Policy Insights
99
December 2020

The Impact of Chinese Tech Provision on Civil Liberties in Africa

IGINIO GAGLIARDONE

African perspectives
Global insights

SAIIA
SOUTH AFRICAN INSTITUTE OF INTERNATIONAL AFFAIRS

Executive summary

The increasing support provided by China to African states to expand their information infrastructure and the rise of Safe City (Huawei) and Smart City (ZTE) projects across Africa have raised concerns about a possible tightening of civil liberties on the continent. Some of these concerns are motivated by cases of abuse of Chinese-deployed surveillance platforms in Africa. Others build on various assumptions and ambiguities this study seeks to unpack and challenge, offering a more fine-grained analysis of the specific technologies, actors and discourses that are indeed endangering individual freedoms. As illustrated both by trends in Chinese support to communications in Africa and by individual case studies, greater financing from China has not led to an increase in authoritarianism or greater adoption of a supposed 'Chinese model' of the Internet in recipient countries. At the same time, Huawei and ZTE have played on perceptions of Chinese tech to market their Safe City/Smart City solutions in African metropoles. In the absence of strong regulatory frameworks, the deployments of these solutions can indeed expose individuals to levels of surveillance and control that can impinge on their rights of expression and association. Yet, as emerging data from already deployed Safe City and Smart City projects suggests, the perception of Chinese surveillance tech as particularly effective and sophisticated is not matched by the actuality of its chaotic implementation. As much as promises of 'liberation technologies' to free the world from abuse and dictators have been challenged by the actual interaction of these technologies with existing networks of power and politics, so new surveillance technologies or 'technologies of unfreedom' run similar risks when inserted into contexts that are very different from those where they originated.

Introduction

The strategies the Chinese government has developed to discipline domestic media, and its increasing support in developing information infrastructures abroad, have created an expectation of China as a net exporter of authoritarianism. In 2018 Google's former CEO, Eric Schmidt, suggested that in 10 or 15 years users may have to deal with a bifurcated Internet, with one half controlled by an alliance of democratic states and the other by a network of sophisticated autocracies with China at its centre.[1] Early assessments of China's expansion into African media and telecommunications have warned about China's 'emphasis … on forming alliances that are anti-Western and on promoting an anti-Western media model to combat what the Chinese regularly portray as part of an imperialist plan to distort the truth'.[2]

1 Hamza Shaban, "Former Google Chief Predicts the Internet Will Split by 2028: A Chinese Web and an American One", *The Washington Post*, September 21, 2018, https://www.washingtonpost.com/technology/2018/09/21/former-google-chief-predicts-internet-will-split-by-chinese-web-an-american-one/.

2 Douglas Farah and Andy Mosher, *Winds From the East* (Washington DC: Center for International Media Assistance, 2010).

The strategies the Chinese government has developed to discipline domestic media, and its increasing support in developing information infrastructures abroad, have created an expectation of China as a net exporter of authoritarianism

The narrative framing China as active promoter of its own alternative Internet model is powerful and seemingly convincing. It rests, however, on assumptions that have not been tested and a lack of engagement with what China has actually done in countries where it has begun contributing to the development of information infrastructure.

A common supposition is that China would behave as Western countries have in the past, when they sought to advance their own models in the form of development assistance. However, studies that have examined Chinese support of the evolution of information and communications technology (ICT) on the African continent – as well as in other sectors – have shown there is little proof of its seeking to impose a blueprint based on its model(s).[3] On the contrary, China seems to have adapted to the requests advanced by its partners, leading to the emergence of relatively diverse types of projects and agreements. While this strategy can be criticised for the lack of pressure put on governments – especially those with authoritarian tendencies – to promote information societies that are open and inclusive, it does not amount to the imposition of a particular template.

China seems to have adapted to the requests advanced by its partners, leading to the emergence of relatively diverse types of projects and agreements

The lack of clarity surrounding the distinction between government and corporate interests has fuelled fears that any form of Chinese engagement in the information space may lead to an erosion of individual liberties. The ban imposed by the Trump administration on contracts with Chinese telecom giant Huawei – motivated by the possibility of security breaches and connivance between the company and the Chinese government – and the subsequent pressure by the US on other countries to follow its lead, have exacerbated

3 Iginio Gagliardone, *China, Africa, and the Future of the Internet* (London: Zed Books, 2019); Deborah Brautigam, *The Dragon's Gift: The Real Story of China in Africa* (Oxford: Oxford University Press, 2009); Giles Mohan and Ben Lampert, "Negotiating China: Reinserting African Agency into China-Africa Relations", *African Affairs* 112, no. 446 (2013): 92–110.

this concern. Numerous Chinese companies involved in telecommunications (eg, ZTE) and surveillance (eg, Hikvision) are indeed partially state-owned and have clear ties with ministries of the Chinese government. However, the tendency to assume that even privately owned companies will promote the interests of the Chinese government can be deceiving. It fails to recognise, at least, how some of these companies have not behaved differently from their counterparts in the US or Europe (eg, Ericsson, Facebook, Vodaphone), seeking profit where they could spot lucrative opportunities, in ways that only loosely – and instrumentally – tie in with the interests of the leadership in the countries where they are headquartered (eg, availability of preferential loans; diplomatic support). Worse, for those who are interested in the geopolitical consequences of Chinese engagement in the information sector, these assumptions prevent one from recognising that the strategies followed by Huawei, Alibaba or Tencent may be very different from – and in some cases even contradict – those pursued by the Chinese government. Indeed, a greater footprint of Chinese companies in foreign countries can motivate concerns that in the future the Chinese government might exploit them, applying pressure to disclose sensitive information, or worse. However, as Edward Snowden's leaks of the US National Security Agency's global surveillance programme revealed, this has already been the case with numerous US companies, including Cisco, Facebook and Google.[4]

The tendency to assume that even privately owned companies will promote the interests of the Chinese government can be deceiving. It fails to recognise, at least, how some of these companies have not behaved differently from their counterparts in the US or Europe

Unlike other studies that have highlighted the negative repercussions for civil liberties of Chinese engagement in the global information sector,[5] this policy insight seeks to locate the operations of Chinese companies in a broader context, one where multiple actors and processes are helping to erode some of the freedoms and opportunities once associated with the Internet. Keeping the focus narrowly on China does uncover worrying practices that deserve scrutiny and for which corporate and government agents need to be held accountable. It also emboldens, however, a false sense of moral complacency in those pointing fingers at China as possibly the main agent responsible for this tightening of users' rights and possibilities to act freely online and offline. If one's ambition is detecting

4 Glenn Greenwald, *No Place to Hide* (New York, London: Penguin, 2014).

5 Sarah Cook, Beij*ing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017* (Washington DC: Freedom House, 2020); Sarah Cook, *The Long Shadow of Chinese Censorship*, Report (Washington DC: Center for International Media Assistance, 2013), https://freedomhouse.org/sites/default/files/CIMA-China_Sarah%20Cook_10_22_13.pdf; Farah and Mosher, *Winds From the East*.

fragilities in the system protecting citizens from undue interference, it is important to recognise that China forms part of a larger puzzle.

This does not mean engaging in a form of 'whataboutism', a practice associated in the past with Soviet propaganda and aimed at fending off criticism against the Soviet Union by pointing at how countries in the West engaged in similarly questionable practices, eg, supporting dictators or discriminating against minorities. Indicating how different actors, in the East and in the West, are promoting discourses and practices that are increasingly legitimising corporate and government surveillance and control is not meant to foster a sense of confusion and impotence, as if little could be done to resist an ongoing trend towards restricting civil liberties, or to attach equal blame to any actor. It is aimed, on the contrary, at identifying and assigning distinct responsibilities and roles to different actors in ways that can promote more tailored responses, which could ultimately lead to greater protection of individual rights and freedoms.

China's tech surge in Africa

Since its initial attempts to break into Africa's information sector in the early 2000s, China's expansion has been rapid if not necessarily even (spreading equally across different countries) or linear (growing steadily over time). It has connected large public companies, resellers of affordable tech products, emerging software multinationals and a skilled workforce seeking a better fortune abroad. These actors have pursued different goals and have helped to create often-contradictory images of China's role in Africa's information societies. This means that different answers can be found depending on the vantage point chosen to explore the repercussions of China's increased engagement in this space.

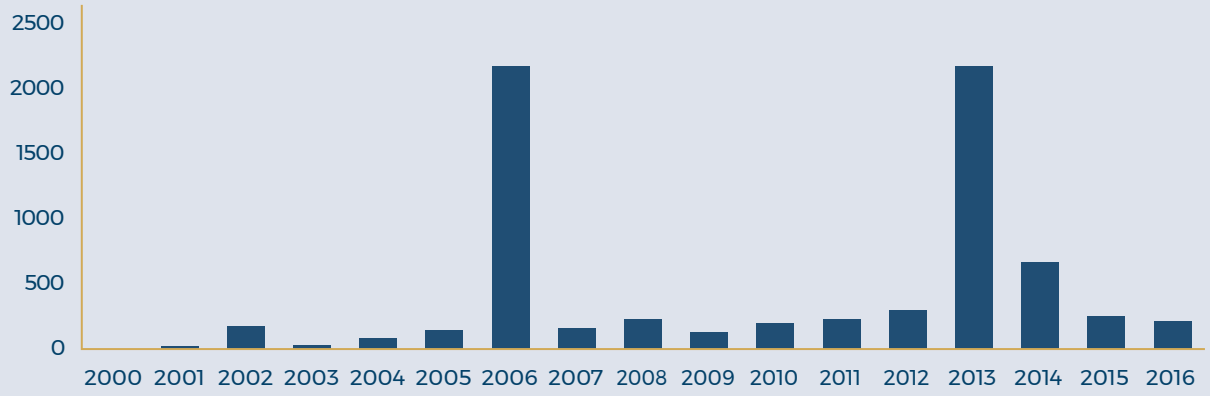
According to data collected by the China-Africa Research Initiative (CARI) at Johns Hopkins University,[6] official support to the ICT sector in Africa has varied significantly over time, going from being non-existent in 2000 to peaking at more than $2 billion in 2006 and 2013. As Figure 1 shows, there has been a significant fluctuation in funding disbursed in different years, tied to the launch of projects in specific countries. This defies impressions of Chinese engagement in this sector either steadily growing over time or representing a continent-wide phenomenon.

Only 27 countries in Africa have received loans in the communications sector, with huge disparities between beneficiaries. Out of the $6,766 million in loans verified by CARI between 2000 and 2016, almost half ($3,162 million) went to just one nation: Ethiopia. Countries with similarly strong ties with China, and that had received massive loans to support other types of infrastructure (eg, transport, power generation) such as Kenya, Ghana, Nigeria and the Democratic Republic of Congo (DRC), were offered significantly

6 China-Africa Research Initiative, "Chinese Loans to African Governments, 2000–2017", 2020, http://www.sais-cari.org/data.

smaller contributions. The case of Ethiopia – as detailed below – is unique not only for the size of the loan but also for its significance in redesigning the national ITC landscape, with potentially significant repercussions in many areas of social and economic life. In all other cases, financing from the Chinese government was instrumental in supporting specific and self-contained projects, mostly geared towards creating or expanding information infrastructure, in competition with projects managed by national or international operators, and with only limited potential to promote or impose a specific model on a national scale.

Figure 1 Official Chinese support to communications in Africa (2000–2016, million $)



Source: China-Africa Research Initiative, "Chinese Loans to Africa Database: Communication", https://chinaafricaloandata.org/

The complex architecture of Chinese development financing has been critically analysed elsewhere, both in general and with respect to the communications sector, and this study allows only limited space for examining it in depth.[7] Possibly the most relevant aspects to point out here are:

- The loans provided to support ICT projects exist in the context of the Chinese government's drive to boost its image as a friendly partner, willing to match the demands of its African counterparts with few questions asked. In most cases, investments in ICT – rather than manufacturing or transport – have been driven by African governments' decision to make use of Chinese 'benevolence' in that specific sector, rather than by the Chinese government's encouragement to choose ICT over other areas.

7 Deborah Brautigam, "Aid 'with Chinese Characteristics': Chinese Foreign Aid and Development Finance Meet the OECD-DAC Aid Regime", *Journal of International Development* 23, no. 5 (2011): 752–764; Iginio Gagliardone, "Media Development with Chinese Characteristics", *Global Media Journal* 4, no. 2 (2014): 1–16; May Tan-Mullins, Giles Mohan and Marcus Power, "Redefining 'Aid' in the China–Africa Context", *Development and Change* 41, no. 5 (2010): 857–881.

- The emergence of ICT alongside other, more 'traditional' spheres of Chinese development assistance to Africa (eg, mining, agriculture, transport) has been driven by a related interest in fending off the image of China as an 'exploitative' partner, seeking to control African resources for its own benefit, rather than helping African countries on their own path towards socio-economic progress.

In general, official loans in the ICT sector can be better understood as a diplomatic tool for the Chinese government to strengthen its relations with key partners in Africa than as a hegemonic attempt to promote its own conception of the information society abroad. China has assisted both countries flagged as authoritarian (eg, Ethiopia, the DRC) and countries recognised as more democratic (eg, Kenya, Ghana).

Official loans in the ICT sector can be better understood as a diplomatic tool for the Chinese government to strengthen its relations with key partners in Africa than as a hegemonic attempt to promote its own conception of the information society abroad

In terms of the possible repercussions of Chinese engagement in the ICT sector on civil liberties, this lack of 'intent', and willingness to support projects under different types of regimes, does not amount to a form of neutrality or a dearth of consequences. The diplomatic nature of the support has meant that invariably it has been African governments that have been strengthened in their pursuit of specific visions, rather than private companies or civil society organisations – two other essential actors in promoting functioning and inclusive information societies. This tendency to privilege some partners over others is particularly worrying in the case of authoritarian regimes, but can also have negative repercussions for democratic states, tilting the balance of power towards an already powerful actor – and one that has shown an inclination towards seizing new technologies to increase its ability to conduct surveillance.

Beyond official channels, Chinese tech companies have also made significant inroads into African markets. In some cases, the nature of their business has raised concerns about their impact. This has applied to handset manufacturer Transsion, which, since its quiet debut in 2006, has risen to become the top-selling phone maker in Africa, overtaking Samsung in 2017.[8] In other cases, companies that had already benefited from projects supported through official loans – as a result of the tied aid commonly pursed by China, offering finance under the condition that Chinese companies are contracted in the

8 Yomi Kazeem, "Samsung Is Making a Comeback, but China's Transsion Is Still Africa's Top Phone Maker", *Quartz*, December 10, 2019, https://qz.com/africa/1765210/transsion-is-africas-top-phone-maker-but-samsung-is-back/.

implementation phase – ventured on their own into agreements with other African private operators or exploited emerging niche markets, securing, for example, lucrative contracts in the surveillance industry. Some of these projects, including Huawei's Safe City and ZTE's Smart City, have fuelled anxieties that the system of centralised control that progressively emerged in China may begin to take root – if not in African countries at large, then at least in their largest cities. Also in this case, however, some of the worst fears seem to have been motivated by a lack of understanding of how specific projects have been implemented on the ground, and by an inability to locate China's role in this sector in the broader context of a race for surveillance that goes well beyond China.

BOX 1 ETHIOPIA AND CHINA: A RELATIONSHIP OF MANY PARADOXES

On 8 November 2006 the Ethiopian Telecommunications Corporation (now Ethio telecom) and ZTE signed the largest agreement in the history of telecommunications in Africa. Backed by the China Development Bank, ZTE offered a loan of $1.5 billion to overhaul and expand Ethiopia's telecommunications system. Six years later, another $1.6 billion was entrusted to ZTE and Huawei to continue the expansion, bringing Chinese government support for Ethiopia's communications sector to over $3 billion; the largest by far of all Chinese interventions in Africa's communications sector.

The magnitude and significance of China's exposure in shaping Ethiopia's information infrastructure may lead one to expect this would also amount to Chinese dominance in shaping the country's policies and strategies, especially in areas of surveillance and information control. And yet, things are significantly more complex.

Because of the evidence leaked by Snowden, we now know that it was not China but the US that first trained Ethiopia's intelligence forces on how to tap online communications. Under the codename of Lion's Pride, the US National Security Agency launched in 2002 what began as a modest counterterrorism operation to eavesdrop on communications in Somalia, Sudan and Yemen. This slowly evolved into a larger effort, enabling Ethiopia to conduct surveillance on online communications across the Horn of Africa.[a]

Thanks to research by The Citizen Lab,[b] we also know Ethiopian authorities did not stop at requesting support from China to build their infrastructure and from the US to strengthen their surveillance capabilities. They also shopped in the European market for advanced surveillance technologies, acquiring tools to spy not only on individuals living in Ethiopia but also on Ethiopians in the diaspora. FinSpy, a surveillance system sold by a firm first headquartered in the UK and later in Germany, was bought by the Ethiopian government to allow the remote accessing of infected computers. Hacking Team, an Italian company selling 'eavesdropping software' that 'hides itself inside target devices',[c] provided services to the Ethiopian government allowing it to acquire communications from opposition leaders and journalists in the diaspora.[d]

Given this evidence, one could imagine a hypothetical scenario where an Ethiopian spy may have been trained by US forces to use European software to harvest data from a Chinese-built network.

This scenario shows the importance of not focusing narrowly on China as a possible engine of greater surveillance and control, if one's concern is not just attaching blame but also understanding what forces and actors are actually driving a tightening of individuals' liberties. It also serves as a reminder of the significance of domestic politics and policies. Even a country with limited technical capabilities, rather than being pushed into complying with agendas imposed by the West or the East, can exploit its partners to strengthen its own political plan.

Domestic agency and a deeper understanding of the interests and ideologies of African governments are important when charting processes that lead to a possible tightening of civil liberties, as well as those potentially leading to their strengthening, despite global trends pointing in a different direction.

In another paradoxical turn of events, since the rise to power of Prime Minister Abiy Ahmed – who served in the military and headed the Ethiopian Information Network Security Agency for two years – Ethiopia has embarked on an unprecedented process of opening up and liberalising its communications sector. Press freedom has dramatically improved, allowing even the most critical opponents of the regime – many of whom hail from the vocal Ethiopian diaspora based in the US – to launch news outlets and resume their work as journalists.[e] A bid has been issued for the privatisation of state-owned Ethio telecom, appointing international consulting firm KPMG to manage the transition.[f] At the time of this policy insight's going to press, it appears that mobile operators headquartered in Africa (eg, Safaricom, MTN) and Europe (eg, Orange), but none from China, will have submitted their offers.[g]

a Nick Turse, "How the NSA Built a Secret Surveillance Network for Ethiopia", *The Intercept* (blog), September 13, 2017, https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/.

b A consortium of academic institutions combining political and technical expertise to map how different technologies are used in ways that can impinge on citizens' rights and liberties.

c Ironically, Hacking Team was hacked in 2015, leading to 400GB of private communications entering the public domain.

d Bill Marczak et al., "Hacking Team and the Targeting of Ethiopian Journalists", The Citizen Lab (blog), February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/; Morgan Marquis-Boire et al., "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools", The Citizen Lab (blog), January 2013, https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/; Morgan Marquis-Boire et al., "You Only Click Twice: FinFisher's Global Proliferation", *The Citizen Lab* (blog), March 2013, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

e Even Freedom House, which in the past has not reserved criticism of Ethiopia, has included it among the "encouraging examples of democratic progress" in its 2019 report on the global state of Media Freedom. See Freedom House, *Freedom and the Media 2019: A Downward Spiral* (Washington DC: Freedom House, 2019), https://freedomhouse.org/sites/default/files/FINAL07162019_Freedom_And_The_Media_2019_Report.pdf.

f "Ethiopia Appoints Ethio Telecom Privatization Adviser, Seeks Another for Licensing", *Reuters*, September 26, 2019, https://www.reuters.com/article/us-ethiopia-privatisation-idUSKBN1WB1I5.

g "Safaricom Likely to Borrow to Fund Ethiopia Telecom Bid", *Bloomberg.Com*, February 19, 2020, https://www.bloomberg.com/news/articles/2020-02-19/safaricom-likely-to-borrow-to-fund-ethiopia-telecom-bid; "Privatisations in Ethiopia: Could MTN Pull off a Surprise?", *The Africa Report*, January 28, 2020, https://www.theafricareport.com/22663/privatisations-in-ethiopia-could-mtn-pull-off-a-surprise/.

The state and the corporate

Over the past two decades, the Chinese government has developed one of the most sophisticated apparatuses of digital surveillance and control; one that has become even more stringent and unforgiving under the tenure of President Xi Jinping. The limited, but concrete, avenues to use digital media to promote reform at a local and national level, experimented with in the 2000s and early 2010s, have been progressively reduced since Xi took power in 2012.[9] This has led to a deterioration in civil liberties for Chinese citizens, constrained from speaking outside the discursive and political spaces deemed relatively safe by the top leadership and coordinating to promote political change in ways that contradict the party's ideology.[10]

The tightening of the national information space, however, has not amounted – at least to date – to a more aggressive attempt to promote a supposed Chinese model of the Internet abroad. On the contrary, in public statements or when discussing projects supported with Chinese funds, Chinese officials have been consistent in refraining from portraying China as a model that should be followed by other partners. As numerous scholars have pointed out, the emergence of a complex techno-political regime in China, able to contain dissent, channel it when necessary, and steer public opinion through an ever-changing combination of machine and human agents, has been guided by the need to respond to local and emerging challenges, rather than a supposed hegemonic ambition to experiment with and redesign the global Internet.[11]

Despite the increasing availability of studies on China's Internet, and an appetite for shortcuts towards models of an information society that combine economic growth and political stability, it would be difficult to distil the essential components of a system that has emerged through trial and error over two decades into guidelines for export. In addition, it would be a controversial – and likely counterproductive – move for Beijing to change course and start promoting its supposed model abroad at a time it has become even more oppressive.

An interesting contradiction, however – and one that has not been fully captured by the increasingly numerous reports on Chinese-driven authoritarianism or surveillance – is that the persistent silence of Chinese officials has not been matched by a similar approach among Chinese corporate agents. The opposite, in fact, seems to have been the case.

---

9 Baogang He and Mark E Warren, "Authoritarian Deliberation: The Deliberative Turn in Chinese Political Development", *Perspectives on Politics* 9, no. 02 (2011): 269–289; Min Jiang, "Authoritarian Informationalism: China's Approach to Internet Sovereignty", in *Essential Readings of Comparative Politics*, eds. P O'Neill and R Rogowski (New York: WW Norton & Company, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2119692; Guobin Yang, "(Un)Civil Society in Digital China: Demobilizing the Emotions of Online Activism in China – A Civilizing Process", *International Journal of Communication* 12 (2018): 21.

10 Anne-Marie Brady, "Plus Ça Change?: Media Control Under Xi Jinping", *Problems of Post-Communism* 64, no. 3–4 (July 4, 2017): 128–40, https://doi.org/10.1080/10758216.2016.1197779.

11 Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (New York: Columbia University Press, 2013); Yang, "(Un) Civil Society in Digital"; Yuezhi Zhao, "Understanding China's Media System in a World Historical Context", in *Comparing Media Systems Beyond the Western World*, eds. Daniel C Hallin and Paolo Mancini (Cambridge: Cambridge University Press, 2012), 143–173.

In their leaflets, promotional materials and accounts of projects developed in foreign countries, companies such as Huawei and ZTE often boast about the revolutionary potential of their solutions. These, they claim, can facilitate centralised control, reduce crime, and improve the efficiency of policing at competitive prices. The apparent – and so far unexplored – incongruities of these approaches (one championed by the Chinese government, the other by Chinese companies) can offer important clues on the nature of different types of projects and their possible consequences on civil liberties and other aspects of socio-political life in the countries where they are implemented.

From the city to the countryside?

As discussed, large, official loans by China to African states in the ICT field do not seem to have led to a deterioration of civil liberties in recipient countries thus far, even if they have benefited governments over other important players, with potential consequences in the longer term. Ethiopia (see Box 1) is the strongest case in point, having received almost half of the funds disbursed by China to Africa in the communications sector despite having embarked on an unprecedented programme of reform under the leadership of Abiy, leading to an opening of the communications space.

As argued above, and more extensively in academic studies mapping the evolution of China's information society and its possible ramifications beyond its borders, the sheer complexity of the system developed over time by the Chinese government, with variable support from local tech companies, makes replicating a similar combination of strategies and technologies almost impossible in another socio-political context.

However, while it may be difficult to link shifts in national relevance and scale directly to China, it is still possible that Chinese interventions or access to advanced technologies that first emerged in China may have notable repercussions on a more limited scale. This could be the case with the numerous projects targeting African – and global – metropoles, in which, possibly for the first time, Huawei and ZTE have played with the perception of Chinese tech as uniquely effective when it comes to maintaining law and order.

Both Huawei and ZTE have aggressively marketed their Safe City and Smart City solutions – as they respectively brand their technology-aided urban law enforcement packages – to foreign buyers by citing significant successes not only in Africa and Latin America but also in Europe. This despite the relatively greater resistance to Chinese tech that has emerged in some European countries, among others as a result of US pressure. As Steven Feldstein illustrated in his comprehensive analysis of the global expansion of surveillance powered by artificial intelligence (AI), both liberal democracies and autocratic states have been buying surveillance systems.[12] Huawei and other Chinese companies indeed dominate this

12 Steven Feldstein, "The Global Expansion of AI Surveillance" (Paper, Carnegie Endowment, Washington DC, 2019), https://carnegieendowment. org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

sector, followed by companies headquartered in the US and Japan, but regime type per se is seemingly not correlated with the adoption of such technologies, nor with the types of companies providing them. Chinese companies have signed contracts with governments in liberal democracies, and US companies have offered their services to authoritarian regimes.[13] This does not mean, however, that the expansion of powerful surveillance systems is unproblematic, and abuses are more likely to occur in authoritarian states.

Figure 2 Slide from a presentation by ZTE illustrating the global outreach and diversity of its Smart City projects

Source: ZTE, "Smart City Solution Overview", October 13, 2017, https://www.slideshare.net/TechUK/zte-smart-city-solution-overview

As the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has pointed out, the unregulated or inadequately regulated diffusion of surveillance technologies poses severe challenges to individuals' rights to freedom of association and expression.[14] Principles of necessity and proportionality need to be followed to justify increased surveillance, and governments seldom engage in public debates before launching new measures as part of their Safe City/Smart City projects. In this sense, the dominance of Chinese companies in urban surveillance, the affordability of their solutions, and their tendency to sign contracts with governments irrespective of

13 Feldstein, "The Global Expansion of AI".

14 Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (New York: UN, 2013); Frank La Rue, *The Right to Privacy in the Digital Age* (New York: UN, 2014); David Kaye, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (New York: UN, 2019).

whether these governments respect the principles highlighted by the UN, do represent a potential threat to individual liberties.

Huawei has provided advanced tools, either as part of its Safe City solution or in support of interventions aimed at stepping up local surveillance capabilities, in numerous African countries, confirming its position as a leader in this emerging segment of the industry. ZTE, while able to secure large contracts in Europe and Latin America, helping for example Marseille to brand itself as 'the first "safe city" of France and Europe', has deployed only a limited number of Smart City projects in Africa.[15]

BOX 2 THE NUMBER OF SAFE CITY AND SMART CITY PROJECTS IN AFRICA

According to data released by Huawei and ZTE, as well as collected by the Endowment for International Peace and the Center for Strategic and International Studies, in 2019, 16 African countries had signed contracts with Huawei in this area: Algeria, Botswana, Côte d'Ivoire, Egypt, Ethiopia, Ghana, Kenya, Mauritius, Morocco, Nigeria, Rwanda, South Africa, Uganda, Zambia and Zimbabwe. ZTE had a smaller presence, with projects launched in only five countries: Egypt, Ethiopia, Nigeria, Sudan and Zambia.

Both companies have developed diverse and layered packages. Relying on a system connecting an operation centre that analyses vast amounts of data in real time with a multiplicity of sensors and cameras deployed across the city, they offer services ranging from mundane smart metering to more worrying emergency assessments aimed at keeping 'social peace', and predictive policing.[16]

The deployment of these systems on African soil has been supported by public authorities, invoking increasingly pervasive discourses of securitisation and the need to protect citizens. Yet, counter-narratives pointing to cases of abuse have begun to emerge. As reported by the *Wall Street Journal*, Huawei technicians have helped the governments of Uganda and Zambia to track political opponents.[17] In 2017 Huawei invited Ugandan security officials to study its newly operational video surveillance system deployed in Algiers. As one of the officials conceded, 'We discussed hacking individuals in the opposition who can threaten national security', remarking that Algerians were already advanced in that field.[18] In 2019

15 Alvaro Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Forms and Their International Expansion to Emerging Markets" (Institut Barcelona Estudis Internacionals, Barcelona, 2017).

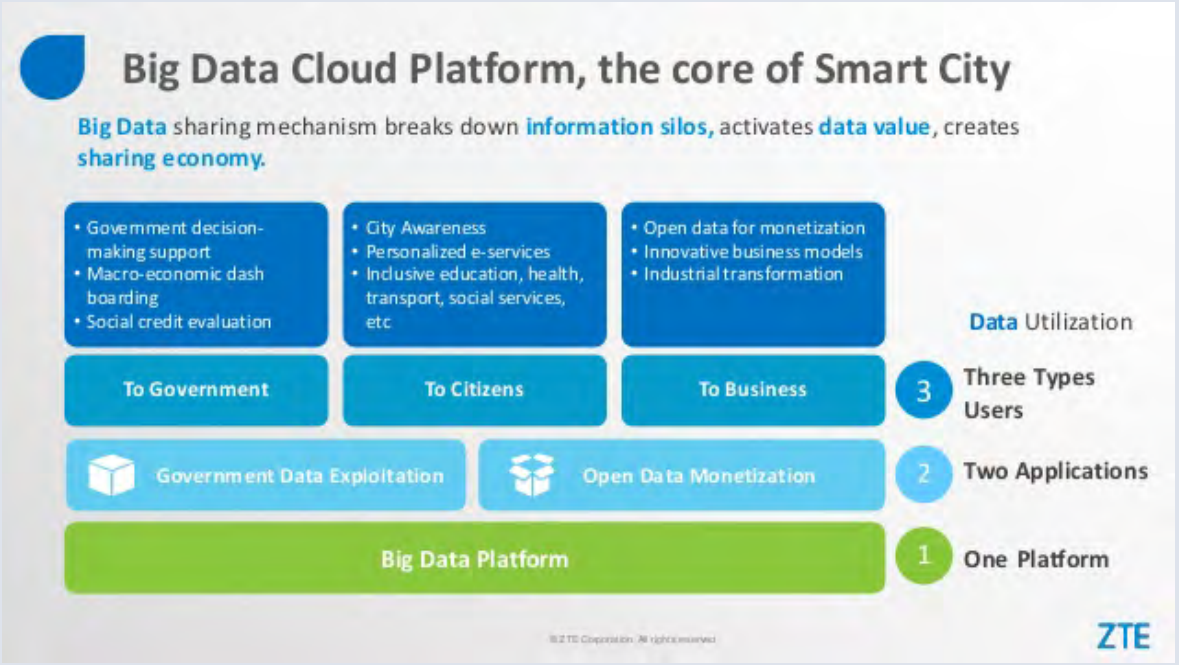
16 Artigas, "Surveillance, Smart Technologies".

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

18 Parkinson, Bariyo and Chin, "Huawei Technicians Helped African".

the Ugandan government signed a $126 million contract with Huawei for a closed-circuit television camera (CCTV) system to be deployed in Kampala and in other major cities.[19]

Figure 3 Slide from a presentation by ZTE illustrating the functioning and different types of services offered by its Smart City



Source: ZTE, "Smart City Solution Overview", October 13, 2017, https://www.slideshare.net/TechUK/zte-smart-city-solution-overview

One of the tactics pursued by Mao Tse-tung in the civil war against the Kuomintang was encircling cities from the countryside. A similar strategy has apparently characterised Huawei's own evolution, as it targeted first peripheral markets in China and globally and grew from there to become a leader nationally and internationally. Projects like Safe City and Smart City seem to – paradoxically – go in the opposite direction, deploying and normalising practices in urban spaces perceived as chaotic and unruly, as a possible first step towards scaling these practices for wider implementation. As with every technology, however, it is important to reflect on the challenges posed by transferring innovations from the context where they first originated to new environments, characterised by unique technical and political conditions.

19 Elias Biryabarema, "Uganda's Cash-Strapped Cops Spend $126 Million on CCTV from Huawei", *Reuters*, August 16, 2019, https://www.reuters.com/article/us-uganda-crime-idUSKCN1V50RF.

The techno-politics of surveillance

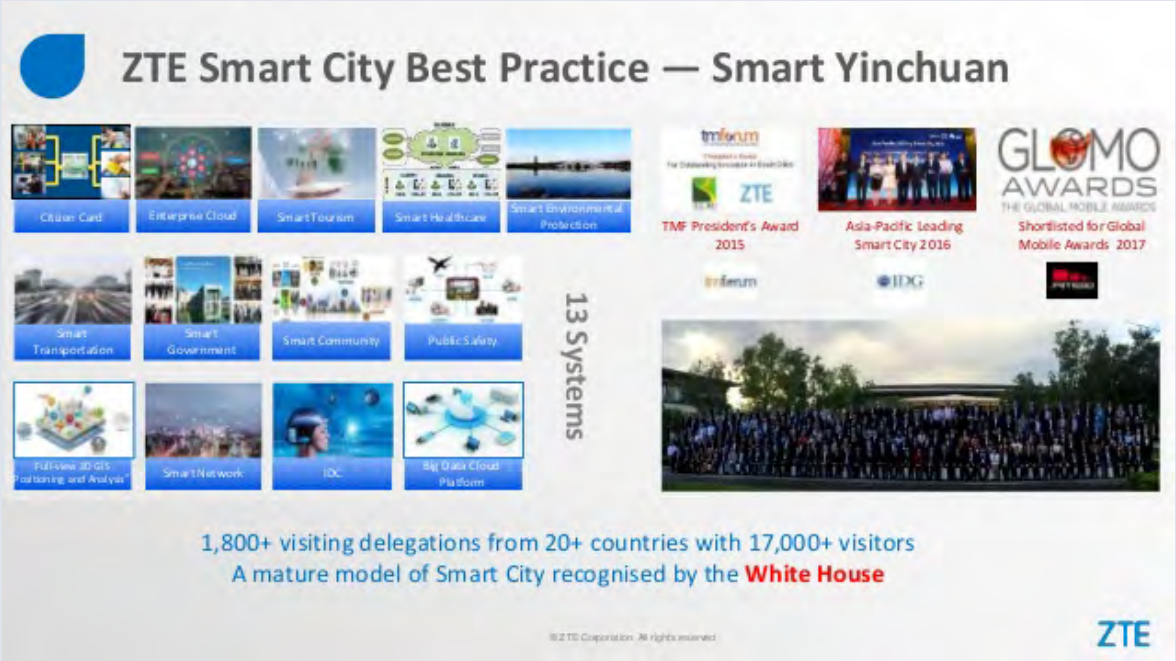
Using language that seems to contradict the subdued tone employed by Chinese authorities when providing support in the communications sector (but that is quite ordinary for companies seeking to sell their products), Huawei and ZTE have boasted about the ability of their solutions to uniquely match the needs of overcrowded and chaotic African cities. In presentations and promotional materials both companies have sought to create an image of unparalleled efficiency, stressing their ability to offer tangible results over short timeframes.

Figure 4 Slide from a presentation by Huawei offering stats on the supposed impact of the deployment of Safe City

Source: Huawei, "Network-Wide Intelligence, Opening and Sharing: Development Trend of Video Surveillance Technology and Service", https://reconasia-production.s3.amazonaws.com/media/filer_public/aa/3d/aa3d5c68-e826-46c6-a2a5-bc8454d6a5ba/huawei_intelligent_video_surveillance_technology_and_service_development_trend_material.pdf

Huawei and ZTE have also capitalised on perceptions of Chinese technology and surveillance strategies as particularly effective, drawing on examples from Chinese cities as proof of the benefits of a comprehensive deployment of Smart City and Safe City solutions (See Figure 5).

Figure 5 Slide from a presentation by ZTE detailing the benefits of the deployment of Smart City in Yinchuan (capital of the Ningxia Hui region)



Source: ZTE, "Smart City Solution Overview", October 13, 2017, https://www.slideshare.net/TechUK/zte-smart-city-solution-overview

Data emerging from projects developed outside of China, however, has begun to reveal how promises of curbing crime and improving centralised city management clash with the – quite predictable – complexity of the socio-political and technological realities of different locales. Reports from Pakistan, one of the main beneficiaries of China's Belt and Road Initiative, indicate that, after a slight reduction in the year following the installation of Huawei's Safe City in the country's major urban centres, violent crime has continued to rise.[20] 'Huawei claimed that the endeavour would dramatically improve order, with a projected 15% reduction in violent crime. But while crime in Islamabad did fall in 2016, by the end of 2018, it had increased by 33%.'[21] Kenya, an early African adopter of Huawei's Safe City, experienced a similar trajectory, with crime rates apparently unaffected by the installation of new surveillance technologies in Nairobi and Mombasa.[22]

20 Nicole Hao, "Huawei 'Safe City' Systems Are Ineffective, Crime Figures Show", *The Epoch Times*, December 29, 2019, https://www.theepochtimes.com/huawei-safe-cities-are-ineffective-according-to-crime-figures_3187283.html; Prasso, "Huawei's Claims That It Makes Cities Safer Mostly Look Like Hype", *Bloomberg.Com*, November 12, 2019, https://www.bloomberg.com/news/articles/2019-11-12/huawei-s-surveillance-network-claims-face-scrutiny.

21 Hao, "Huawei 'Safe City' Systems".

22 Prasso, "Huawei's Claims That It".

Data emerging from projects developed outside of China, however, has begun to reveal how promises of curbing crime and improving centralised city management clash with the – quite predictable – complexity of the socio-political and technological realities of different locales

These failures should not be surprising. The hype surrounding surveillance technologies and the fear provoked by their coming from China have led to some overlooking the fact that every artefact is part of wider networks that profoundly influence its functioning.[23] As much as promises of 'liberation technologies' that would free the world from abuse and dictators have been challenged by the actual interaction of these technologies with existing networks of power and politics, so new surveillance technologies risk faltering and failing when inserted into contexts that are very different from those where they originated. The 'successes' recorded by Safe City and Smart City when deployed in China are only in part due to the technological solutions developed by Huawei and ZTE. They also depend on larger networks shaped by norms, bureaucracies and policies that significantly affect the outcomes of these technologies.

Similarly, the functioning of locally deployed systems of surveillance is heavily influenced by the trajectories followed by the technologies that pre-date them and the discourses that have informed their deployment. The latest – Chinese-made – surveillance solutions, while bringing innovation to some components of these systems, cannot but relate to existing realities, adapting to, rather than radically reshaping, pre-existing networks of power. As vividly illustrated in an analysis of smart CCTV networks in South Africa, the systems of private surveillance deployed in wealthy neighbourhoods have become progressively more efficient as a result of their integration with and increasing reliance on systems of facial recognition and crime prediction developed in Australia and Israel.[24] As the systems learned how to detect unusual behaviours, however, they also began to reproduce deep-rooted biases in South African society, disproportionally flagging black South Africans as potential threats and somehow reinstating a new form of 'AI-powered apartheid'.[25] The recently signed contract between one of South Africa's leading surveillance companies and China's Hikvision is helping to take this system – which has developed over a decade – to scale, rather than determining how it operates.[26]

23 Iginio Gagliardone, *The Politics of Technology in Africa* (Cambridge: Cambridge University Press, 2016).

24 Michael Kwet, "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa", VICE, November 22, 2019, https://www.vice.com/en_us/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa.

25 Kwet, "Smart CCTV Networks Are".

26 Heidi Swart, "Visual Surveillance and Weak Cyber Security, Part One: When Cameras Get Dangerous", *Daily Maverick*, June 13, 2019, https://www.dailymaverick.co.za/article/2019-06-13-visual-surveillance-and-weak-cyber-security-part-one-when-cameras-get-dangerous/.

Conclusion

Increasing Chinese support for the development of information societies in Africa, and the deployment of surveillance technologies relying on facial recognition and AI by Huawei and ZTE on the continent, have raised concerns about the potential impact on civil liberties, including freedom of expression and freedom of association. As this policy insight has illustrated, while Chinese authorities and companies are playing a role in making some surveillance technologies more pervasive, they represent only one component of a more complex phenomenon. Arguments supporting the greater securitisation of public life have increased, often driven by African governments and corporate agents rather than a desire among Chinese actors to promote a supposed Chinese model of the information society worldwide. Huawei and ZTE have indeed aggressively marketed their Safe City and Smart City packages in Africa, and the relative affordability and readiness of their solutions have made them more accessible to African governments with limited resources. However, Chinese companies are not alone in this emerging market; companies headquartered elsewhere in the East and in the West have similarly sought contracts with government and corporate agents with dubious records in terms of protecting individual rights and liberties. If the concern is defending civil liberties, greater pressure needs to be exerted on a broader variety of actors, at both the national and international level, to set standards that any company should respect, and to promote a deeper public debate on the necessity and repercussions of expanded surveillance technologies.

Author

Iginio Gagliardone
is Associate Professor in Media and Communication at the University of the Witwatersrand and Associate Research Fellow in New Media and Human Rights at the University of Oxford (Programme in Comparative Media Law and Policy). He is the author of The Politics of Technology in Africa (Cambridge University Press) and China, Africa, and the Future of the Internet (ZED, Bloomsbury).

Acknowledgement

SAIIA would like to acknowledge the Swedish International Development Cooperation Agency for their generous support for this publication.

About SAIIA

SAIIA is an independent, non-government think tank whose key strategic objectives are to make effective input into public policy, and to encourage wider and more informed debate on international affairs, with particular emphasis on African issues and concerns.

SAIIA's policy insights are situation analysis papers intended for policymakers, whether in government or business. They are designed to bridge the space between policy briefings and occasional papers.

Cover image

A worker cleans a surveillance camera on a street in Nairobi, on January 18, 2019. (Yasuyoshi Chiba/AFP via Getty Images)

African perspectives.
Global insights.

Jan Smuts House, East Campus, University of the Witwatersrand
PO Box 31596, Braamfontein 2017, Johannesburg, South Africa
Tel +27 (0)11 339-2021 • Fax +27 (0)11 339-2154
www.saiia.org.za • info@saiia.org.za