# Digital Neocolonialism: The Chinese Surveillance State in Africa

Willem H. Gravett *

*Associate Professor, University of Pretoria Faculty of Law, Pretoria, South Africa.

I gratefully acknowledge the very able and conscientious assistance of S. P. Nortjé in the preparation of this article.

## ABSTRACT

China has developed into a twenty-first-century surveillance state with unprecedented abilities to censor speech and infringe upon basic human rights. The effects of China's digital authoritarianism reach well beyond its national borders. The Chinese government has begun exporting its high-tech surveillance blueprint, and the censorship and surveillance technologies on which it is based, to authoritarian-leaning governments in Africa. This blueprint is suffused with the potential for developing surveillance societies in China's image, particularly in African countries with poor human rights records, where democratic institutions are either weak or still in their infancy. This may yield even greater repression, rather than liberalisation, in Africa. The consequences for human rights on the African continent are likely to be dire.

Keywords: Africa, China, Digital authoritarianism, Digital Neocolonialism, Surveillance technology

## I. INTRODUCTION

In January 2020 the United States Defense Secretary, Mark Esper, stated that China has developed into 'a 21st century surveillance state with unprecedented abilities to censor speech and infringe upon basic human rights'.[1] China has become the first digital authoritarian state.[2] 'Digital authoritarianism' refers to the use of digital information technology by authoritarian regimes to surveil, repress and manipulate domestic and foreign populations.[3]

The Chinese have long pioneered digital tools for domestic censorship and surveillance,[4] harking back to the launch of the digital bulwark of Chinese information control – the so-called 'Great Firewall' of China – more than two decades ago.[5] Under President Xi Jinping the Chinese government has vastly expanded domestic surveillance to play a greater role in strengthening the Communist Party's hold on society.[6]

Rapid advances in surveillance technology, coupled with growing police access to user data, have turned China into a 'techno-dystopia' and have helped facilitate the prosecution of prominent human rights advocates and ordinary users.[7] More content is considered sensitive and activists and journalists are receiving heavy penalties for their online activities.[8] Ethnic and religious minorities continue to be mercilessly surveilled and persecuted for their spiritual and cultural expression or for exposing human rights abuses against their communities.[9]

This increased emphasis on domestic censorship and surveillance is fuelling a new generation of companies that manufacture sophisticated surveillance technology. These surveillance systems could help underpin a 'future of tech-driven authoritarianism … leading to a loss of privacy on an industrial scale'.[10] Although they are sold to citizens as 'public security systems', these technologies have darker potential uses as tools of political repression.[11]

Moreover, China has also begun to export its model of digital authoritarianism across the globe, including to Africa.[12] It is clear that if the Chinese government is able to surveil, control, track and curtail almost 1,400,000,000 people, then other nations with much smaller populations can do it as well.[13] China has been selling its blueprint abroad, including the hardware and software it uses in its surveillance regime.[14] This blueprint is suffused with the potential for developing surveillance societies in China's image, particularly in countries with poor human rights records, where democratic institutions are either weak or still in their infancy.[15] Moreover, as China makes further advances in information technology, this may yield even greater repression, rather than liberalisation, in Africa.[16]

In this article I argue that Chinese technological penetration in Africa raises the spectre of 'digital neocolonialism' – the application by China of economic and political pressures, through technology, to control and influence African nations.

## II. CHINA: 'THE PERFECT SURVEILLANCE STATE'[17]

Paul Mozur, a journalist for the *New York Times*, succinctly describes China's digital authoritarianism thus:[18]

> With millions of cameras and billions of lines of code, China is building a high-tech authoritarian future … It wants to assemble a vast and unprecedented surveillance system, with crucial help from its thriving technology industry.

### *A. 'Sharp Eyes'*

China has gradually been applying new technologies to build 'an ever-growing, ever-intruding surveillance state'.[19] China has become the world's biggest market for security and surveillance technology.[20] By 2010 Beijing alone was blanketed by 800,000 surveillance cameras, and by 2015 Beijing police boasted that the city was 100 per cent covered.[21] In 2015 the government set itself the goal of covering all public spaces and leading industries in 300,000,000 cameras by 2020, with the aim of creating an 'omnipresent, fully networked, always working and fully controllable' surveillance system – a nationwide panopticon[22] – combining data mining with sophisticated video and image analysis.[23]

This 'Sharp Eyes' ('Xue Liang') initiative is extraordinary for its reach and scope.[24] The name of the project is taken from the Communist slogan 'the masses have sharp eyes', and is a throwback to Mao Zedong's attempt to coerce every citizen to spy on others.[25] As 'Sharp Eyes' feeds are coupled with location data taken from smartphones and vehicles, Beijing will increasingly be able to monitor the movements and behaviour of its citizens in unprecedented detail.[26] These efforts will then merge with a vast database of information on every citizen – a 'police cloud' that aims to encompass criminal records, medical records, travel bookings, online purchases and even social media comments – and link all this information to every citizen's identity card and face.[27] The national watchlist of would-be criminals and potential political agitators is already comprised of between 20,000,000 and 30,000,000 people.[28]

China's vision for a real-time, nationwide surveillance network requires more than just ubiquitous video streaming and sensor data. It also needs to leverage artificial intelligence to identify and track individuals across the network.[29] As a result Chinese companies, such as Hikvision (the world's largest manufacturer of surveillance equipment), Sensetime, Yitu and Megvii, have moved aggressively to meet this demand. These companies received over US$2,000,000,000 in government-initiated investment in 2018.[30] Thus to the eyes of the masses are added the brains of the country's fast-growing technology industry.[31]

> According to the German academic, Adrian Zenz:[32]
>
> [T]he [Chinese] government craves omnipotence over a vast, complex and restive population. Surveillance technologies are giving the government a sense that it can finally achieve the level of control over people's lives that it aspires to.

***B. 'Big Data Meets Big Brother'[33]***

In 2014 the State Council announced its goal to establish a national Social Credit System (SCS) by 2020 that will 'allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step'.[34] It is the 'most ambitious experiment in digital social control in the world', aiming explicitly to influence the behaviour of an entire society.[35]

Although nationwide databases assessing the financial credibility of individuals exist in many countries, the SCS will assign each citizen a comprehensive score based not only on finances, but also on personal behaviour.[36] The SCS will collect all the data it can possibly acquire on individual Chinese citizens – social status, bank data, hospital records, real-world movements, employment, social interactions, online consumption, travel plans, social media activity and Internet browsing history.[37] Ultimately the government will have inordinate amounts of data at its disposal to control and intervene in society, politics and the economy,[38] and to quietly guide and influence behaviour.[39]

A citizen's social ranking in the government's eyes might be lowered if she gets a traffic ticket, pays her bills late, engages in rude or annoying behaviour on public transportation,[40] evades taxes, swindles other people, creates fake advertisements, or even if one of her friends posts a negative comment online.[41] Another punitive function of the system is to shame 'debtors' by displaying their faces on large screens in public spaces.[42]

Other sorts of 'untrustworthy behaviour' that will draw the attention of the authorities include: 'conduct that seriously undermines … the normal social order … [and] seriously undermines the order of cyberspace transmissions', and 'assembling to dispirit social order [and] endangering national defence interests'. Such broad and vague categories foreshadow a system that could be used to rate and punish dissent, expressions of opinions and perceived threats to security.[43]

A person's social credit score determines her access to services such as priority medical care, travel tickets, high-speed Internet, government subsidies, job opportunities,[44] private school education for her children, investment opportunities, the purchase of real estate and more advantageous terms on bank loans.[45]

There is no codification of what constitutes 'untrustworthy' behaviour or the number of points assigned to different actions.[46] There is no distinction between civil and criminal wrongs. Different municipalities also employ varying criteria and scales for calculating points, thereby affecting the entitlement of citizens to the same benefits.[47] Sanctions are imposed without following principles of natural justice, without a trial, without affording any right to appeal, and without any mechanism to be removed from the blacklist.[48]

The SCS foreshadows the disastrous consequences of technological advancement without a commensurate commitment to human rights.[49] The SCS's first casualty will be the right to privacy, as the scores for all 1,393,000,000 Chinese citizens, compiled from both private and public data, will be made publicly available. The scheme will be mandatory for all citizens – there will be no opt in or consent for either data collection or end use.[50] Private companies already share users' data with each other and the government.[51]

Freedom of speech is already being flouted with financial and travel restrictions imposed on dissidents, and freedom of association is curtailed by the widespread imposition of travel bans for blacklisted individuals.[52] According to a report from China's National Public Credit Information Center, during the last week of February 2019 people were blocked 17,500,000 times from purchasing airplane tickets and 5,500,000 times from buying high-speed train tickets for unspecified 'behavioural crimes'.[53]

***C. 'The World's Largest Digital Prison'***

To evaluate just how effective China's novel model of digital authoritarianism could be, one has to look no further than China's far-flung western province of Xinjiang. It is an area in which individual freedom, liberty and security is absent, replaced by a comprehensive state surveillance system that aims for near total control.[54] Xinjiang has become a window into the possible dystopian future of ubiquitous surveillance technology, wielded by states like China, states that have both the capital and political will to monitor – and repress – minority groups.[55]

The Xinjiang Uyghur Autonomous Region is home to the Turkic Muslim ethnic minority Uyghur population of 11,000,000 people.[56] In a country with an ethnic majority Han population, the central government in Beijing has long treated Xinjiang as a 'frontier' in which the Uyghurs require pacification and assimilation.[57]

Starting in May 2014 a spate of ethnic and separatist violence sent the Chinese government's repressive tendencies into overdrive.[58] The national police ministry implemented a 'Strike Hard Campaign Against Violent Terrorism'.[59] Beijing has drawn wide international condemnation for its harsh crackdown on, and heavy-handed tactics towards, the Uyghurs, including holding as many as 1,000,000 of these ethnic Muslims in 're-education' camps.[60] The Chinese Communist Party has subjected the entire Uyghur population in Xinjiang to arbitrary arrest, draconian surveillance and systemic discrimination.[61] As a briefing in *The Economist* makes clear:[62]

> [It is] Apartheid with Chinese characteristics … [The] regime is racist, uncaring and totalitarian, in the sense of aiming to affect every aspect of people's lives. It has created a fully-fledged police state. And it is committing some of the most extensive, and neglected, human rights violations in the world.

This Strike Hard campaign is unprecedented, not simply for its sheer scale in imposing social control, but also for its novel use and deployment of technology.[63] As the *New York Times* columnist, James Millward, puts it: '[T]he Chinese Communist Party has updated its old totalitarian methods with cutting-edge [surveillance and biometric] technology … spying from every street corner and mobile phone.'[64]

A major objective of the Strike Hard Campaign has been to weave an ever-tighter net of surveillance across the region.[65] By adding tens of thousands of new security personnel and so-called 'convenience' police stations, and by greatly increasing the number of police checkpoints in Xinjiang (one approximately every 100m) and equipping them with facial-recognition cameras, biometric sensors and iris scanners, the security services have been able to monitor the movement and behaviour of Xinjiang's residents in unparalleled detail – in vehicles on roads, in residential areas and at any point where crowds might gather, such as bus and train stations, entry points to towns and villages, hotels, restaurants, markets and mosques.[66]

Human Rights Watch has documented the Xinjiang authorities' collection of biometrics, including DNA samples, fingerprints, iris scans and blood types of all residents between the ages of 12 and 65.[67] These biometric data, as well as voice samples, are collected as part of the passport application process. DNA and blood samples are collected by stealth, through a free – but obligatory – public health programme called 'Physicals for All'.[68] Needless to say, residents of Xinjiang have absolutely no ability to challenge the collection, use, distribution or retention of their data.[69]

are also frequently forced to install spyware[70] on their smartphones through which the government can track all of their online activity, identify the people they have called and record social media use.[71] Wi-fi sniffers – probes that gather the unique addresses of devices such as laptops and smart phones – secretly collect data from all networked devices within range, and allow the government to covertly read users' e-mails.[72] All communications software on smart devices are banned, except WeChat, which grants police direct access to users' phone calls, texts and other shared content.[73] To monitor Uighur movement between checkpoints, Beijing has also mandated that all vehicles in Xinjiang must install the Chinese version of GPS.[74] In addition, security forces in Xinjiang have begun to deploy flocks of small dove-like surveillance drones to cover areas not covered by the CCTV feeds.[75]

The authorities in Xinjiang have also implemented an artificially intelligent tool, the Integrated Joint Operations Platform (IJOP), which aggregates data about people – information from smartphones, cameras, financial and family planning records, and even unusual electricity usage – mostly without their knowledge, and detects deviations from what the authorities deem 'normal' (such as paying a telephone bill late), and treats them as indicators that a person may be politically 'untrustworthy'.[76] The IJOP then generates lists of people considered to be threatening to the authorities; the police then apprehend them, interrogate them and detain some of them.[77]

In theory the security system in Xinjiang applies to everyone equally. In practice, however, it is as raced-based as apartheid was in South Africa.[78] It is abundantly clear that one segment of the population is being specifically targeted.[79] Even domestic Chinese tourists visiting the region have marvelled that, in some places, the authorities have established 'green channels' where Han can pass through without checks, while Turkic Muslims have to queue in another lane to wait for stringent security controls.[80]

It is small wonder that Human Rights Watch has described the Strike Hard Campaign in Xinjiang as arguably the world's largest open-air digital prison and an early glimpse of what digital authoritarianism might have in store.[81] In its report 'Eradicating Ideological Viruses: China's Campaign of Repression Against Xinjiang's Muslims', it found human rights violations 'of a scope and scale not seen in China since the 1966–1976 Cultural Revolution'.[82] Not only is the regime of Xi Jinping persecuting millions of people based on their ethnicity and religion, but it is also developing tools of high-tech repression that could be used by dictatorships around the world.[83] This 'Orwellian model of repression' is likely to become the norm in China, and to be exported to like-minded totalitarian regimes elsewhere, unless the Xi regime encounters significant resistance.[84]

## III. CHINESE SURVEILLANCE TECHNOLOGY IN AFRICA

### *A. Chinese Technological Penetration in Africa*

Although China's presence in Africa has been growing steadily for 20 years, it started escalating drastically in 2013 following President Xi Jinping's unveiling of the Belt and Road Initiative (BRI), a trillion dollar soft-power international development strategy to extend Beijing's influence in host countries through bilateral loans and infrastructure projects.[85] Most countries on the African continent have enthusiastically embraced the BRI.[86] China has emerged as the largest source of financing for infrastructure projects in Africa[87] and evidence of its influence is on display everywhere on the continent.

China is also sponsoring thousands of the next generation of African leaders, bureaucrats, students and entrepreneurs to undergo training and education in China.[88] China hosts tens of thousands of African university and postgraduate students every year, and the Chinese government offers thousands of scholarships to African students annually.[89] The *Hanban* (the Chinese Language Council) has also founded 59 Confucius Institutes in Africa to propagate Chinese language and culture.[90]

The BRI includes a major emphasis on information technology.[91] In Africa, China is unrivalled on the technological front.[92] Large swaths of the continent have fundamentally come to rely on Chinese companies for their telecommunications and digital services.[93] China Telecom plans to lay a 150,000km fibre optic network covering 48 African nations.[94] Transsion Holdings, a Shenzhen-based company, has overtaken Samsung to become the leading smartphone provider in Africa.[95] Huawei, the Chinese telecommunications giant, has built 70 per cent of the 4G networks and most of the 2G and 3G networks on the continent, vastly outpacing its European rivals.[96] The Kenyan government has also appointed Huawei as principal advisor on its 'master plan' for information and communication technologies.[97]

The Chinese telecommunications conglomerate, ZTE, provides the Ethiopian government with infrastructure to enable it to monitor and surveil communications by opposition activists and journalists.[98] Another Chinese company, H3C, has won the contract to construct the Nigerian airport's new telecommunications network.[99] Hikvision has established an office in Johannesburg[100] and through a local video surveillance provider has rolled out 15,000 cameras throughout the Johannesburg metropolitan area in 2019.[101]

The huge inroads that especially Huawei in recent years has made in Africa – despite the United States warning its allies to avoid contracting with the company because of cybersecurity fears – is evidence of the fact that, in Africa, the imperative for greater Internet

access trumps all.[102] Clearly, the fact that the Chinese government is the only viable provider of Internet connectivity on the continent gives it significant leverage over African governments.[103]

For many countries, Chinese technology has become an enticing commodity in light of the difficulty of developing these technologies and the costs involved to acquire them.[104] This is the reason why many African nations, through the lure of easy loans and investments, have become almost entirely dependent on China for its technology and services[105] and susceptible to pressure to subscribe to the Chinese notion of 'Internet sovereignty'. The great danger, of course, is that the Chinese model of sprawling censorship and automated surveillance systems[106] is leading to a dramatic reduction in digital freedom across the continent and threatening several emerging democracies.[107]

The threat to democracy on the continent posed by Chinese technological penetration is exacerbated by the well-known fact that African nations have experienced perennial struggles in their quest for democratisation and human rights. To date, most African countries have 'greatly backslidden in terms of growing their democracies' even after the adoption of multi-partism and liberal democracy in the 1990s.[108] The problem is that many states have merely focused on holding elections – which are most often not free and fair – neglecting the other principles of democracy, rule of law and accountable governments.[109] In the early 1990s the return to party politics was closely associated with the resumption of the civil war in Angola in 1993 and the genocide in Rwanda in 1994.[110] The reputation of Zambia's Movement for Multi-Party Democracy – one of the first opposition parties to defeat an authoritarian government at the polls – suffered when, in 1996, evidence surfaced of a flawed election and widespread corruption.[111] In 2000 Côte d'Ivoire's seemingly stable political system descended into civil war following a disputed election.[112]

Unfortunately, these democratic breakdowns continue to be a prominent feature of multi-party politics up to the present day. In 2007 election observers described the polls in Nigeria as some of the worst that they had witnessed. In that same year, accusations of electoral manipulation in Kenya set off a month of civil conflict which claimed the lives of more than 1,000 people. Also in 2007, Zimbabwe's President Robert Mugabe refused to accept defeat at the hands of the Movement for Democratic Change amid the mass repression of opposition supporters. More recently democratic experiments in South Sudan and Mali have also been undone by violent conflict.[113] Presidential elections in Uganda (2015) and Zambia (2016) were characterised by widespread voting irregularities, fraud, repeated arrest of opposition leaders and voter intimidation.[114]

It is thus clear that Chinese digital neocolonialism poses a significant threat to fragile African democracies as a robust democratic and human rights culture is yet to fully take root and flourish across the continent.

***B. The Beguiling 'Safe Cities' Narrative***

Many African nations are embracing the Chinese model of sprawling censorship and automated surveillance systems,[115] leading to a dramatic reduction in digital freedom across the continent and threatening several emerging democracies.[116] Ostensibly to help governments identify threats to 'public order', China promotes digital authoritarianism as a way for African governments to control their citizens through technology.[117] But the price to be paid for the technological expertise and infrastructure may not principally be money.

African governments are signing up for China's surveillance state, but citizens will pay the price.[118]

For example, in 2000 China's telecommunications titan, ZTE Corporation, made its debut in Ethiopia, immediately becoming the country's primary supplier of telecommunications equipment.[119] As mentioned above, the technology provided by China has been integral to the Ethiopian government's monitoring efforts of private citizens and organisations, especially those who are critical of the government.[120] Ethiopia's complete control over its telecommunications system[121] has been linked to the erosion of privacy, freedom of expression and association, and access to private information.[122] Arrests, interrogations and detention have followed in the wake of the Ethiopian government's illegal surveillance of its citizens.[123] Ethiopian authorities, using mobile surveillance, have also frequently targeted the ethnic Oromo population.

Human Rights Watch has found that the government's actual control is exacerbated by the perception among many Ethiopians that government surveillance is omnipresent. This results in considerable self-censorship, with Ethiopians refraining from openly communicating on a variety of topics across the telecommunications networks.[124]

Huawei is the leading vendor of advanced surveillance systems worldwide by an enormous margin.[125] It aggressively seeks new markets in sub-Saharan Africa.[126] It is setting up advanced 'safe city' platforms, offering facial recognition and intelligent video surveillance systems to repressive governments and providing advanced analytic capabilities.[127] The company is not only providing advanced equipment, but also offering ongoing technological support to set up, operate and manage these surveillance systems.[128]

A recent investigative report by the *Wall Street Journal* found that Huawei technicians in both Uganda and Zambia have assisted government officials to spy on political opponents.[129] This included 'intercepting their encrypted communications and social media, and using cell data to track their whereabouts'.[130] Not only did Huawei employees play a 'direct role in government efforts to intercept the private communications of opponents', but they also encouraged Ugandan security officials to travel to Algeria so that they could study Huawei's 'intelligent video surveillance system' operating in Algiers.[131]

At an academic conference of African mayors and local government officials[132] in Mombassa, Kenya, in 2019, Huawei was afforded an exclusive slot to pitch its vision for the future of African cities.[133] It is a vision centred on surveillance, artificial intelligence and 5G communication networks, in which a citizen's every movement is tracked and then captured in a searchable database.[134] The narrative is seductive because it focuses on a principal concern in African cities: security and public safety.[135] But of the technology's Orwellian ability to significantly intrude into the lives of residents and to stifle dissent, the Huawei sales team was conspicuously silent.

Ecuador, an early adopter of 'smart city' technology, stands as a particularly pertinent example for African countries. As reported in the *New York Times*, the footage from 4,300 smart cameras feeds directly into the police and 'the country's feared domestic [National Intelligence Secretariat], which under the previous president, Rafael Correa, had a lengthy track record of following, intimidating and attacking political opponents'.[136] Journalists for the *New York Times* comment:[137]

> This voyeur's paradise is made with technology from what is fast becoming the global capital of surveillance: China. Equador's system … is a basic version of a program of computerised controls that Beijing has spent billions to build out over a decade of technological progress.

In response to questions from the *New York Times*, Huawei – the manufacturer of the surveillance system in use in Equador – released a statement:[138]

> Huawei provides technology to support smart city and safe city programs across the world. In each case, Huawei does not get involved in setting public policy in terms of how the technology is used.

As in Equador, left to choose between privacy and safety, many African governments opt for the unblinking gaze of electronic eyes.[139] Concerns about the long-term human rights implications seem to trail behind the pressing realities of violence and crime.

***C. National Security Concerns***

For Beijing exporting information technology is not simply about securing important new sources of revenue and data, but also about generating greater strategic leverage vis-à-vis the West.[140]

A major part of the BRI is a 'digital Silk Road' of Chinese-built fibre optic networks across the continent, raising the concern that Chinese telecommunications technology may not only benefit repressive local authorities, but also facilitate surveillance by Chinese intelligence services.[141] These platforms can double as tools for information collection.[142] This is a particular cause for concern because the Chinese government has a 'dark history of using high-tech exports for espionage activities'.[143]

In 2012 the completion of the African Union (AU) headquarters in Ethiopia signified a symbolic gesture aimed at solidifying Sino-African relations.[144] In January 2018 *Le Monde* reported that the IT network of the AU headquarters – funded in the amount of approximately US$200,000,000 by the Chinese government, built by a Chinese state-owned company and installed by Huawei – had been hacked and had been transmitting confidential data daily to servers located in Shanghai for a period of five years.[145]

> Samuel Woodhams commented on this reported incident in *The Diplomat*:[146]
>
> That one of the most prominent political organizations on the continent had been unknowingly sending all of [its] confidential data directly to the Chinese state certainly raises concerns about the implications of China's growing influence in the technological infrastructure of Africa.

Concerns about the degree of control that the Chinese government has over Chinese technology companies' operations have led other countries to scrutinise these companies more closely.[147]

In August 2018 the United States banned government agencies and contractors from using surveillance products from several Chinese companies, including Huawei and ZTE.[148] Citing security risks, the Australian government also blocked Huawei and ZTE from building the country's 5G network. In April 2018 UK Member of Parliament, Karen Lee, stated in an

interview that she was advocating for the British government to boycott Hikvision, particularly from government facilities.[149]

United States officials have repeatedly accused Huawei and ZTE of providing a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants (so-called 'back doors') into critical telecommunications components and systems that would allow Chinese intelligence services to access the data.[150]

However, in the great need to get online, African countries have apparently chosen to overlook these concerns about the risks of allowing any company that is beholden to a foreign government – one that does not share African values – to occupy positions of power inside their telecommunications networks.[151]

A noteworthy exception are broadcasters in Ghana who, in September 2018, raised concerns about the government's negotiations with a Chinese company to build the country's digital television infrastructure.[152] The government of Ghana entered into a US$95,000,000 agreement with the Chinese company, StarTimes, to supply and install the digital terrestrial television network platform in Ghana.[153] In response, the Ghana Independent Broadcasters Association stated:[154]

> If StarTimes is allowed to control both Ghana's only digital television infrastructure and the satellite space … Ghana would have virtually submitted its broadcast space to Chinese control and content.

The Chinese Communist Party has become the dominant player in full-spectrum surveillance programmes of citizens and society in Africa.[155] China's success in exporting its surveillance hardware and software, under the guise of public security and safety, has laid the foundation for a US$150,000,000,000 industry, 'but with hidden, insidious consequences for free and open societies'.[156]

A race to the lowest common denominator of widespread and invasive surveillance is precisely what Beijing would be happy to see take place.[157] Arming autocratic-leaning governments in Africa with the ability to track the movements of their populations definitely raises concerns about the future of human rights in those states.[158]

**IV. CONCLUSION**

Although at this time African technology start-up companies cannot compete with the size and scope of Chinese technology companies, the African continent is far from helpless in staunching the creep of authoritarian Chinese technology. Not only can Africans call upon a well-established international human rights framework to address the violation of their human rights, but they also have access to a robust regional human rights system that can be used to stem the tide of Chinese repressive technology.

Human rights offer a strong value: an approach to technology governance that upholds human dignity based on international human rights law.[159] In general terms, human rights, as a language and legal framework, is itself a source of power, because human rights carry significant moral legitimacy and the reputational cost of being branded a human rights violator can be high.[160]

Targets of surveillance suffer interference with their rights to privacy and freedom of opinion and expression.[161] Surveillance may be used in an effort to silence dissent, sanction criticism or punish independent reporting.[162] In environments subject to rampant illicit surveillance, such as Ethiopia, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise the rights to freedom of expression, association, religious belief and culture. In short, interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression.[163]

The International Covenant on Civil and Political Rights (Covenant) and the Universal Declaration of Human Rights (Universal Declaration) protect everyone's rights to privacy, opinion and expression. Article 19 of both instruments protects every person's right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. Article 17(1) of the Covenant, echoing Article 12 of the Universal Declaration, provides that '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence'.

Privacy and expression are intertwined in the digital age, with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression.[164] Article 17 of the Covenant permits interference with the right to privacy only where it is 'authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant', is in pursuit of 'a legitimate aim' and 'meet[s] the tests of necessity and proportionality'.

Targeted surveillance creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information. The Human Rights Committee has emphasised that restrictions may never be invoked as a justification for the muzzling of any advocacy of multiparty democracy, democratic tenets and human rights. Attacks on a person because of the exercise of his or her right to freedom of expression may not be justified by Article 19 of the Covenant.[165]

The African Charter on Human and Peoples' Rights (African Charter) recognises in its Preamble that 'freedom, equality, justice and dignity are the essential objectives for the achievement of the legitimate aspirations of the African peoples'. It also pledges to eradicate all forms of colonialism from Africa and to have due regard to the Charter of the United Nations and the Universal Declaration.

Although the African Charter does not expressly protect the right to privacy, as stated above, particularly in the digital age, privacy is essential to, and reinforces, other fundamental rights that are expressly protected in the African Charter, to wit: respect for 'the dignity inherent in a human being';[166] 'freedom of conscience' and the 'profession and free practice of religion';[167] 'the right to receive information' and 'to express and disseminate his opinions within the law';[168] 'the right to free association';[169] 'the right to assemble freely with others';[170] and 'the right to freedom of movement'.[171] Moreover, Article 19 of the African Charter specifically protects against the persecution of minorities by the state.[172]

In May 2019 the United Nations Special Rapporteur on freedom of expression and opinion, David Kaye, concluded that the problem of pervasive technological surveillance is so serious that what is warranted is not merely tighter regulation of surveillance exports and restrictions

on their use, but for an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry, until rigorous human rights safeguards are put in place to regulate such practices.[173]

The Special Rapporteur also captured the dynamic between the government and technology companies in China. He found that government and the private sector are close collaborators in the market for digital surveillance tools. The Chinese government has requirements that its own departments and agencies may be unable to satisfy. Private companies have the incentives, the expertise and the resources to meet those needs.[174]

The Special Rapporteur found that, given the nature of the private surveillance industry and the widespread use of its products for purposes that are inconsistent with international human rights law, it is difficult to imagine that companies take the human rights impacts of their products into account.[175] Put another way:[176]

> [G]iven the broad public knowledge of the repression practised by many of their clients, the companies cannot seriously claim to lack insight into the repressive uses of their tools.

Credible allegations have shown that companies are selling their digital tools to governments, including governments in Africa, that use them to target journalists, activists, opposition figures and others who play critical roles in a democratic society.[177]

The Special Rapporteur also noted that, while human rights law provides definite restrictions on the use of surveillance tools, states conduct unlawful surveillance without fear of legal consequence.[178] It is imperative – urgently so – that states limit the uses of surveillance technologies to lawful ones only, subject to the strictest forms of oversight and authorisation, and that states require that private sector participation in the surveillance tools market – from research and development to marketing, sale, transfer and maintenance – be conditioned on human rights, due diligence and a track record of compliance with human rights norms.[179]

That is why African governments should acknowledge their human rights obligations and incorporate a duty to protect fundamental rights in national technology policies, guidelines, regulations and legislation.[180] For one thing, African countries could mandate that a human rights impact assessment be performed prior to acquiring any digital technology system, as well as on a regular and ongoing basis during the life cycle of the system.[181] They could also insist that maximum possible transparency is necessary for any technology system, including transparency regarding its purpose, how it will be used and how it works, which must continue throughout a system's life cycle.[182] Regular reporting will be necessary on where and how African governments use and manage digital technology systems.

Strong advocacy at the policy and legislative level aimed at improving the rule of law, transparency and accountability – in the government *and* the private sector – is more important than ever.[183] As digital technologies continue to shape modern life and become embedded in governance and politics to an increasing degree, the window is closing for much needed public debate about the proper balance between technology, government surveillance and the privacy rights of citizens.[184]

**ORCID**

Willem H. Gravett https://orcid.org/0000-0001-7400-0036.

**Notes**

1 As quoted in J. C. Weiss, 'Understanding and rolling back digital authoritarianism', *Texas National Security Review* (17 February 2020), available at <https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/> (accessed 31 March 2020).

2 Briefing, 'China Invents the Digital Totalitarian State', *The Economist* (17 December 2016), available at <https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state> (accessed 11 February 2020).

3 A. Polyakova and C. Meserole, 'Policy Brief: Exporting digital authoritarianism: the Russian and Chinese Models', *Brookings Institution* (August 2019), available at <https://www.brookings.edu/research/exporting-digital-authoritarianism/> (accessed 13 March 2020).

4 Digital repression comprises six techniques: surveillance, censorship, social manipulation and harassment, cyber-attacks, Internet shutdowns and targeted persecution against online users. S. Feldstein, 'When it comes to digital authoritarianism, China is a challenge, but not the only challenge', *Carnegie Endowment for International Peace* (12 February 2020), available at <https://carnegieendowment.org/2020/02/12/when-it-comes-to-digital-authoritarianism-china-is-challenge-but-not-only-challenge-pub-81075> (accessed 31 March 2020).

5 Polyakova and Meserole, *supra*, note 3.

6 L. Yuan, 'Learning China's forbidden history, so they can censor it', *New York Times* (2 January 2019), available at <https://www.nytimes.com/2019/01/02/business/china-internet-censor.html> (accessed 27 January 2020).

7 Freedom House, *China Country Report: Freedom on the Net 2018* (Freedom House 2019), available at <https://freedomhouse.org/country/china/freedom-net/2019> (accessed 27 January 2020).

8 *Ibid*.

9 *Ibid*.

10 P. Mozur, J. Kessel and M. Chan, 'Made in China, exported to the world: the surveillance state', *New York Times* (24 April 2019), available at <https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html> (accessed 23 March 2020).

11 'They're selling this as the future of governance; the future will be all about controlling the masses through technology.' Adrian Shahbaz, research director at Freedom House, as quoted in Mozur et al., *supra*, note 10.

12 Polyakova and Meserole, *supra*, note 3.

13 T. Burgers and D. Robinson, 'Networked authoritarianism is on the rise', 34 *Sicherheit und Frieden* (2016) 251.

14 S. N. Romaniuk and T. Burgers, 'How China's AI technology exports are seeding surveillance societies globally', *The Diplomat* (18 October 2018), available at <https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/> (accessed 27 January 2020).

15 *Ibid*.

16 Polyakova and Meserole, *supra*, note 3.

17 Romaniuk and Burgers, *supra*, note 14.

18 P. Mozur, 'Inside China's dystopian dreams: A.I., shame, and lots of cameras', *New York Times* (8 July 2018), available at <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> (accessed 6 February 2020).

19 Romaniuk and Burgers, *supra*, note 14.

20 Mozur, *supra*, note 18.

21 Polyakova and Meserole, *supra*, note 3.

22 E. Barrett, 'In China, facial recognition tech is watching you', *Fortune* (28 October 2018), available at <http://fortune.com/2018/10/28/in-china-facial-recognition-tech-is-watching-you/> (accessed 25 March 2020). China has plans to increase the number of facial recognition cameras to a staggering 626,000,000 by the decade's close. X. Qiang, 'The road to digital unfreedom: President Xi's surveillance state', 30 *Journal of Democracy* (2019) 57.

23 S. Denyer, 'The all-seeing "sharp eyes" of China's security state', *Washington Post* (8 January 2018), available at <https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/> (accessed 23 March 2020); Polyakova and Meserole, *supra*, note 3; Mozur, *supra*, note 18.

24 Polyakova and Meserole, *supra*, note 3. Beijing began constructing a nationwide surveillance system in 2005 called 'Skynet' to better control public order in urban areas. 'Sharp Eyes' represents the dramatic expansion and update of Skynet in 2015, intended to cover the entire country with facial recognition systems and other technology. C. Rollet, 'In China's far west, companies cash in on surveillance program that targets Muslims', *Foreign Policy* (13 June 2018), available at <https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/> (accessed 18 February 2020).

25 Denyer, *supra*, note 23.

26 S. Denyer, ‘Beijing bets on facial recognition in a big drive for total surveillance’, *Washington Post* (7 January 2018), available at <https://www.washingtonpost.com/> (accessed 20 March 2020).

27 Denyer, *supra*, note 23; Mozur et al., *supra*, note 10.

28 Mozur et al., *supra*, note 10.

29 Polyakova and Meserole, *supra*, note 3.

30 *Ibid*.

31 Denyer, *supra*, note 23.

32 As quoted in *ibid*.

33 R. Botsman, ‘Big data meets Big Brother as China moves to rate its citizens’, *Wired* (21 October 2017), available at <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion> (accessed 28 March 2020).

34 Qiang, *supra*, note 22, at 59.

35 Briefing, *supra*, note 2.

36 Qiang, *supra*, note 22, at 59.

37 The national social credit system originally planned for 2020 will be an ‘ecosystem’ of schemes of various sizes and reaches, run by cities, government ministries and online payment providers, as well as neighbourhoods, libraries and businesses. It will all be interconnected by an invisible web of information. S. Mistreanu, ‘Life inside China's social credit laboratory’, *Foreign Policy* (3 April 2018), available at <https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/> (accessed 18 March 2020); Polyakova and Meserole, *supra*, note 3; Qiang, *supra*, note 22, at 59; Burgers and Robinson, *supra*, note 13, at 251.

38 Mistreanu, *supra*, note 37. Big data, for instance, is an invaluable resource for making predictions. Officials can draw on this capacity to anticipate protests and major surges in online public opinion, enabling them to act pre-emptively to quash opposition. Qiang, *supra*, note 22, at 54.

39 Botsman, *supra*, note 33.

40 The Chinese travel authority already maintains a ‘no-fly’ list for ill-mannered passengers, who can be banned from travelling abroad for up to ten years. Briefing, *supra*, note 2.

41 Botsman, *supra*, note 33.

42 M. Latonero, ‘Governing Artificial Intelligence: upholding human rights and dignity’, *Data and Society* (date unknown), available at <https://datasociety.net/library/governing-artificial-intelligence/> (accessed 2 March 2020).

43 Briefing, *supra*, note 2.

44 Citizens with low scores will not be employed by certain employers and will be forbidden from obtaining some employment opportunities, such as the civil service, journalism and legal fields, where one must be deemed 'trustworthy'. Botsman, *supra*, note 33.

45 Mistreanu, *supra*, note 37; V. Vinayak, 'The human rights implication of China's social credit system', *Oxford Human Rights Hub* (6 September 2019), available at <https://ohrh.law.ox.ac.uk/the-human-rights-implications-of-chinas-social-credit-system/> (accessed 28 February 2020); R. Fontaine and K. Frederick, 'The autocrat's new tool kit: the next generation of repressive technology will make past efforts to spread propaganda and quash dissent look primitive', *Wall Street Journal* (15 March 2019), available at <https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637?> (accessed 25 March 2020).

46 Vinayak, *supra*, note 45.

47 *Ibid*.

48 *Ibid*.

49 *Ibid*.

50 *Ibid*.

51 *Ibid*.

52 *Ibid*.

53 See Qiang, *supra*, note 22, at 60.

54 Romaniuk and Burgers, *supra*, note 14.

55 M. Rajagopalan, 'This is what a 21st-century police state really looks like', *BuzzFeed News* (17 October 2017), available at <https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here> (accessed 23 March 2020).

56 M. Wang, '"Eradicating ideological viruses": China's campaign of repression against Xinjiang's Muslims', *Human Rights Watch* (September 2018), available at <https://www.hrw.org/sites/default/files/report_pdf/china0918_web.pdf> (accessed 13 March 2020).

57 *Ibid*.

58 Briefing, 'China has turned Xinjiang into a police state like no other', *The Economist* (31 May 2018), available at <https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other> (accessed 24 February 2020).

59 Polyakova and Meserole, *supra*, note 3; Wang, *supra*, note 56.

60 P. Mozur, 'One month, 500,000 face scans: how China is using A.I. to profile a minority', *New York Times* (14 April 2019), available at <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> (accessed 9 May 2019). These camps, of which there are thousands, are not governed by any judicial process; detentions are on orders of the police or party officials, not the verdict of a court. Briefing, *supra*, note 58.

61 J. Millward, 'What it's like to live in a surveillance state', *New York Times* (3 February 2018), available at <https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html> (accessed 27 January 2020).

62 Briefing, *supra*, note 58.

63 Polyakova and Meserole, *supra*, note 3.

64 Millward, *supra*, note 61.

65 Wang, *supra*, note 56.

66 Wang, *supra*, note 56; Polyakova and Meserole, *supra*, note 3.

67 Wang, *supra*, note 56; Qiang, *supra*, note 22, at 59.

68 Briefing, *supra*, note 58; Wang, *supra*, note 56; Qiang, *supra*, note 22, at 58; S. Feldstein, 'The global expansion of AI surveillance', *Carnegie Endowment for International Peace* (September 2019), available at <https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf> (accessed 27 January 2020), p. 21.

69 Wang, *supra*, note 56.

70 Called 'Jingwang' or 'web cleansing' the app works to monitor 'illegal religious' content and 'harmful information'. Rajagopalan, *supra*, note 55.

71 Millward, *supra*, note 61; Polyakova and Meserole, *supra*, note 3; Briefing, *supra*, note 58.

72 Rollet, *supra*, note 24.

73 Millward, *supra*, note 61.

74 This navigation system is powered by Beidou. Polyakova and Meserole, *supra*, note 3; Millward, *supra*, note 61.

75 Polyakova and Meserole, *supra*, note 3.

76 Wang, *supra*, note 56.

77 *Ibid*.

78 Briefing, *supra*, note 58.

79 Polyakova and Meserole, *supra*, note 3.

80 Wang, *supra*, note 56.

81 *Ibid*.

82 *Ibid*.

83 *Ibid*.

84 Editorial Board, 'China's Orwellian tools of high-tech repression', *Washington Post* (18 September 2018), available at <https://www.washingtonpost.com/opinions/global-opinions/chinas-orwellian-tools-of-high-tech-repression/2018/09/17/b06a9a72-baa1-11e8-9812-a389be6690af_story.html> (accessed 5 March 2020).

85 A. Roussi, 'China's bridge to Africa', 569 *Nature* (16 May 2019) 326.

86 Thus far, 39 African countries and the African Union Commission have entered into BRI cooperation agreements, with others expected to follow suit. *Ibid.*, at 325.

87 China funds one in five infrastructure projects on the continent. B. Gill, C. Huang and J. S. Morrison, 'Assessing China's growing influence in Africa', 3 *China Security* (2007): 9; B. Sautman and Y. Hairong, 'Friends and interests: China's distinctive links with Africa', 50 *African Studies Review* (2007) 80.

88 Gill et al., *supra*, note 87, at 6.

89 For example, China hosted almost 62,000 African university and postgraduate students in 2016, and the Chinese government offered 8,470 scholarships to African students in 2015. Roussi, *supra*, note 85, at 326.

90 J. Eisenman and J. Kurlantzick, 'China's Africa strategy', *Current History* (2006) 221.

91 M. Abramowitz and M. Chertoff, 'The global threat of China's digital authoritarianism', *Washington Post* (1 November 2018), available at <https://www.washingtonpost.com/opinions/the-global-threat-of-chinas-digital-authoritarianism/2018/11/01/46d6d99c-dd40-11e8-b3f0-62607289efee_story.html> (accessed 26 February 2020); Freedom House, *supra*, note 7.

92 Roussi, *supra*, note 85, at 326.

93 A. Hawkins, 'Beijing's Big Brother tech needs African faces', *Foreign Policy* (24 July 2018), available at <https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/> (accessed 27 January 2020).

94 D. Ignatius, 'China has a plan to rule the world', *Washington Post* (29 November 2017), available at <https://www.washingtonpost.com/opinions/china-has-a-plan-to-rule-the-world/2017/11/28/214299aa-d472–11e7-a986-d0a9770d9a3e_story.html> (accessed 13 March 2020).

95 Hawkins, *supra*, note 93; L. Chutel, 'China is exporting facial recognition software to Africa, expanding its vast database', *Quartz Africa* (25 May 2018), available at <https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/> (accessed 31 March 2020).

96 A. MacKinnon, 'For Africa, Chinese-Built Internet Is Better Than No Internet At All', *Foreign Policy* (19 March 2019), available at <https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/> (accessed 31 March 2020).

97 Abramowitz and Chertoff, *supra*, note 91.

98 Hawkins, *supra*, note 93.

99 Freedom House, *supra*, note 7.

100 Hawkins, *supra*, note 93.

101 H. Swart, 'Video surveillance and cybersecurity (part two): Chinese cyber espionage is a real threat', *Daily Maverick* (26 June 2019), available at <https://www.dailymaverick.co.za/article/2019–06–26-video-surveillance-and-cybersecurity-part-two-chinese-cyber-espionage-is-a-real-threat/> (accessed 27 March 2020).

102 MacKinnon, *supra*, note 96.

103 'There is leverage that comes with being the low-cost solution provider to a country whose political leadership might, in part, derive their popular support from being able to offer connectivity to their population.' MacKinnon, *supra*, note 96.

104 Romaniuk and Burgers, *supra*, note 14.

105 *Ibid*.

106 A. Shahbaz, 'Freedom on the net 2018: the rise of digital authoritarianism', *Freedom House* (October 2018), available at <https://freedomhouse.org/report/freedom-net/freedom-net-2018> (accessed 2 March 2020).

107 S. Woodhams, 'How China exports repression to Africa', *The Diplomat* (23 February 2019), available at <https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/> (accessed 27 January 2020).

108 A. Mwale and M. Libati, 'Getting to Denmark: is democracy a failed project in Africa?', 6(3) *International Journal of Scientific Research and Innovative Technology* (2019) 2.

109 *Ibid.*, at 2.

110 N. Cheeseman, *Democracy in Africa: Successes, Failures and the Struggle for Political Reform* (Cambridge University Press 2015), p. 1.

111 *Ibid.*

112 *Ibid*.

113 *Ibid.*, at 1–2.

114 Mwali and Lebati, *supra*, note 108, at 2.

115 Shahbaz, *supra*, note 106.

116 Woodhams, *supra*, note 107.

117 Abramowitz and Chertoff, *supra*, note 91.

118 Hawkins, *supra*, note 93.

119 Romaniuk and Burgers, *supra*, note 14.

120 *Ibid*.

121 The government has a monopoly over all mobile and Internet services through its sole, state-owned telecommunications operator, Ethio Telecom. C. Wong, '"They know everything we do": telecom and Internet surveillance in Ethiopia', *Human Rights Watch* (March 2014), available at <https://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_1.pdf> (accession 31 March 2020).

122 These internationally protected rights are also enshrined in the Ethiopian constitution. *Ibid*. Romaniuk and Burgers, *supra*, note 14.

123 Romaniuk and Burgers, *supra*, note 14.

124 Wong, *supra*, note 121.

125 Feldstein, *supra*, note 68, at 14.

126 *Ibid*.

127 Feldstein, *supra*, note 4.

128 Feldstein, *supra*, note 68, at 14.

129 J. Parkinson, N. Bariyo and J. Chin, 'Huawei technicians helped African governments spy on political opponents', *Wall Street Journal* (14 August 2019), available at <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 (accessed 31 March 2020).

130 Parkinson, Bariyo and Chin, *supra*, note 130.

131 *Ibid*. Uganda subsequently agreed to purchase a similar facial recognition surveillance system from Huawei for US$126,000,000. Feldstein, *supra*, note 68, at 14.

132 There were officials present from all over the continent, including Ethiopia, Kenya, Nigeria, Somaliland, South Africa, Uganda and Zimbabwe. S. Allison, 'Our cameras will make you safe', *Mail and Guardian* (15 November 2019), available at <https://mg.co.za/article/2019-11-15-00-our-cameras-will-make-you-safe/> (accessed 27 January 2020).

133 *Ibid*.

134 *Ibid*.

135 *Ibid*. A media source sympathetic to Beijing stated: 'In the bigger context, facial recognition is badly needed in Zimbabwe, and even across the whole of the African continent, since security protection, where the technology is widely used, plays a key role in Africa's social stability.' Z. Hongpei, 'Chinese facial ID tech to land in Africa', *Global Times* (17 May 2018), available at <https://www.globaltimes.cn/content/1102797.shtml> (accessed 28 January 2020).

136 Allison, *supra*, note 132.

137 Mozur et al., *supra*, note 10.

138 *Ibid*.

139 *Ibid*.

140 Polyakova and Meserole, *supra*, note 3.

141 Abramowitz and Chertoff, *supra*, note 91; Shahbaz, *supra*, note 106.

142 Qiang, *supra*, note 22, at 61.

143 *Ibid*. For example, on 11 December 2017 Germany's intelligence agency accused China of harvesting the personal information of German officials through the career-networking site LinkedIn. Qiang, *supra*, note 22, at 60–1.

144 A. L. Dahir, 'China "gifted" the African Union a headquarters building and then allegedly bugged it for state secrets', *Quartz Africa* (30 January 2018), available at <https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/> (accessed 27 January 2020).

145 Abramowitz and Chertoff, *supra*, note 91; Woodhams, *supra*, note 107. The Chinese government has strongly denied allegations that it had built in a backdoor into the AU's IT system to allow it to transfer data. The hack was apparently discovered in January 2017 when technicians noticed that there was a peak in data usage between midnight and 02:00 every day, although the building was empty. After investigation, it was found that the continental organisation's confidential data was being copied to servers in Shanghai. Dahir, *supra*, note 115. It was also reported at the time that microphones hidden in desks and walls were detected and removed during a sweep. C. White, 'Chinese companies using Zimbabweans as guinea pigs to identify black faces', *National Interest* (3 December 2019), available at <https://nationalinterest.org/blog/buzz/chinese-companies-use-zimbabweans-guinea-pigs-

identify-black-faces-report-101447> (accessed 27 January 2020). Needless to say, both the African Union and the Chinese government dismissed the allegations. MacKinnon, *supra*, note 96.

146 Woodhams, *supra*, note 107.

147 Shahbaz, *supra*, note 106; Swart, *supra*, note 101.

148 Shahbaz, *supra*, note 106. Hikvision has also attracted scrutiny in the West, especially in the United States where the company's cameras are deployed at army bases and other sensitive locations. Hikvision's strong ties to the Chinese government have raised concerns in the United States that China might be harnessing these cameras for espionage. Rollet, *supra*, note 24; Swart, *supra*, note 101. Australia similarly banned local providers from purchasing 5G equipment from Huawei and ZTE. Shahbaz, *supra*, note 106.

149 Swart, *supra*, note 101. Previously, in September 2016 the *Times of London* reported that retired MI6 officers and security ministers warned that increased oversight of Chinese businesses in the UK was warranted. Swart, *supra*, note 101.

150 Allison, *supra*, note 132; Feldstein, *supra*, note 68, at 33. The strength of these secret back doors is that they are remotely exploitable – they allow someone access to the compromised system from the outside with very little chance of being detected. Swart, *supra*, note 101.

151 Shahbaz, *supra*, note 106. Eric Olander, co-founder of the China Africa Project, a non-profit and independent multimedia resource in Shanghai, commented: 'You can see why when the US said "don't work with Huawei," the Africans looked and shrugged and said "Yeah, that's not going to happen."'

152 S. Cook, 'China's cyber superpower strategy: implementation, Internet freedom implications, and US responses', *Freedom House* (28 September 2018), available at <https://freedomhouse.org/article/chinas-cyber-superpower-strategy-implementation-internet-freedom-implications-and-us> (accessed 27 January 2020).

153 'Don't hand digital migration contract to StarTimes – GIBA warns government', *Balancing Act* (21 September 2018), available at <https://www.balancingact-africa.com/news/broadcast-en/44028/dont-hand-digital-migration-contract-to-startimes-giba-warns-government> (accessed 18 February 2020).

154 *Ibid*.

155 Romaniuk and Burgers, *supra*, note 14.

156 *Ibid*.

157 Cook, *supra*, note 152; L. Andersen, 'Human rights in the age of artificial intelligence', *Access Now* (November 2018), available at <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> (accessed 2 March 2020).

158 See Woodhams, *supra*, note 107.

159 Latonero, *supra*, note 42.

160 C. van Veen and C. Cath, 'Artificial intelligence: what's human rights got to do with it?', *Data & Society Points* (14 May 2018), as referred to in Latonero, *supra*, note 42.

161 D. Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', *Human Rights Council* (28 May 2019), A/HRC/41/35 para. 21, at 7.

162 *Ibid.*, para. 21, at 7.

163 *Ibid.*, para. 24, at 8.

164 *Ibid.*

165 General Comment No. 34, paras 25, 34, 35. Kaye, *supra*, note 161, para. 24, at 9.

166 Article 5.

167 Article 8.

168 Article 9.

169 Article 10.

170 Article 11.

171 Article 12.

172 It states that '[a]ll people shall be equal; they shall enjoy the same respect and shall have the same rights. Nothing shall justify the domination of a people by another.'

173 Kaye, *supra*, note 161, at 3.

174 *Ibid*., para. 15, at 6.

175 *Ibid*., para. 29, at 9–10.

176 *Ibid*., para. 29, at 10.

177 *Ibid*., para. 48, at 14.

178 *Ibid*., para. 46, at 14.

179 *Ibid*.

180 Latonero, *supra*, note 42.

181 Andersen, *supra*, note 159.

182 *Ibid*.

183 R. MacKinnon, ‘Liberation technology: China's “networked authoritarianism”’, 22 *Journal of Democracy* (2011) 44.

184 Feldstein, *supra*, note 68, at 24.