trace individuals like never before. Facial recognition technology is moving to a point where it can expressly be applied to discriminate on the basis of race, age, gender and even one's emotional state. For all of these analytic types, the extent to which they can be used to control human behaviour are only limited by the imagination – as is becoming clear with their numerous uses in China.

Apart from being on the receiving end of these technologies, African citizens will also serve as guinea pigs for testing this equipment, and their data is being and will be collected without their consent, and utilised to further develop AI technology. This technology will again be sold back to the African countries, at the expense of its citizens' privacy and control of their personal data.

Added to this, is the fact that manufacturers are not at all reluctant to sell this equipment to regimes with poor human rights track records. Huawei has openly stated that it is only concerned with the laws of a country, and with obeying those laws. The company, a major driver of AI surveillance in Africa, therefore does not concern itself with the effects of its technology on African citizens, or how governments use it, as long as it does not contravene any local laws. Thus, the company effectively strives to keep governments happy, even if it is at the expense of citizens' wellbeing, and regardless of that government's stance on human rights. For Huawei, human rights are not even a remote consideration when it comes to selling their surveillance technology.

Citizens, civic group, journalists, and academics in countries surveyed in this review need to seriously take stock of the future implications of the current rate of AI video surveillance proliferation on their human rights, and plan action accordingly.

Citizens should insist on being consulted before the installation of surveillance cameras – not after their installation. Governments and businesses take the approach of "It's easier to ask for forgiveness than permission". However, citizens need to insist on their fundamental right to privacy, which includes the right to *not be under camera surveillance at all*, and to not have their personal images captured. Citizens need to take the stance that, even if the cameras are placed in a public space, the images they generate of an individual constitute that individual's personal information. All the metadata that accompanies the image – such as the date, time and location stamps of the image – also belong to that individual. It is up to civil society to not only fight for control of personal information by individuals to whom it rightfully belongs, but to also stop the generation of that information in the first instance.

As was illustrated in the case of Zimbabwe, governments argue that the benefit of surveillance cameras (to deter crime) outweighs privacy concerns. However, these claims are very seldom based on scientific evidence. Thus privacy is traded for an assumption of safety. Civil society needs to insist that governments prove, with factual, scientific evidence, that their collection of personal data (in the form of video surveillance images) meets the criteria of being necessary and proportionate. Unless this burden of proof is placed on the government, the debate around privacy vs security will circle endlessly, while camera surveillance networks continue to spread.

Recommendations for further research

Democracy doesn't stop surveillance

The level of democratic freedoms enjoyed by a country's citizens will not necessarily lead to greater public calls for privacy in terms of public space surveillance. In authoritarian countries like Angola and Zimbabwe, for instance, governments are implementing public digital surveillance without public consultation. In South Africa, supposedly a democracy, the corporate sector and private civic organisations are leading the charge to expand public surveillance networks, with seemingly little interference or protest from government or civil society. Even in a country like Botswana, where civil society organisations and parliamentarians speak freely in public about the perils of mass surveillance, the government has commenced the establishment of city-wide surveillance networks, seemingly without resistance from citizens.

There is room for future research to explore this lack of citizens' response to the threat surveillance cameras pose to their personal privacy.

Safety and security before privacy

In all countries, safety was used as a major motivation for installing large-scale surveillance networks. Addressing crime, road safety, and increasing the response-time of emergency services were major motivators for public surveillance. Nowhere did governments cite research evidence that visual surveillance would in fact contribute to community safety. The unproven assumption that citizens should sacrifice privacy in the name of safety appears to be generally accepted by citizens and governments alike.

Future studies should question this assumption: there is ample academic research available on the topic illustrating that the jury is still out on the actual effectiveness of video surveillance on impacting crime and improving citizen safety, yet this is seldom brought to the attention of those parties purchasing these networks.

Big data and video surveillance

The push towards integrating big data with public video surveillance can be seen clearly in the case of Angola, where national identification systems are being linked to a national surveillance camera network.

Further research should take a hard look at the tendency of distributors of surveillance network equipment to market all-inclusive data services to governments. Such systems have the potential to strictly control every aspect of a citizen's information, and therefore their lives.

China

This study noted trends similar to those mentioned by other observers in terms of China's sales of video surveillance equipment to African governments. Huawei, ZTE and Hikvision all featured prominently in countries studied during this research, although they were not the only equipment providers, and China was not the only country found to contribute to surveillance equipment infrastructure.

However, China's long-standing economic relationships with many African countries, its investment in local African ICT infrastructure, and its ability to provide soft loans and much cheaper network (and surveillance) equipment, has put it in a position to lead the proliferation of video surveillance in Africa.

Researchers should further explore the role that China plays in increased surveillance in authoritarian regimes. Sales of Huawei, ZTE and Hikvision equipment in particular could provide an indication of the growth and capabilities of such networks.

Questionable actions of intelligence and security forces

In every country, state intelligence agencies and security forces stand accused of extra-legal activities, ranging from corruption to gross human rights violations. In the case of Angola, indications are that security forces could have access to public surveillance network data during the normal course of their business. In other countries, just who has access to the network is less clear.

Researchers should look at just who has access to the data collected through mass surveillance networks, and how these agencies will use such data – if at all. Further studies can also explore whether or not countries have protocols in place to manage legitimate data access, and to which extent misuse of data by authorities can be policed and addressed (if at all).

Legal protection

None of the countries in this study have adequate legal protection mechanisms in place to protect the privacy of those subject to public space video surveillance.

This study only briefly glanced at current legislation. Further studies should take a more detailed look at existing laws and their practical implementation (or lack thereof).

The integration of national public surveillance networks

Not all networks are integrated. In Angola and Botswana, for instance, there is a move towards national public video surveillance networks in which all data is connected to a main control centre. In South Africa, the surveillance networks are far more fractured. Cape Town municipal authorities' surveillance networks are separate from residentially funded licence plate recognition networks, for instance. Johannesburg's new fibre-based surveillance cameras are not linked to the Cape Town system, and it doesn't seem likely that they will be in future.

Research into this area should consider to what extent data from surveillance systems is centralised, who controls the data, and who accesses it. This will differ depending on the degree of system integration. Whereas a single system with national coverage and a central control hub would fit the picture of a dystopian surveillance society, fragmented systems controlled by different parties (both public and private) pose their own dangers: these include data leaks during data sharing processes, or a lack of a legitimate central authority ultimately taking responsibility for data security. Future research should explore the different pitfalls of these systems when it comes to data security.

The latest, state-of-the-art surveillance tech

There seems to be a tendency to install the latest and most sophisticated equipment in surveillance networks, if government reports and corporate messages are to be believed. However, very little information about the actual effectiveness of these systems (including data analytics software like facial recognition technology that can be applied to video feed) is known to the public.

Future research should question authorities' expenditure on this technology and look at whether or not it really works, and, if so, to what extent its use further corrodes individual privacy.

6 References

Ace, E. 2018. Hikvision DeepInMind tested terribly. *IPVM*, 15 February 2018. Accessed on 15 October 2019 at: https://ipvm.com/reports/deepinmind-test

Adepoju, P. 2019. Huawei Francistown Botswana earmarked for next Huawei CCTV rollout. *ITWeb Africa,* 2 September 2019. Accessed on 19 September 2019 at: www.itwebafrica.com/unified-communications/643-botswana/246355-francistown-botswana-earmarked-for-next-huawei-cctv-rollout

Agência Angola Press. 2019. Conselho-Ministros-aprecia-Lei-video-vigilancia. 22 April 2019. Accessed on 19 September 2019 at: https://www.angop.ao/angola/pt_pt/noticias/politica/2019/4/22/Conselho-Ministros-aprecia-Lei-video-vigilancia,80039c38-ebf0-43ff-9391-157c40029a2e.html

Agência Angola Press. 2017. Interior minister highlights change in public security paradigm. 16 August 2017. Accessed on 19 September 2019 at: https://www.angop.ao/angola/en_us/noticias/ politica/2017/7/33/Interior-minister-highlights-change-public-security-paradigm,9eabc0bf-2d89-4bee- 95bb-9649fafb613b.html

American Civil Liberties Union (ACLU). 2019. You are being tracked: How licence plate readers are being used to record Americans' movements, New York, July 2013. Accessed 19 September 2019 at: https://www.aclu.org/other/you-are-being-tracked-how-licence-plate-readers-are-being-used-record-americans-movements

Angolan Ministry of the Interior. 2019. Minint wants to count on Huawei to supply technological means to fight crime. 29 November 2019. Accessed on 20 March 2020 at: www.minint.gov.ao/vernoticia.aspx?id=47622

ANPR International. n.d. The history of ANPR. Accessed on 15 October 2019 at: http://www.anpr-international.com/history-of-anpr/

Arnold, B. & Harris, O. 2013. Number plate recognition: The technology behind the rhetoric. *The Conversation,* 1 September 2013. Accessed on 1 March 2020 at: http://theconversation.com/number-plate-recognition-the-technology-behind-the-rhetoric-17572

Axis Communications. 2015. *Safe Cities Case Study Book: A smart city is a city where people feel safe.* Accessed on 19 September 2019 at: https://www.axis.com/files/brochure/bc_casestudies_safecities_en_1506_lo.pdf

Beijing Percent Information Technology Co., Ltd. 2018. Company Profile. Accessed on 15 September 2019 at: https://en.percent.cn/Company

Bhoroma, Victor. 2018. Chinese deals: good or bad for Zim? *The Zimbabwe Independent,* 9 November 2018. Accessed on 20 March 2020 at: https://www.theindependent.co.zw/2018/11/09/chinese-deals-good-or-bad-for-zim/

Big Brother Watch. 2018. Face Off - The lawless growth of facial recognition in UK policing. May 2018. Accessed on 19 September 2019 at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

BIS Research. 2019. Increasing Penetration of IP Cameras Driving the Global Video Surveillance Market. 20 February 2019. Accessed on 1 March 2020 at: https://blog.marketresearch.com/increasing-penetration- of-ip-cameras-driving-the-global-video-surveillance-market

Botlhomilwe, Z., Sebudubudu, D., & Maripe, B. 2011. Limited freedom and intolerance in Botswana. *Journal of Contemporary African Studies*, 29: 331-348. Accessed on 15 September 2019 at: DOI:10.1080/02589001.2011.581501

Botswana Fibre Networks. 2017. Annual Report 2017. Accessed on 15 September 2019 at: https://www.bofinet.co.bw/images/2018/Report/BOFINET_Annual_Report_2017_11Dec.pdf

Botswana Fibre Networks. 2018. Annual Report 2018. Accessed on 15 September 2019 at: https://www.bofinet.co.bw/images/2019/Documents/BOFINET_Annual_Report_2018_Web.pdf.

Breuer, J. 2017. *Two Belts, One Road? The role of Africa in China's Belt and Road initiative*. July 2017. Accessed on 15 September 2019 at: https://www.eu-china.net/uploads/tx_news/Blickwechsel_OBOR-Afrika_Maerz2018_03.pdf.

Brownlee, J. 2019. A Gentle Introduction to Object Recognition With Deep Learning. Machine Learning Mastery. 22 May 2019. Accessed on 17 March 2020 at https://machinelearningmastery.com/object-recognition-with-deep-learning/

Bulawayo News. 24 March 2017. Zimbabwe Police install CCTV cameras, drones, ahead of NERA demonstration. Accessed on 12 February 2020 at: https://bulawayo24.com/index-id-news-sc-national-byo-106730.html.

Business Insider SA. 15 February 2019. Accessed on 1 October 2019 at: https://www.businessinsider.co.za/vumatel-launches-vumacam-cctv-security-cameras-around-johannesburg-suburbs-2019-2

Businesstech. 2018. Joburg is getting new CCTV surveillance cameras*.* 23 July 2018. Accessed on 15 September 2019 at: https://businesstech.co.za/news/business/260151/joburg-is-getting-new-cctv-surveillance-cameras/

Businesstech. 2019. South Africa's worst hijacking hotspots. 19 August 2019. Accessed on 15 September 2019 at: https://businesstech.co.za/news/motoring/335463/south-africas-worst-hijacking-hotspots/

Caldeira, A. 2018. Câmaras de vídeo vigilância em Maputo e Matola são para distrair do comando de intercepção de informação de Moçambique. *Verdade*, 4 April 2018. Accessed on 20 September 2019 at: http://www.verdade.co.mz/tema-de-fundo/35-themadefundo/65381-camaras-de-video-vigilancia-em-maputo-e-matola-sao-para-distrair-do-comando-de-intercepcao-d

Carte Blanche. 2019. Vumacam – Big Brother or Guardian Angel? *M-Net*. YouTube video. 26 March 2019. Accessed on 15 September 2019 at: https://www.youtube.com/watch?v=fynagsROnRM&t=6s

CEIEC (Guangdong) Fullgain Industrial & Trading Co., Ltd. 2017. Commencement Ceremony of CISP of Angolan National Public Security. 18 October 2017. Accessed on 15 September 2019 at: http://www.fullgain.com/en/qydt/info_46.aspx?itemid=119

Chen, A.Y. 2009. China's role in infrastructure development in Botswana. *South African Institute of International Affairs (SAIIA)*. September 2009. Accessed on 15 September 2019 at: https://saiia.org.za/research/chinas-role-in-infrastructure-development-in-botswana/

Chen, W. 2018. Twenty years on, China-SA relations embrace a new chapter. *Business Day,* 25 September 2018. Accessed on 15 September 2019 at: https://www.businesslive.co.za/bd/world/asia/2018-09-25-twenty-years-on-china-sa-relations-embrace-a-new-chapter/

Chikono, M. 2019*.* Econet in massive network overhaul. *The Zimbabwe Independent,* 12 April 2019. Accessed on 20 March 2020 at: https://www.theindependent.co.zw/2019/04/12/econet-in-massive-network-overhaul/

China Daily. 2016. Chinese President lauds Chinese technology saving lives in Ecuador. 21 November 2016. Accessed on 15 September 2019 at: http://www.chinadaily.com.cn/beijing/2016-11/21/content_27464184.htm

China Global Television Network. 2018. China, Botswana agree to promote ties to higher level. 31 August 2018. Accessed on 15 September 2019 at: https://news.cgtn.com/news/3d3d514f3363444f79457a6333566d54/share_p.html

Churu, J. 2016. Huawei's Botswana footprint 'commendable'- MD. *Biztech Africa*, 22 June 2016. Accessed on 15 September 2019 at: https://www.biztechafrica.com/article/huaweis-botswana-footprint-commendable-md/11461/

City of Cape Town. 2012. City of Cape Town Metropolitan Police Department Master Plan for an Integrated Closed Circuit Television System. January 2012. Accessed on 25 September 2019 at: https://www.khayelitshacommission.org.za/bundles/category/29-10-city-of-cape-town-documents-coi.html?download=554:cctv%20master%20plan%20ammended%202012jan

City of Cape Town. 2017. Mitchells Plain CCTV Masterplan Presentation. 18 May 2017. Accessed on 25 September 2019 at: https://www.capetown.gov.za/councilonline/_layouts/OpenDocument/OpenDocument.aspx?DocumentId=a3918acf-6910-487a-acb9%20fdd2fe1f6399.

Civicus. 2018. Human rights defender barred from entering Botswana. *Civicus*, 1 August 2018. Accessed on 25 September 2019 at: https://monitor.civicus.org/newsfeed/2018/08/01/prominent-human-rights-lawyer-declared-person-non-grata/

Clarke, J. 2014. *E-tolls: From good concept to embarrassing disaster.* Mail and Guardian. 28 January 2014. Accessed on 25 September 2019 at: https://mg.co.za/article/2014-01-28-how-e-tolls-turned-from-being-a-good-concept-into-a-flop

Confidential research interview. October 2018.

Constantia Ratepayers' and Residents' Association. 2016. *Automatic Number Plate Recognition Tech at Last.* Accessed on 25 September 2019 at: crra.co.za/automatic-number-plate-recognition/

Constitution of the Republic of Botswana. 1966. Accessed on 25 September 2019 at: https://www.parliament.gov.bw/images/constitution.pdf

Constitution of the Republic of South Africa. 1996. Accessed on 25 September 2019 at: http://www.justice.gov.za/legislation/constitution/SAConstitution-web-eng.pdf

Cook, C.M., Howard, J.J., Sirotin, Y.B., Tipton J.L., & Vemury, A.R. 2019. Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 1(1): 32-41. Accessed on 5 March 2020 at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8636231&isnumber=8444126

Cook, S. 2019. China's cyber superpower strategy: Implementations, internet freedom implications and US responses. Accessed on 7 May 2020 at: https://freedomhouse.org/article/chinas-cyber-superpower-strategy-implementation-internet-freedom-implications-and-us

Cox, Joseph. 2019. *This Company Built a Private Surveillance Network. We Tracked Someone With It.* Motherboard. 17 September 2019.

Accessed at https://www.vice.com/en_us/article/ne879z/i-tracked-someone-with-license-plate-readers-drn on 14 March 2020.

Czernowalow, M. 2005. Inner city surveillance a success. *ITWeb*. 27 Jun 2005. Accessed on 25 September 2019 at: https://www.itweb.co.za/content/DZQ587V6mLp7zXy2

Dahir, A.L. 2019a. The African Union is doubling down on deepening its relationship with Huawei. *Quartz Africa*. 31 May 2019. Accessed on 25 September 2019 at: https://qz.com/africa/1632111/huawei-african-union-sign-deal-to-boost-5g-ai-cloud-computing/

Dahir, A.L. 2019b. These are the African countries not signed to China's Belt and Road project. *Quartz Africa*, 30 September 2019. Accessed on 17 March 2020 at: https://qz.com/africa/1718826/the-african-countries-not-signed-to-chinas-belt-and-road-plan/

Daniel, L. 2018. SANRAL says all e-tolls defaulters will be summoned to court*. The South African,* 18 March 2019. Accessed on 25 September 2019 at: https://www.thesouthafrican.com/news/etolls-gauteng-pay-court-action-sanral/

Data Protection Act of Botswana, 2018. Accessed on 25 September 2019 at: https://www.bocra.org.bw/data-protection-act

Defence Web. 2009. Johannesburg adjudges CCTV project a success. 11 December 2009. Accessed on 25 September 2019 at: https://www.defenceweb.co.za/security/civil-security/johannesburg-adjudges-cctv- project-a-success/

Demonstration attended by researcher. 2014.

Dhlela, D. 2020. Military-driven surveillance endangers democracy. *NewsDay.* Accessed on: 20 March 2020 at: https://www.newsday.co.zw/2020/03/military-surveillance-could-endanger-democracy/

Dube, M. 2019. Botswana opposition leader questions election results, wants to challenge them court*. The Star,* 1 November 2019. Accessed on 25 November 2019 at: https://www.iol.co.za/the-star/news/botswana-opposition-leader-questions-election-results-wants-to-challenge-them-court-36432492

Duval, M. 2016. Seeing the big picture. *Media 24,* 19 October 2016. Accessed on 25 September 2019 at: https://www.netwerk24.com/ZA/Tygerburger/Nuus/seeing-the-big-picture-20161018-2

Edgemead News. 2018*. Bothasig & Edgemead LPR Project*. October 2018. Accessed on 25 September 2019 at: https://edgemeadnews.co.za/lpr/

Edjo, M. 2017*.* Huawei renforce sa collaboration avec Madagascar pour l'aider à devenir un hub TIC. *Agence Ecofin*, 31 March 2017. Accessed on 25 September 2019 at: https://www.agenceecofin.com/investissement/3103-46223-huawei-renforce-sa-collaboration-avec-madagascar-pour-l-aider-a-devenir-un-hub-tic

Embassy of the Republic of Botswana. n.d. Accessed on 25 September 2019 at: http://www.botswanaembassy.org/page/history-of-botswana

Executive Research Associates. 2009. China in Africa: A strategic overview*.* Accessed on 25 September 2019 at: https://www.ide.go.jp/library/English/Data/Africa_file/Manualreport/pdf/china_all.pdf.

Feldstein, S. 2019. *The Global Expansion of A.I. Surveillance*. Carnegie Endowment for International Peace. 17 September 2019. Accessed on 5 September 2019 at: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Finance24. 2013. E-tolls timeline: How it unfolded. 2 December 2013. Accessed on 25 September 2019 at: https://www.fin24.com/Economy/E-tolls-timeline-How-it-unfolded-20131202

Forum for Economic and Trade Co-operation between China and Portuguese-speaking Countries (Macao). 2017. Angola spends on Chinese technology to manage national records*.* 18 January 2017. Accessed on 5 September 2019 at: http://www.forumchinaplp.org.mo/angola-spends-us243-mln-on-chinese-technology-to-manage-national-records/

Freedom House. 2019. *Freedom in the World Report 2019*. Accessed on 5 September 2019 at: https://freedomhouse.org/report/freedom-world/2019/angola

Gierlack, K. Williams, S. LaTourrette, T. Anderson, J.M., Mayer, L.A., & Zmud, J. 2014. *Licence Plate Readers for Law Enforcement: Opportunities and Obstacles.* Santa Monica, CA: Rand Corporation.

Goodwood Patrols. 2019. Improve the safety in your neighbourhood with licence plate recognition cameras. Accessed on 25 September 2019 at: https://goodwoodpatrols.co.za/lpr-project/

Government of the Republic of South Africa. 2019. *History.* Accessed on 25 September 2019 at: https://www.gov.za/about-sa/history

Gough, N. 2016. Snooping in the bathroom to assess credit risk in China. The New York Times. 10 October 2016. Accessible on:https://www.nytimes.com/2016/10/11/business/international/snooping-in-the-bathroom-to-assess- credit-risk-in-china.html?searchResultPosition=4. Accessed on 12 March 2020.

GP/OK City Improvement District. 2018. Safer CID: new cameras installed to accelerate fight against crime. January 2018. Accessed on 25 September 2019 at: gpokcid.co.za/2018/01/safer-cid-new-cameras-installed-accelerate-fight-crime/

Gras, M.L. 2004. The legal regulation of CCTV in Europe. *Surveillance & Society,* 2(2/3): 75-88. Halt Security. 2018. Criminals beware, HALT has eyes on Durbanville with LPR Cameras. Accessed on 25 September 2019 at: https://www.haltsecurity.co.za/lpr-cameras-in-durbanville

Harmon, L. 2020. *Unbiased Surveillance: AI Security Tech That Spots Guns, Not People*. The Observer. 4 February 2020. Accessed on 14 March 2020 at https://observer.com/2020/02/athena-security-surveillance-bias-gun-control/

Hawkins, A. 2018. Beijing's Big Brother Tech Needs African Faces. Foreign Policy. 24 July 2018. Accessed on 14 March 2020 at: https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/

Hikvision. 2015. Sea Point sees two-thirds Crime Drop after Hikvision Cameras Deployed. 8 May 2015. Accessed on 25 September 2019 at: https://www.hikvision.com/cz/Press/SuccessStories/Transportation/305529081636891

Hon, T., Jansson, J., Shelton, G., Haifang, L., Burke, C., & Kiala, C. 2010. *Evaluating China's FOCAC commitments to Africa and mapping the way ahead.* Stellenbosch: Centre for Chinese Studies, University of Stellenbosch. Accessed on 5 September 2019 at: http://www.ccs.org.za/wp-content/uploads/2010/03/ENGLISH-Evaluating-Chinas-FOCAC-commitments-to-Africa-2010.pdf

Honovich, J. & Rollet, C. 2019. Critiquing Carnegie's AI Surveillance Paper. *IPVM,* 25 September 2019. Accessed on 30 September 2019 at: https://ipvm.com/reports/carnegie

Huawei. 2019a. Huawei Marine WACS Upgrade II Successfully Completed. 1 February 2019. Accessed on 25 September 2019 at: https://www.huawei.com/en/press-events/news/2019/2/huawei-marine-wacs-upgrade

Huawei. 2019b. Rain and Huawei Jointly Announce the 5G Provisioning to Selected Users in South Africa. 19 September 2019. Accessed on 25 September 2019 at: https://www.huawei.com/za/press-events/news/za/2019/rain-huawei-jointly-announce-the-provisioning-to-selected-users-in-south-africa

Huawei. n.d. Huawei Helps The City of Ekurhuleni Grow into a South African Smart City Pioneer. Accessed on 20 March 2020 at: https://e.huawei.com/topic/leading-new-ict-en/ekurhuleni-smartcity-case.html

Human Rights Watch. 2019. *Human Rights Watch World Report 2019*. Accessed on 5 September 2019 at: https://www.hrw.org/world-report/2019/country-chapters/angola

Independent Online. 2019. City of Cape Town to add dozens of CCTV cameras to surveillance network. 11 April 2019. Accessed on 25 September 2019 at: https://www.iol.co.za/capeargus/news/city-of-cape- town-to-add-dozens-of-cctv-cameras-to-surveillance-network-20941663

Independent Online. 2019. Zimbabwe High Court court rules internet shutdown illegal. 21 January 2019. Accessed on 20 March 2020 at: https://www.iol.co.za/news/africa/zimbabwe-high-court-court-rules-internet-shutdown-illegal-18898174

Industry source interview, October 2018.

Intelligent Surveillance and Detection Systems (Pty) Ltd (ISDS). 2013. iSentry Ultra Smart Video Analytics. YouTube video. 2 April 2013. Accessed on 1 March 2020 at: https://www.youtube.com/watch?v=RoI-oeBvM0c

Intelligent Transport Society South Africa. 2013. City CCTV tender in dispute*.* 13 September 2008. Accessed on 25 September 2019 at: itssa.org/city-cctv-tender-in-dispute/

Interview with representative of Cape Town LPR User Group. October 2018.

IPVM. 2019. *Security camera basics 2019*. Accessed 19 September 2019 at: https://ipvm.com/book/book

IPVM. 2020. Video Surveillance Cameras State Of The Market. IPVM. 3 January 2020. Accessed at https://ipvm.com/reports/cameras-2020 on 14 March 2020.

IT News Africa. 2018. Smart cities in Africa start with smart broadband infrastructure. 11 July 2018. Accessed on 25 September 2019 at: https://www.itnewsafrica.com/2018/07/smart-cities-in-africa-start-with-smart-broadband-infrastructure/

iTrackLPR. 2014. Growing Footprint in Cape Town. 4 March 2014. Accessed on 25 September 2019 at: www.itracklpr.com/?q=node/11

iTrackLPR. n.d. Overview. Accessed on 25 September 2019 at: www.itracklpr.com/?q=documentation/overview

Jefferis, K. 2009. The role of TNCs in the extractive industry of Botswana. *Transnational Corporations*, 18(1): 62-92. Accessed on 25 September 2019 at: https://unctad.org/en/docs/diaeiia20097a3_en.pdf

Jing, J. 2019. Review: China helps South Africa's telecommunications industry leapfrog development. *Xinhua News Agency,* 16 April 2019. Accessed on 25 September 2019 at: www.gov.cn/xinwen/2019-04/16/content_5383271.htm

Johannesburg Metropolitan Police Department. 2015. Businesses returning to safer Joburg CBD. 14 August 2015. Accessed on 25 September 2019 at: https://www.news24.com/SouthAfrica/News/Businesses-returning-to-safer-Joburg-CBD-JMPD-20150814

Jornal de Angola. 2019a. Centro Integrado de Segurança Pública*.* 23 February 2019. Accessed on 5 September 2019 at: http://jornaldeangola.sapo.ao/provincias/benguela/centro-integrado-de-seguranca- publica

Jornal de Angola. 2019b. Instaladas 700 câmaras para vigilância da capital. 13 August 2019. Accessed on 5 September 2019 at: jornaldeangola.sapo.ao/sociedade/instaladas-700-camaras-para-vigilancia-da-capital

Karas, B. 2017. *Deep Learning Tutorial for Video Surveillance.* IPVM. 17 October 2017. 5 September 2019 at: https://ipvm.com/reports/deep-learning-tutorial

Kariuki, H. 2019. *Data: An Integral Part of China's New Belt and Road Initiative Strategy in Africa.* Medium. 28 April 2019. Accessed at https://medium.com/@harriet436/chinas-new-belt-and-road-initiative-strategy-in-africa-involves-data-8af96492003f on 17 March 2020.

Kebotse, K. 2019. Crime-monitoring cameras to be installed in Francistown*. Mmegi Online*. 4 June 2019. Accessed on 5 September 2019 at: https://www.mmegi.bw/index.php?aid=81187&dir=2019/june/04

Kilpatrick, R. 2018. Dahua Face Recognition Camera Tested. IPVM. 15 October 2018. Accessed on 19 October 2019 at https://ipvm.com/reports/dahua-face-recognition

Komane, K. 2019. Botswana arrests ex-spy boss. *Mail and Guardian,* 18 January 2019. Accessed on 25 September 2019 at: https://mg.co.za/article/2019-01-18-botswana-arrests-ex-spy-boss

Kwet, M. 2016. Apartheid in the Shadows: the USA, IBM and South Africa's Digital Police State. *CounterPunch,* 3 May 2017. Accessed on 1 September 2019 at: https://www.counterpunch.org/2017/05/03/apartheid-in-the-shadows-the-usa-ibm-and-south-africas-digital-police-state/

Kwet, M. 2020. The Rise of Smart Camera Networks, and Why We Should Ban Them. *The Intercept,* 27 January 2020. Accessed on 12 March 2020 at: https://theintercept.com/2020/01/27/surveillance-cctv- smart-camera-networks/

Larsen, L. 2006. Lights, camera ... less criminal action. *Hi-Tech Security Solutions*. December 2006. Accessed on 25 September 2019 at: https://www.securitysa.com/article.aspx?pklarticleid=4191

Lekgowe, G.R. 2014. The Right to Peaceful Assembly in Botswana: The Constitutionality of the Public Order Act. *University of Botswana Law Journal*, 18: 66-84. Accessed on 25 September 2019 at: https://journals.ub.bw/index.php/ublj/article/view/821

Link, Jordan. 2019. How Huawei could survive Trump. *Washington Post*. June 10, 2019. Accessed on 20 March 2020 at: https://www.washingtonpost.com/politics/2019/06/10/what-do-we-know-about-huaweis-africa-presence/

Liquid Telecom. 2010. Econet subsidiary plans to lower prices with new southern African fibre network. 22 February 2010. Accessed on 20 March 2020 at: https://www.commsupdate.com/articles/2010/02/22/ econet-subsidiary-plans-to-lower-prices-with-new-southern-african-fibre-network/

Loch, P. 2017. Surveillance at: work: the legal issues of using CCTV. Accessible at: https://www.personneltoday.com/hr/surveillance-the-legal-issues-of-cctv-use-at:-work/ Accessed on 14 March 2020.

Ludwig Rausch, S. 2019. The Impact of City Surveillance and Smart Cities. *Security Magazine,* 10 April 2019. Accessed on 25 September 2019 at: https://www.securitymagazine.com/articles/90109-the-impact-of-surveillance-smart-cities

Mabaya, N. & Motsi, M. 2020 Zimbabwe splurges US$20 million on Huawei mass surveillance grid technology. *Spotlight Zimbabwe,* 20 March 2020. Accessed on 27 March 2020 at: spotlight-z.com/news/zimbabwe-splurges-us20-million-huawei-mass-surveillance-grid-technology/

Macauhub. 2017. Angola to have Integrated Public Security Management System*.* 26 June 2017*.* Accessed on 25 September 2019 at: https://macauhub.com.mo/2017/06/26/pt-angola-vai-ter-sistema-integrado-de-gestao-de-seguranca-publica/

MacKinnon, A. 2019. For Africa, Chinese-built Internet is better than no Internet at: all. *Foreign Policy,* 19 March 2019. Accessed on 25 September 2019 at: https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at:-all/

Mail and Guardian. 2011. Hawks bugged reporters' phone*.* 2 October 2011. Accessed on 25 September 2019 at: https://mg.co.za/article/2011-10-02-hawks-bugged-reporters-phone

Massala, G. 2017. Angola will have an Integrated Center for Public Security. *Menosfios,* 16 August 2017. Accessed on 25 September 2019 at: https://www.menosfios.com/en/angola-a-center-integrated-security-public/

Massau, P. 2019. Zimbabwe: Chinese Tech Revolution Comes to Zimbabwe. The Herald. 9 October 2019. Accessed on 30 March 2020 at: https://allafrica.com/stories/201910090185.html.

Mawonde, Abigail. 2018. NetOne, Huawei seal $71m deal. *The Herald,* 3 January 2018. Accessed on 20 March 2020 at: https://www.herald.co.zw/netone-huawei-seal-71m-deal/

Midway Organisation. 26 April 2016. The surveillance control room support. Accessed on 20 September 2019 at: www.mid.org.za/ward-64-control-room-support/

Mmolawa, T. 2019. Francistown gets crime-monitoring cameras. *The Patriot,* 1 August 2019. Accessed on 25 September 2019 at: https://www.thepatriot.co.bw/news/item/7315-f-town-gets-crime-monitoring-cameras.html 32.

Mokwena, N. 2018. MPs okay Data Protection Bill with reservations. *Botswana Guardian,* 3 July 2018. Accessed on 25 September 2019 at: http://www.botswanaguardian.co.bw/news/item/3247-mps-okay-data-protection-bill-with-reservations.html

Moore, W.G. 2019. African countries should stay loyal to China's troubled Huawei – regardless of Trump. *Quartz Africa,* 27 May 2019. Accessed on 25 September 2019 at: https://qz.com/africa/1629078/africa-will-stay-loyal-to-chinas-huawei-regardless-of-trump/

Moubray, C. 2019. Delays in privacy laws are costing South Africans money and security. *The Daily Maverick,* 21 October 2019. Accessed on 25 September 2019 at: https://mail.google.com/mail/u/0/#inbox?compose=DmwnWrRrlZcMCmNwWwGTRFnFhGfnnNkxLWBwTxxlZQXsstFfzCSRGDJskctflNhRLSRMcDZMSDCv

Moyo, A. 2019. Tech makes gains in arresting crime in inner city Joburg. *ITWeb,* 26 July 2019. Accessed on 25 September 2019 at: https://www.itweb.co.za/content/dgp45MaGNGjvX9l8

Moyo, A. 2020. Furore as Zim exempts Huawei from tax obligations. *ITWeb,* 5 February 2020. Accessed on 20 March 2020 at: https://www.itweb.co.za/content/RgeVDqPoxBQMKJN3

Mozur, P. Kessel, J.M., & Chan, M. 2019. Made in China, Exported to the World: The Surveillance State. *The New York Times,* 24 April 2019. Accessed on 25 September 2019 at: https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Mu, M. 2018. Autonomous Region Public Security Department and Huawei signed a "Peaceful Xinjiang Smart Peer" strategic cooperation agreement, *Xinjiang Net News,* 13 May 2018. Accessed on 20 March 2020 at: https://www.sohu.com/a/231424240_118570

Muizenberg Improvement District. 2018. Ward 64 Control Room Support. Accessed on 25 September 2019 at: http://www.mid.org.za/ward-64-control-room-support/

Mzekandaba, S. 2016a. Cape pumps R14m into invisible policing. *ITWeb,* 14 March 2016. Accessed on 25 September 2019 at: https://www.itweb.co.za/content/2JN1gP7OpnAMjL6m

Mzekandaba, S. 2016b. Joburg drives investment in smart policing. *ITWeb,* 5 May 2016. Accessed on 25 September 2019 at: https://www.itweb.co.za/content/KwbrpOMgmpEvDLZn

Nation Master. 2016. Crime Statistics in Zimbabwe. Accessible at: https://www.nationmaster.com/country-info/profiles/Zimbabwe/Crime. Accessed on 12 January 2020.

National Institute of Standards and Technology (NIST). 2019. *Ongoing Face Recognition Vendor Test (FRVT)*. United States Department of Commerce. 5 July 2019. https://www.nist.gov/sites/default/files/documents/2019/07/03/frvt_report_2019_07_03.pdf

National Institute of Standards and Technology (NIST). 2018. *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities.* United States Department of Commerce. 30 November 2018. https://www.nist. gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities

National Law Enforcement and Corrections Technology Center: Small, Rural, Tribal and Border Regional Centre. 2010. *Licence Plate Recognition Systems: Function, performance and considerations for law enforcement agencies.* https://www.justnet.org/pdf/LPR-Report-Lowres.pdf

Nebehay, S. 2018. U.N. says it has credible reports that China holds million Uighurs in secret camps. *Reuters,* 10 August 2018. Accessed on 15 October 2019 at: https://www.reuters.com/article/us-china-rights-un/u-n-says-it-has-credible-reports-that-china-holds-million-uighurs-in-secret-camps-idUSKBN1KV1SU

New Security Learning. 2011. China's mighty telecom footprint in Africa. *The New Security Foundation*. Accessed on 25 September 2019 at: http://www.newsecuritylearning.com/index.php/feature/75-chinas-mighty-telecom-footprint-in-africa

Norman, T.L. 2017. *Effective Physical Security,* 5th edition. Butterworth: Heinemann. Accessed on 4 April 2020 at: https://www.sciencedirect.com/topics/computer-science/video-analytics

Norris, C. 2012. The success of failure. In Ball, L., Haggerty. K.D., & Lyon, D. (eds.) *Routledge Handbook of Surveillance Studies,* 387-410. London: Routledge.

Nyahasha, T. 2019. Court decision was inadequate: Internet may be shut down again*. TechZim,* 14 August 2019 Accessed on 20 March 2020 at: https://www.techzim.co.zw/2019/08/court-decision-was-inadequate-internet-may-be-shut-down-again/

Observatory City Improvement District. 2019. Licence Plate Recognition (LPR) technology working for Observatory. 22 July 2019. Accessed on 25 September 2019 at: https://obsid.org.za/licence-plate-recognition-lpr-technology-working-for-observatory/

Ogundeji, O.A. 2015. Huawei leads new efforts to develop cable infrastructure in Africa. *PCWorld,* 19 March 2015. Accessed on 25 September 2019 at: https://www.pcworld.com/article/2899672/huawei-leads-new-efforts-to-develop-cable-infrastructure-in-africa.html

Oliver, M. 2004. They have your number. *The Guardian,* 29 July 2004 Accessed on 14 March 2020 at: https://www.theguardian.com/world/2004/jul/29/humanrights.markoliver

Omega Group. 2017. Welcome to the Omega group of companies*.* Accessed on 25 September 2019 at: https://www.omegasol.com/

OneTrust Data Guidance. 2018. Accessed on 25 September 2019 at: https://free.dataguidance.com/laws/botswana-data-protection-act-2018/

Orlander, E. 2019a. Q&A: Chinese sales of surveillance technology to African governments is understandably worrisome but in no way exceptional. *The China-Africa Project*. 21 August 2019. Accessed on 5 September 2019 at: https://chinaafricaproject.com/analysis/qa-china-africa-huawei-zambia-uganda-wsj/

Orlander, E. 2019b. China Mobile reportedly in talks to buy one of South Africa's largest mobile operators. *The China-Africa Project*. 9 October 2019. Accessed on 25 October 2019 at: https://chinaafricaproject.com/2019/10/09/china-mobile-reportedly-in-talks-to-buy-one-of-south-africas-largest-mobile-operators

People's Daily. 2018. China-designed big data system aids Angola's intelligent governance. 24 August 2018. Accessed on 25 August2019 at: en.people.cn/n3/2018/0824/c90000-9493984.html

People's Post. 2017. These officers have got eyes on you. 12 December 2017. Accessed on 25 September 2019 at: https://www.news24.com/SouthAfrica/Local/Peoples-Post/these-officers-have-got-eyes-on-you-20171211

People's Post. 2019. Har-Lyn tightens security*.* 5 March 2019. Accessed on 25 September 2019 at: https://www.news24.com/SouthAfrica/Local/Peoples-Post/har-lyn-tightens-security-20190304

Pindula News. 2018. City of Harare to install 2 million traffic cameras. Accessed on 12 December 2019 at: https://news.pindula.co.zw/2018/10/25/the-city-of-harare-to-install-2-million-traffic-cameras-at:-all-intersections/

Pinelands Street Camera Project. 2017. Communication Path: LPR System Users. 20 January 2017. Accessed on 25 September 2019 at: https://www.facebook.com/1462994833950327/posts/communication-path-lpr-system-userslpr-user-group-vehicle-database-is-a-centrall/1787229411526866/

Prior, B. 2019. Huawei's big plans for safer South African cities. *My Broadband,* 4 March 2019. Accessed on 20 March 2020 at: https://mybroadband.co.za/news/industrynews/298112-huaweis-big-plans-for-safer-south-african-cities.html

Pulse. 2018. KT wins order to build optical communication network in Botswana. 30 July 2018. Accessed on 19 September 2019 at: https://pulsenews.co.kr/view.php?year=2018&no=478153

PWP Neighbourhood Watch. 2017. Support the PWP Licence Plate Recognition (LPR) Camera Project. 3 January 2017. Accessed on 19 September 2019 at: https://pwpnw.co.za/2017/01/03/lpr-project-information/

Quartz Africa. 2014. Beijing exporting facial recognition to Africa. Accessed on 4 March 2019 at: https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

Rabkin, F. 2019. SA's suburban camera creep tests privacy. 31 May 2019. Accessed on 19 September 2019 at: https://mg.co.za/article/2019-05-31-00-sas-suburban-camera-creep-tests-privacy

Radio 702. 2018. How to survive a hijacking and outsmart SA burglars. 7 June 2018. Accessed on 17 August 2019 at: http://www.702.co.za/articles/306769/how-to-survive-a-hijacking-and-outsmart-sa-burglars

Rajput, A. 2016. Smart CCTV and the Internet of Things: 2016 trends and Predictions. *IFSEC Global*, 4 February 2016. Accessed on 24 March 2020 at: *https://www.ifsecglobal.com/video-surveillance/smart- cctv-and-the-internet-of-things-2016-trends-and-predications/*

Rakotoniaina, N. 2015. Chinese Huawei turns Nosy Be into "smart city". *Le Eco Austral,* 11 December 2015. Accessed on 19 September 2019 at: http://ecoaustral.com/le-chinois-huawei-transforme-nosy-be-en-smart-city

Ramaphane, R. 2017. Police ropes in Huawei for surveillance project – Botswana. Privacy and Surveillance in Africa. 6 December 2017. Accessed on 19 September 2019 at: https://privacyinafrica.com/2017/12/06/police-ropes-in-huawei-for-surveillance-project

Rangongo, T. 2019*.* These Joburg suburbs are getting 15,000 CCTV cameras*. Business Insider SA,* 15 February 2019. Accessed on 19 August at: https://www.businessinsider.co.za/vumatel-launches-vumacam-cctv-security-cameras-around-johannesburg-suburbs-2019-2

Republic of Botswana. 2017. Press statement: Safer City Project Commences. 14 November 2017. Accessed on 19 September 2019 at: https://www.facebook.com/BotswanaGovernment/posts/safer-city-project-commencesthe-commissioner-of-police-mr-keabetswe-makgophe-and/1498051366944183/

Republic of Botswana. 2018. Press statement: Botswana Police installs cameras to fight crime. 6 September 2018. Accessed on 19 September 2019 at: https://www.facebook.com/BotswanaGovernment/posts/botswana-police-installs-cameras-to-fight-crimebotswana-police-service-bps-has-r/1836720386410611/

República de Angola Tribunal de Contas, n.d. Resolução n.o64/FP/17. Accessed on 19 September 2019 at https://www.tcontas.ao/assets/uploads/pdf/ c2a3e81976d0fe67cead9093af6240d7.PDF

Researcher's correspondence with the City of Cape Town. October 2018.

Revell, T. 2016. Concerns as face recognition tech used to 'identify' criminals. *New Scientist*, 1 December 2016. Accessed on 19 September 2019 at: https://www.newscientist.com/article/2114900-concerns-as-face-recognition-tech-used-to-identify-criminals/

Rhodes, B and Rollet, R. 2019. Facial Recognition Systems Fail Simple Liveness Detection Test. IPVM. 17 May 2019. Accessed on 19 October 2019 at https://ipvm.com/reports/live-detect

Roberts, D.J. & Casanova, M. 2012. *Automated Licence Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement.* U.S. Department of Justice, National Institute of Justice. Accessed on 19 September 2019 at: https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf.

Roberts, J.J. 2019. The Business of Your Face: While you weren't looking, tech companies helped themselves to your photos to power a facial recognition boom. Here's how. *Fortune Magazine,* 27 March 2019. Accessed on 25 March 2020 at: https://fortune.com/longform/facial-recognition/.

Rollet, C. 2019a. Facial Recognition Providers Review (Secutech). IPVM. 9 May 2019. Accessed on 14 March 2020 at https://ipvm.com/reports/secutech-day-2-report

Rollet, C. 2019b. *Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up.* IPVM. 11 November 2019. Accessed on 14 March 2020 at https://ipvm.com/reports/hikvision-uyghur

Ruhanya, P. 2018. Militarisation of state institutions and the November military coup. Accessed on 24 January 2020 at: www.theindependent.co.zw-of-state-institutions-and-the-november-military-coup

Ryoo, M.S. 2011. Human Activity Prediction: Early Recognition of Ongoing Activities from Streaming Videos Electronics and Telecommunications Research Institute, Daejeon, Korea. IEEE International Conference on Computer Vision (ICCV), Barcelona, Spain, November 2011. Accessed on 14 March 2020 at http://cvrc.ece.utexas.edu/mryoo/papers/iccv11_prediction_ryoo.pdf

Samuels, S. 2014. Gantry alarm fixed but residents want answers. *Sandton Chronicle,* 22 August 2014. https://sandtonchronicle.co.za/100333/gantry-alarmed-fixed-but-residents-want-answers/

Sanger, C.W. & Bradley, K. 2020. *Zimbabwe.* Encyclopædia Britannica Website. Encyclopædia Britannica. 8 January 2020. Accessed on 10 March 2020 at: https://www.britannica.com/place/Zimbabwe.

Science and Technology Committee. 2019. Oral Evidence: UK Telecommunications Infrastructure Inquiry. 10 June 2019. House of Commons, United Kingdom Parliament. Accessed on 14 March 2020 at https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2017/uk-telecommunications-infrastructure-17-19/publications/

Segaetsho, T. 2018. *China, Botswana celebrates enduring ties*. China Daily Africa. 3 August 2018. Accessed on 19 September 2019 at: africa.chinadaily.com.cn/weekly/2018-08/03/content_36699046.htm

Seldon, A. 2015. Retail Risk: Integrated Solutions, Security Services & Risk Management, Conferences & Events*. Hi-Tech Security Solutions,* October 2015. Accessed on 19 September 2019 at: https://www.securitysa.com/regular.aspx?pklregularid=4981

Sena, C. 2018. Province wins MININT Integrated Public Security Center. *TV Livre Angola.* 25 October 2018. Accessed on 19 September 2019 at: https://tvlivreangola.org/provincia-ganha-centro-integrado-de-seguranca-publica-do-minint/

Setswalo, U. 2015. Huawei building a better connected Botswana. *Mmegi Online,* 24 April 2015. Accessed on 19 September 2019 at: www.mmegi.bw/index.php?aid=50743&dir=2015/april/24

Shepard, S. 2018. New surveillance tool: Gait recognition. *Security Today,* Nov 12, 2018. Accessed on 14 March 2020 at: https://securitytoday.com/articles/2018/11/12/new-surveillance-tool-gait-recognition.aspx

Sherman, J. 2019. What's the deal with Huawei and a hack at: African Union headquarters? *Medium,* 31 May 2019. Accessed on 19 September 2019 at: https://medium.com/dukeuniversity/whats-the-deal-with-huawei-and-a-hack-at:-african-union-headquarters-1e454c1f31a2

Simonite, T. 2019. The best algorithms struggle to recognize black faces equally. *Wired*, 22 July 2019. Accessed on 19 September 2019 at: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

Slabbert, A. 2017. Joburg CCTV crime fighting cameras unmanned. *Moneyweb,* 1 September 2017. Accessed on 19 September 2019 at: https://www.moneyweb.co.za/news/south-africa/tender-intervention-sets-back-safety-in-joburg/

Smith, David. 2019. Zimbabwe's Intellectual Despot: How Mugabe became Africa's fallen angel. *The Guardian,* 6 September 2019. Accessed on 20 March 2020 at: https://www.theguardian.com/world/2019/sep/06/zimbabwes-intellectual-despot-how-mugabe-became-africas-fallen-angel

Snow, J. 2018. Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots. *American Civil Liberties Union,* 26 July 2018. Accessed on 19 September 2019 at: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Solomon, S. 2019. After Allegations of Spying, African Union Renews Huawei Alliance. *Voice of America,* 7 June 2019. Accessed on 19 September 2019 at: https://www.voanews.com/africa/after-allegations-spying-african-union-renews-huawei-alliance

South African History Online. 2019. *The Drafting and Acceptance of the Constitution.* Accessed on 19 September 2019 at: https://www.sahistory.org.za/article/drafting-and-acceptance-constitution

South African Police Service. *2018/2019 Annual Police Crime Statistics*. Accessed on 19 September 2019 at: https://www.saps.gov.za/services/crimestats.php

Southern African Development Community. 2019. About page. Accessed on 19 September 2019 at: https://www.sadc.int/about-sadc/

Stanley, J. 2019. The dawn of robot surveillance: AI, video analytics, and privacy. *American Civil Liberties Union,* 11 June 2019. Accessed on 17 March 2020 at: https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf

Sunday Standard. 2019. Botswana Police Service a Cesspool of Corruption. 15 July 2019. Accessed on 19 September 2019 at: http://www.sundaystandard.info/botswana-police-service-cesspool-corruption-%E2%80%93-report

Swart, H. 2018a. Activist murder reveals Joburg street cameras are "turned off". *Mail & Guardian,* 10 May 2018. Accessed on 19 September 2019 at: https://mg.co.za/article/2018-05-10-smile-you-may-not-be-on-camera

Swart, H. 2018b. Joburg's new hi-tech surveillance cameras: A threat to minorities that could see the law targeting thousands of innocents. *Daily Maverick*, 28 September 2018. Accessed on 1 October 2019 at: https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/

Swart, H. 2018c. Controlling Cape Town – the real costs of CCTV cameras, and what you need to know. *Daily Maverick,* 5 October 2018. Accessed on 1 March 2020 at: https://www.dailymaverick.co.za/ article/2018-10-05-controlling-cape-town-the-real-costs-of-cctv-cameras-and-what-you-need-to-know/

Swart, H. 2019a. Intimidation, interception and break-ins: SA security forces and the threat of accountability. *Daily Maverick*, 15 March 2019. Accessed on 19 September 2019 at: https://www.dailymaverick.co.za/article/2019-03-15-intimidation-interception-and-break-ins-sa-security-forces-and-the-threat-of-accountability/

Swart, H. 2019b. Visual surveillance and weak cybersecurity (part 1): When cameras get dangerous. *Daily Maverick*, 13 June 2019. Accessed on 19 September 2019 at: https://www.dailymaverick.co.za/article/2019-06-13-visual-surveillance-and-weak-cyber-security-part-one-when-cameras-get-dangerous/

Technology Zimbabwe. 2015. Econet secures $500 million loan facility from the Chinese government. 4 December 2015. Accessed on 20 March 2020 at: https://myzol.co.zw/articles/291/econet-secures-500-million-loan-facility-from-the-chinese-government

TechQoon. 2019. Angola's National Assembly approves surveillance cameras. August 2019. Accessed on 19 September 2019 at: https://techqoon.net/2019/08/14/angolas-national-assembly-approves-surveillance-cameras-bill/

Techzim. 2019. Econet denies selling people's private data. Accessed on 12 September 2019 at: https://www.techzim.co.zw/2018/07/econet-denies-selling-customers-data-to-3rd-parties-refutes-zecs-allegations-so-who-sold-data-to-zanu-pf/

Teleste. 2011. Securing Cape Town. *Hi-Tech Security Solutions,* April 2011. Accessed on 19 September 2019 at: https://www.securitysa.com/regular.aspx?pklregularid=4981

Teleste. 2013. Case study: Securing the safety of people in South Africa*. Security Newdesk,* 12 December 2013. Accessed on 19 September 2019 at: https://securitynewsdesk.com/author/teleste/

Tendi, B.M. 2020. The motivations and dynamics of Zimbabwe's 2017 military coup. *African Affairs,* 119(474): 39-67.

The Guardian. 2018. The Belt and Road Initiative. Accessed on 12 September 2019 at: https://www.theguardian.com/cities/ng-interactive/2018/jul/30/what-china-belt-road-initiative-silk-road-explainer.

The Business Live. 15 May 2019. EU recommends more sanctions on Zimbabwe. Accessed on 2 May 2019 at: https://www.businesslive.co.za/bd/world/africa/2019-02-15-eu-recommends-more-sanctions-against-zimbabwe/.

The China Institute at the University of Alberta. 2019. Examining Huawei's Growth and Global Reach: Key Implications, Issues and the Canadian Connection. Occasional paper series, 5(4). August 2019. University of Alberta. Accessed on 19 September 2019 at: https://cloudfront.ualberta.ca/-/media/china/media-gallery/research/occasional-papers/2019examininghuaweisgrowthandglobalreach.pdf

The Economist. 2007. Africa is attracting interest from powers elsewhere. Accessed on 14 August 2018 at: https://www.economist.com/briefing/2019/03/07/africa-is-attracting-ever-more-interest-from-powers-elsewhere.

The Global Times, 12 April 2019. China exports facial ID technology to Zimbabwe. Accessed on 30 March 2020 at: https://www.globaltimes.cn/content/1097747.shtml.

The Herald. 2018. Surveillance cameras for Harare. Accessed on 16 March 2019 at: https://www.herald.co.zw/2m-surveillance-cameras-for-harare/.

The Herald. 2019. ED lays US$23,6m internet backbone. 14 March 2019. Accessed on 20 March 2020 at: https://www.herald.co.zw/ed-lays-us236m-internet-backbone/

The Irish Times. 2003. Zimbabwe's first black president (67) dies. 11 November 2003. Accessed on 20 March 2020 at: https://www.irishtimes.com/news/zimbabwe-s-first-black-president-67-dies-1.510102

The New York Times. 2019. China's racial profiling technology. Accessed on 23 May 2019 at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

The Presidency. 2019. President Ramaphosa releases Review Panel Report on State Security Agency. 9 March 2019. Accessed on 19 September 2019 at: http://www.thepresidency.gov.za/press-statements/ president-ramaphosa-releases-review-panel-report-state-security-agency

The Zimbabwe Independent. 2008. High court dismisses CIO application. Accessed on 2 February 2019 at: https://www.theindependent.co.zw/2008/03. /27/high-court-dismisses-cio-application-on-zimind-story/

The Zimbabwe Independent. 2013. CIO steps up mass citizen surveillance. Accessed Accessed 3 March 2019 at: https://www.theindependent.co.zw/2013/08/30/cio-steps-up-mass-citizen-surveillance/

The Zimbabwe Mail. 2019. Charamba loyalist targeted in fresh round of purges. Accessed on 12 March 2019 at: https://www.thezimbabwemail.com/editors-memo-pad/charamba-loyalists-targeted-in-fresh-round-of-purges-at:-the-herald/

The Zimbabwe News, 2018. Leaked WhatsApp messages blamed for Judith Makwanya's death. Accessed on 19 September 2019 at: https://zwnews.com/leaked-zbc-whatsapp-chats-insulting-ed-blamed-for-judith-makwanya-death/.

The Zimbabwe Urban Councils Act of 2015. Accessed on 6 May 2020 at: https://zimlii.org/zw/legislation/act/2001/222001

Toll Infrastructure Services. 2015. SANRAL ITS rehabilitation. Accessed on 19 September 2019 at: http://www.tollinfra.co.za/projects-clients-2/local-projects/sanral-its-2/

Transparency International. 2019. *Global Corruption Barometer 2019*. Accessed on 19 September 2019 at: https://www.transparency.org/gcb10/africa?/news/feature/global_corruption_barometer_gcb_africa_2019

Transport Telematics Africa Pty Ltd. 2010. CCTV Safety and Security Installation for the Central Business District and 2010 Soccer World Cup Fan Mile Walkway. Accessed on 14 August 2019 at: https://transtelafrica.co.za/portfolio/cctv-for-cbd-soccer-world-cup/

Tredger, C. 2018. US$1.5 billion fund launched to help build Africa's smart city ecosystem*. ITWeb Africa,* 16 May 2018. Accessed on 14 August 2019 at: http://www.itwebafrica.com/business-intelligence/507-africa/244230-us15-billion-fund-launched-to-help-build-africas-smart-city-ecosystem

VPRO Documentary. 2015. Bringing internet to Africa. *YouTube video*. 12 June 2015. Accessed on 19 September 2019 at: https://www.youtube.com/watch?v=qlTZetW1Sy8&feature=youtu.be&t=2162

Vumacam press conference, 14 February 2019.

Vumacam. 2019a. Home page. Accessed on 14 August 2019 at: https://www.vumacam.co.za

Vumacam. 2019b. Next level security. Home page. Accessed on 1 October 2019 at: https://www.vumacam.co.za

Vumacam. 2019c. Vumacam not in the business of tracking movements. 25 September 2019. Access on 10 October 2019 at: https://www.vumacam.co.za/vumacam-not-in-the-business-of-tracking-movements/

Wen, Y. 2017. *The Rise of Chinese Transnational ICT Corporations: The Case of Huawe*i. Simon Frazer University. Accessed on 14 August 2019 at: https://summit.sfu.ca/item/17505

West, E. 2019. SA-China trade ties get R27bn boo*st*. *Independent Online,* 24 June 2019. Accessed on 14 August 2019 at: https://www.iol.co.za/business-report/economy/sa-china-trade-ties-get-r27bn-boost-27367274

Workman, D. 2019a. *Diamond Imports by Country.* 19 June 2019. Accessed on 14 August 2019 at: http:// www.worldstopexports.com/diamond-imports-by-country/

Workman, D. 2019b. *Diamond Exports by Country*. 9 August 2019. Accessed on 14 August 2019 at: http:// www.worldstopexports.com/diamond-exports-country/

Xinhua News Agency. 2018. Botswana seeks to promote nation's diamonds in Chinese market: official. 6 November 2018. Accessed on 14 August 2019 at: http://www.xinhuanet.com/english/2018-11/06/c_137586568.htm

Xinhua News Agency. 2019. Huawei project in Botswana to help reduce crime incidents: official. 27 August 2019. Accessed on 14 September 2019 at: www.xinhuanet.com/english/2019-08/27/c_138340372.htm

Yujie, X. 2019. Camera above the classroom. *Sixth Tone,* 26 March 2019. Accessed on 14 March 2020 at: https://www.sixthtone.com/news/1003759/camera-above-the-classroom

Zhongxiang, Z. 2011. Developing a Mindset of Corporate Consciousness. *China Report*, vol. 3. 3 January 2011. Accessed on 7 September 2019 at: http://www.chinafrica.cn/english/china_report/txt/201101/02/content_322394.htm

Zimbabwe Lawyers for Human Rights. 2016. Enforced disappearances – An information guide for human rights defenders and CSOs. Accessed on 19 September 2019 at: https://www.zlhr.org.zw/wp-content/uploads/2016/10/Enforced-Disappearances-An-Information-Guide-for-Human-Rights-Defenders-and-CSOs.pdf

Zimbabwe News, 11 May 2019. Charamba loyalists demoted. Accessed on 19 September 2019 at: http:// zimbabwe.shafaqna.com/EN/AL/483271

Zimbabwe Peace Project. 2009. *Peace Monthly Report: November 2009*. Harare. Zimbabwe Peace Project Printers

Zimbabwe Situation. 2019. Civil society leaders under military watch list. Accessed on 2 May 2019 at: https:// www.zimbabwesituation.com/news/civil-society-activists-on-military-watch-list/

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 the Open Society Initiative for South Africa (OSISA)

OSISA
Open Society Initiative for Southern Africa