AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: W Gravett 'Digital neo-colonialism: The Chinese model of internet sovereignty in Africa' (2020) 20 *African Human Rights Law Journal* 125-146
http://dx.doi.org/10.17159/1996-2096/2020/v20n1a5

Digital neo-colonialism: The Chinese model of internet sovereignty in Africa

*Willem Gravett**
Associate Professor, Faculty of Law, University of Pretoria, South Africa
https://orcid.org/0000-0001-7400-0036

Summary: *China is making a sustained effort to become a 'cyber superpower'. An integral part of this effort is the propagation by Beijing of the notion of 'internet sovereignty' – China's supreme right to govern the internet within its borders and keep it under rigid control. Chinese companies work closely with Chinese state authorities to export technology to Africa in order to extend China's influence and promote its cyberspace governance model. This contribution argues that the rapid expansion across Africa of Chinese technology companies and their products warrants vigilance. If African governments fail to advance their own values and interests – including freedom of expression, free enterprise and the rule of law – with equal boldness, the 'China model' of digital governance by default might very well become the 'Africa model'.*

Key words: *Chinese internet censorship; data surveillance; digital authoritarianism; digital neo-colonialism; global cyber governance; internet sovereignty*

* BLC LLB (Pretoria) LLM (Notre Dame) LLD (Pretoria); willem.gravett@up.ac.za.
I gratefully acknowledge the very able and conscientious assistance of SP Nortjé in the preparation of this article.

1 Introduction

Digital technology often is lauded as liberating, favouring the striving for equal justice, democracy and human rights.[1] Liberal democracies assume that a global and open internet 'supports free speech, and progressively spurs global interconnectivity … Principles like "freedom", "openness", and "interoperability" are critical in this liberal-democratic approach.'[2] These assumptions prompted the New York Times columnist, Nicholas Kristof, in 2005 to write: '[I]t's the Chinese leadership itself that is digging the Communist Party's grave, by giving the Chinese people broadband.'[3] However, the Chinese government has shown the 'techno-optimists' to be wrong; far from igniting a political transformation in China the internet is an indispensable tool advancing state censorship and surveillance.[4] China discovered how to exploit the internet and information technology in ways that reduce – instead of enhance – freedom.

Perhaps of greater concern is the fact that the Chinese government has transferred its domestic policies on digital technology to its foreign policy.[5] As part of President Xi Jinping's strategy to transform China into a 'cyber superpower', the government and Chinese technology companies engage in a sustained effort to export the technology at the heart of the country's information-control system to nations around the globe.[6] This 'China model' of digital governance is a palatable guise for a far-reaching system of state censorship that is enhanced by cutting-edge digital technologies.[7] Through a global infrastructure project, the Belt and Road Initiative (BRI), China

1 T Burgers & D Robinson 'Networked authoritarianism is on the rise' (2016) 34 *Sicherheit und Frieden* 248. In January 2010 Hillary Clinton, then United States secretary of state, delivered a landmark address on internet freedom. She argued that the spread of communications technology and free flow of information would ultimately lead to greater freedom and democracy. HR Clinton 'Remarks on internet freedom' 21 January 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (accessed 20 March 2020).

2 J Sherman & R Morgus 'Authoritarians are exporting surveillance tech, and with it their vision for the internet' *Council on Foreign Relations* 5 December 2018, https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet (accessed 31 March 2020).

3 N Kristof 'Death by a thousand blogs' *The New York Times* 24 May 2005, https://www.nytimes.com/2005/05/24/opinion/death-by-a-thousand-blogs.html (accessed 31 March 2020).

4 A Polyakova & C Meserole 'Policy brief: Exporting digital authoritarianism: The Russian and Chinese models' *Brookings Institution* August 2019, https://www.brookings.edu/research/exporting-digital-authoritarianism/ (accessed 13 March 2020).

5 Polyakova & Meserole (n 4).

6 Freedom House 'China country report: Freedom on the net 2018' *Freedom House* 2019, https://freedomhouse.org/country/china/freedom-net/2019 (accessed 27 January 2020).

7 X Qiang 'The road to digital unfreedom: President Xi's surveillance state' (2019) 30 *Journal of Democracy* 62.

spreads this technology which advocates its vision of a government-supervised internet across the globe including to Africa.[8]

This article opens with a brief exposition of the Chinese model of internet sovereignty; a model in terms of which the Xi regime has built a national version of the internet 'walled off' from the global internet and allowing complete state control over the free flow of information online. Next the focus is on demonstrating how influential the Chinese notion of 'internet sovereignty' has become offering an alternative version to the Western view of the internet as traversing national borders by allowing the regime to demand that domestic as well as foreign technology companies abide by its rules on censorship and advance its regime's strategic goals. This demonstration is followed by an accounting of the extent of Chinese technological penetration in Africa, supporting the argument that the combination of a near wholesale reliance on Chinese technology infrastructure and soft loans from Chinese banks are conducive to establishing a framework in which an increasing number of African nations subscribe to the Chinese technology governance model. The conclusion expresses a warning that the rapid expansion of Chinese technology across Africa warrants vigilance and a proposition that although the nascent technology industry in Africa cannot compete with the likes of China or the United States, African nations have leverage and are able to set policy. In the sphere of digital governance these nations have started and must continue to prioritise the rule of law, transparency and accountability in the service of political discourse that is free and democratic.

Chinese technological penetration in Africa is of a nature to raise the spectre of 'digital neo-colonialism' – the application by China of economic and political pressure through technology in order to control and influence the actions of African nations.[9] Chinese digital neo-colonialism in Africa takes the form of three principal elements, namely, (i) advocating the Chinese model of 'internet sovereignty' in African nations; (ii) exporting authoritarian surveillance technology

8 P Mozur et al 'Made in China, exported to the world: The surveillance state' *The New York Times* 24 April 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html (accessed 23 March 2020); L Yuan 'Learning China's forbidden history, so they can censor it' *The New York Times* 2 January 2019, https://www.nytimes.com/2019/01/02/business/china-internet-censor.html (accessed 27 January 2020).

9 Through its deep technological penetration into Africa Chinese 'digital neo-colonialism' results in African nations exhibiting a relationship characterised by dependence and financial obligation towards China, functionally an imitation of the relationship under the erstwhile colonisers. This situation leads to an undue degree of political control that China is in a position to exert in order to advance its model of digital governance across the African continent.

to African states[10] and (iii) deploying artificial intelligence technology and data-mining techniques across Africa.[11] This article is an exposition of the Chinese model of 'internet sovereignty' and its application in Africa.

2 The Chinese model of internet sovereignty and the rise of a walled internet

China has subverted the popular perception that technology will act in the role of a great democratising force[12] leading to the increase in freedom, transparency and participation.[13] In China technology brings surveillance and control.[14] The phrase 'internet sovereignty' first entered the public debate in June 2010 when China published a white paper in which it reaffirmed the primacy of its right to govern the internet within its borders and to keep it under rigid control. This white paper stated that '[w]ithin Chinese territory the internet is under the jurisdiction of Chinese sovereignty. The internet sovereignty of China should be respected and protected.'[15] It declared: 'Laws and regulations clearly prohibit the spread of information that contains content subverting state power, undermining national unity [or] infringing upon national honour and interests.'[16]

The Chinese state has successfully built a national version of the internet – 'walled off' from the global internet – in which it holds full

10 See, eg, Polyakova & Meserole (n 4).
11 See, eg, A Gwagwa & L Garbe 'Exporting repression? China's artificial intelligence push into Africa' 17 December 2018 *Council on Foreign Relations*, https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa (accessed 23 March 2020).
12 J Sherman & R Morgus 'Authoritarians are exporting surveillance tech, and with it their vision for the internet' *Council on Foreign Relations* 5 December 2018, https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet (accessed 31 March 2020).
13 JC Weiss 'Understanding and rolling back digital authoritarianism' 17 February 2020 *Texas National Security Review*, https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/ (accessed 31 March 2020).
14 P Mozur 'Inside China's dystopian dreams: AI, shame, and lots of cameras' *The New York Times* 8 July 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html (accessed 6 February 2020); Weiss (n 13). For a brief but insightful history of China's internet controls, see JL Goldsmith & T Wu *Who controls the internet? Illusions of a borderless world* (2006) 87-104.
15 As quoted in S Woodhams 'How China exports repression to Africa' *The Diplomat* 23 February 2019, https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/ (accessed 27 January 2020). Qiang explains internet sovereignty as the 'primacy of rules made by national governments and the authority of national-level regulators over web content and providers'; Qiang (n 7) 53.
16 As quoted in M Bristow 'China defends internet censorship' *BBC News* 8 June 2010, http://news.bbc.co.uk/2/hi/8727647.stm (accessed 27 January 2020).

power and at will exercises control.[17] A senior analyst at the Heritage Foundation, Joshua Meservey, explains: '[T]he Chinese government frame[s] it as a sovereignty issue, but what [it is] really talking about is the ability of a state to control the free flow of information online.'[18]

In the course of 20 twenty years the Great Firewall of China[19] has become the most sophisticated, multi-layered and ominous digital apparatus of censorship and surveillance in the world.[20] It enables the Chinese government to render tens of thousands of websites inaccessible to Chinese users,[21] instantly to censor politically-sensitive material[22] and to employ an army of human censors estimated to be in the tens of thousands manually to search the internet and remove potentially subversive content.[23]

The principal danger the Great Firewall poses, writes Griffiths, 'is that, by its very existence, it acts as daily proof to authoritarians the world over that the internet can be regulated and brought to heel'.[24] The Great Firewall now could 'easily become the next major Chinese export'.[25]

The sweeping 2017 Cyber-Security Law expands online censorship and surveillance to a degree unprecedented in order to facilitate

17 China's internet governance model is unique in that it nationalised its part of the global internet. Burgers (n 1) 250.

18 As quoted in A MacKinnon 'For Africa, Chinese-built internet is better than no internet at all' *Foreign Policy* 19 March 2019, https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/ (accessed 31 March 2020).

19 See GR Barme & S Ye 'The Great Firewall of China' *Wired* 1 June 1997, https://www.wired.com/1997/06/china-3/ (accessed 20 March 2020).

20 Freedom House 'Freedom on the net 2018: The rise of digital authoritarianism' October 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2018 (accessed 2 March 2020); Woodhams (n 15); S Cook 'China's cyber superpower strategy: Implementation, internet freedom implications, and US responses' *Freedom House* 28 September 2018, https://freedomhouse.org/article/chinas-cyber-superpower-strategy-implementation-internet-freedom-implications-and-us (accessed 27 January 2020).

21 R MacKinnon 'Liberation technology: China's "networked authoritarianism"' (2011) 22 *Journal of Democracy* 32.

22 'The cyber-censors can suspend internet or social-media accounts if users send messages containing sensitive terms such as 'Tibetan independence' or 'Tiananmen Square incident'. Briefing 'China invents the digital totalitarian state' *The Economist* 17 December 2016, https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state (accessed 11 February 2020). Ironically, but not surprisingly, references to George Orwell's *Nineteen eighty-four* are also forbidden. Yuan (n 8).

23 Woodhams (n 15); Yuan (n 8); Burgers (n 1) 250.

24 J Griffiths *The great firewall of China: How to build and control an alternative version of the internet* (2019) as quoted in S Wade 'New book examines the great firewall of China' *China Digital Times* 19 March 2019, https://chinadigitaltimes.net/2019/03/new-book-examines-the-great-firewall-of-china/ (accessed 26 February 2020).

25 As above.

state control over and access to data.[26] It tightened internet controls by mandating that social-media companies register users under their real names and requires that foreign companies host all data on Chinese users on the mainland ostensibly the purpose is to increase Chinese security agencies' access to records.[27] The legislation closes loopholes in internet controls that allowed millions of Chinese citizens to 'share breaking news, expose corruption and rights abuses, [and] debate government policies'.[28]

Dissidents and human rights activist habitually are detained for posts on popular social-media platforms such as Weibo and WeChat. In January 2019 alone the regime of Xi Jinping closed down more than 700 websites and 9 000 mobile applications that allegedly did not comply with Beijing's dictate.[29]

In China's one-party autocracy the independent rule of law does not exist and virtually there is no restraint on the government's authority[30] with the consequence that many of the constraints with regard to accessing personal data present in democratic societies[31] are absent in China.[32] The Cybersecurity Law gives the government unrestricted access to virtually all the personal information of its citizens.[33] In response to the 'drastic limits on content, pervasive obstacles to access and harsh violations of user rights', in 2018 Freedom House for the fourth year in a row bestowed on China the title labelling it the world's 'worst abuser of Internet Freedom'.[34]

Speaking at the Nineteenth Communist Party Congress in 2017, President Xi Jinping declared it his aspiration to transform China into

26 See Cook (n 20); Qiang (n 7) 55.
27 Freedom House (n 17). The local storage of data would give the Chinese government unfettered access to search histories and other personal information that global technology companies routinely acquire. Qiang (n 7) 63.
28 Cook (n 17).
29 Polyakova & Meserole (n 4).
30 Qiang (n 7) 60. 'The Chinese Communist Party … remains thoroughly entrenched in power, and President Xi Jinping enjoys an extraordinary degree of political control,' having eliminated term limits on the presidency in 2018. J Doubek 'China removes presidential term limits, enabling Xi Jinping to rule indefinitely' *NPR* 11 March 2018, https://www.npr.org/sections/thetwo-way/2018/03/11/592694991/china-removes-presidential-term-limits-enabling-xi-jinping-to-rule-indefinitely (accessed 20 March 2020). 'In the months leading up to the 19th Communist Party Congress in October 2017, the trend of censorship and propaganda, and prosecutions increasingly focused on controlling and protecting Xi's image, coinciding with his evolution into the country's "paramount leader".' Freedom House (n 6).
31 In democracies, laws limit what companies may do with and the extent to which governments can access users' personal data. Briefing (n 22).
32 Qiang (n 7) 60.
33 As above; Briefing (n 22).
34 Freedom House (n 20).

a 'science and technology superpower'.[35] A month before President Jinping's speech, the Cyber Administration of China (CAC) published an article in the vanguard Communist Party journal, *Qiushi*, which was uncharacteristically forthright about the government's true aim.[36] The article acknowledges that controlling the internet was crucial to ensuring that 'the Party's ideas always become the strongest voice in cyberspace' and, in fact, is a means to ensure the party's political survival.[37]

The article further notes that online propaganda should target international audiences in 200 countries and more than one billion users globally.[38] Most disconcertingly with reference to the future in Africa the article states that the explicit aim in 'strengthening international exchanges and cooperation in the field of information technology and cybersecurity' is 'to push China's proposition of Internet governance toward becoming an international consensus'.[39]

Since 2010 China has advanced its notion of 'internet sovereignty' as an alternative to the dominant Western view that the internet exemplifies a 'singular, highly-interconnected web that traverses national borders'.[40]

3 Chinese government's influence over domestic and foreign technology companies

Manifestly, Chinese companies play a role in the Chinese government's goal of telecommunication dominance.[41] Some firms ostensibly are private enterprises apparently governed by market forces and the profit motive but they are answerable to the government and serve its strategic ends.[42] For these companies the possibility of success or failure in China's technology landscape is dependent entirely on maintaining government support.[43]

35 J Ding Deciphering *China's AI dream: The context, components, capabilities, and consequences of China's strategy to lead the world in AI* March 2018 7; Freedom House (n 20); Woodhams (n 15).
36 Cook (n 20).
37 As above.
38 As above.
39 As above.
40 Woodhams (n 15). President Jinping held his country's model of internet governance to bbe 'a new option for other countries and nations that want to speed up their development while preserving their independence'. Freedom House (n 20).
41 Freedom House (n 20).
42 As above.
43 Cook (n 20).

For example, Hikvision, the world's leading manufacturer of surveillance camera equipment, is linked closely to the Chinese government. In its 2018 annual report the company openly declared that the Chinese government is a controlling shareholder[44] and the company's Chairperson was appointed in 2018 to the National People's Congress (the rubber-stamp Parliament).[45] Similarly, a company owned by the Chinese government is the controlling shareholder in ZTE.[46]

Huawei was founded by Ren Zhengfei, a former officer in the 'military technology division' of the People's Liberation Army, the armed forces of the People's Republic of China.[47] From its foundation there are continuing strong ties between Huawei's management and the Chinese security and intelligence apparatus.[48] It has been reported consistently[49] that Huawei benefits by billions of dollars in government subsidies.[50] Huawei's ownership structure appears notably opaque. A recent academic study concluded that '99% of Huawei shares are controlled by a "trade union committee", which in all likelihood is a proxy for Chinese state control of the company'.[51]

The Chinese Communist Party systematically places 'party cells' in technology companies to enhance its access to and control over these companies.[52] At the same time senior executives are appointed

44 In a leaked confidential investors' prospectus the company candidly acknowledged that '[our controlling shareholder] … is subject to the control of the People's Republic of China government … [and] will continue to be in a position to exert significant influence over our business'. H Swart 'Video surveillance and cybersecurity (Part Two): Chinese cyber espionage is a real threat' *Daily Maverick* 26 June 2019, https://www.dailymaverick.co.za/article/2019-06-26-video-surveillance-and-cybersecurity-part-two-chinese-cyber-espionage-is-a-real-threat/ (accessed 27 January 2020).

45 C Rollet 'In China's far west, companies cash in on surveillance program that targets Muslims' *Foreign Policy* 13 June 2018, https://foreignpolicy.com/2018/06/13/in-chinas-far-west-companies-cash-in-on-surveillance-program-that-targets-muslims/ (accessed 18 February 2020).

46 Swart (n 44).

47 *Bloomberg Businessweek* reports that Zhengfei may have been a 'high-ranking Chinese spymaster and indeed may still be', as quoted in S Feldstein *The global expansion of AI surveillance* (2019) 15. The original report may be accessed at M Chafkin & J Brustein 'Why America is so scared of China's largest tech company' *Bloomberg Businessweek* 23 March 2018, https://www.bloomberg.com/news/features/2018-03-22/why-america-is-so-scared-of-china-s-biggest-tech-company (accessed 31 March 2020).

48 'Sun Yafang, for example, chairwoman of Huawei from 1999 to 2018, once worked in China's ministry of state security.' Feldstein (n 47)15.

49 Such as a 2012 US Congressional Report from the House Intelligence Committee.

50 As referred to in Feldstein (n 47) 33.

51 C Balding & D Clarke 'Who owns Huawei?' *SSRN Scholarly Paper, Rochester, NY: Social Science Research Network* 17 April 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669 (accessed 31 March 2020).

52 'China's large privately-owned firms are becoming more like state-owned enterprises, as many in recent years have implanted in their businesses cells of the Communist Party, the Communist Youth League and even discipline inspection committee.' Z Lin 'Chinese Communist Party needs to curtail its

to head the 'party cells' in companies.[53] Moreover, a national security law enacted in 2015 mandates that companies acquiesce in permitting 'third-party' (that is, government) access to their networks, source codes and encryption keys.[54]

Not only Chinese technology companies are anxious to please the Chinese government;[55] many of the world's largest technology companies either are forbidden from or are significantly hampered in the provision of services to Chinese internet users.[56] For example, Facebook and Twitter are blocked completely.[57] The Chinese government uses its authority to bar online services and dangles the lure of its enormous market (one billion potential users) to wrest cooperation from international technology companies, including their actively abetting its censorship and surveillance system.[58]

The Chinese description of 'internet sovereignty' has gained sufficient currency that Silicon Valley firms and other commercial actors kowtow to Beijing's rules, even encouraging the censorship of information to which internet users outside of China should have access.[59] In a series of incidents during 2018 international airline, hotel and automobile companies amended the presentation of information relating to topics such as Taiwan and Tibet in an effort to appease the Chinese government.[60] Fearful of restrictions on their operations in China United States aviation companies Delta, American Airlines and United acceded to the Chinese government's demand that they include references to Taiwan as part of mainland China. The CAC shut down the Marriott hotel group's website and booking application after apparently it 'hurt the feelings of the Chinese people' by listing Taiwan, Hong Kong, Tibet and Macau separately in a customer satisfaction questionnaire.[61] Automaker Mercedes Benz suffered a similar imposition after the company had featured a quote from the Dalai Lama in an advertisement on Instagram.[62]

This trend of the increasing acceptability of a 'walled internet' that encourages China to command that multinational companies submit

---

presence in private business' *South China Morning Post* 25 November 2018, https://www.scmp.com/economy/china-economy/article/2174811/chinese-communist-party-needs-curtail-its-presence-private (accessed 31 March 2020).

53 Lin (n 52).
54 Feldstein (n 47) 15.
55 Cook (n 20).
56 As above.
57 As above.
58 As above.
59 As above.
60 As above.
61 Woodhams (n 15).
62 Freedom House (n 20).

to its mandate is epitomised by the behaviour of the international technology giant Google.[63] In 2010 the company departed China in protest at China's censorship apparatus. In 2017 there was an outcry among Google employees after media reports that the company's scheme had been unearthed to introduce a censored search and mobile news service specifically for the Chinese market code-named Project Dragonfly, which pairs users' accounts with their personal telephone numbers and eliminating anonymity.[64] This application evidently was developed to allow Google to return to the Chinese market having appeased the dictates of Chinese censorship, further entailed barring search results and compiling a censorship blacklist of topics such as 'free speech', 'protests', 'democracy', 'human rights' and 'religion'.[65] Moreover, Chinese security services which routinely target dissidents, activists and journalists would have unfettered access to user data that Google stored on the Chinese mainland.[66] These concessions potentially make Google complicit in human rights abuses.

After the disclosure of Google's secret Chinese search engine project some high-profile employees resigned in protest.[67] One of these is Jack Poulson, a senior Google research scientist, who in his letter of resignation stated that it was his

> ethical responsibility to resign in protest of the forfeiture of our public human rights commitments … Due to my conviction that dissent is fundamental to functioning democracies, I am forced to resign in order to avoid contributing to, or profiting from, the erosion of protection for dissidents … I view our intent to capitulate to censorship and surveillance demands in exchange for access to the Chinese market as a forfeiture of our values.[68]

More than 1 400 of Google's employees signed a petition in which they demanded that an ombudsman be appointed to assess the 'urgent moral and ethical issues' raised by the company's censorship plan.[69]

In a similar vein in 2018 Apple removed more than 600 applications from its mobile store that previously enabled Chinese users to access

63 Woodhams (n 15).
64 Freedom House (n 20).
65 Qiang (n 7) 63; R Gallagher 'Google China prototype links searches to phone numbers' *The Intercept* 14 September 2018, https://theintercept.com/2018/09/14/google-china-prototype-links-searches-to-phone-numbers/ (accessed 18 February 2020).
66 Gallagher (n 65).
67 Cook (n 20).
68 As quoted in Gallagher (n 65).
69 As quoted in Gallagher (n 65).

websites that had been blocked by the Chinese government.[70] In 2016 it was revealed that Facebook clandestinely had been developing software that could ensure that users in China would not receive certain posts in their newsfeeds, Facebook's efforts undoubtedly were geared to satisfy Beijing's desire for online censorship.[71]

If Facebook enters and Google re-enters the Chinese market, these actions exemplify Beijing's effective advancing of 'internet sovereignty'.[72] The supine acquiescence of international companies in satisfying Beijing's requirements only strengthens the Xi regime's effort to recast the international rules on internet regulation.[73]

Moreover, as both Chinese and international companies to an increasing degree mollify this authoritarian regime, the human toll their behaviour causes continues to mount.[74] For populations in the crosshairs such as activists, religious believers, and ethnic minorities the effect of their self-serving has been calamitous.[75] Censorship of controversial subject-matter (Taiwan, Tibet, Xinjiang and the 1989 Tiananmen square massacre, for example) and surveillance serve to conceal or, worse, aggravate gross violations of human rights including mass detentions, torture and extra-judicial killings.[76] On a daily basis the Chinese government withholds vital information from the public[77] and at the same time curtails the freedom of the Chinese people to discuss events in their country or the policies of the government. [78]

4 Chinese technology in Africa

China is massively involved in circumstances in Africa as Chinese companies trade with and invest in African countries.[79] Some comments accuse Chinese aid of assisting in propping up totalitarian governments, of building infrastructure of poor quality, employing workers brought from China and of concentrating its 'benevolence' principally on countries with oil, minerals and other natural resources

70 Cook (n 20).
71 Qiang (n 7) 62.
72 Qiang (n 7) 63.
73 Freedom House (n 20).
74 Cook (n 20).
75 As above.
76 As above.
77 As above.
78 As above.
79 AL Dahir 'China "gifted" the African Union a headquarters building and then allegedly bugged it for state secrets' *Quartz Africa* 30 January 2018, https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/ (accessed 27 January 2020).

of which China has a shortage,[80] and at the same time 'saddling countries with more debt than they can ever repay'.[81]

China's presence in Africa grew steadily over a period of 20 years but escalated dramatically in 2013 following President Xi Jinping's unveiling of the BRI, an ambitious trillion dollar soft-power international development strategy directed at extending Beijing's influence on host countries by providing bilateral loans and building infrastructure projects.[82] Most countries on the African continent enthusiastically embrace the BRI[83] with the result that China has emerged as the largest source of financing for infrastructure projects in Africa[84] and everywhere evidence of its influence is on display as African governments embrace the offer of Chinese expertise and soft loans.[85]

China sponsors thousands of the next generation of African leaders, bureaucrats, students and entrepreneurs to undergo training and education in China.[86] Chinese financial support of post-graduate and post-doctoral African students is unparalleled;[87] each year China hosts tens of thousands of university undergraduate and post-graduate students from Africa and annually the Chinese government offers thousands of scholarships to African students.[88] The *Hanban* (the Chinese Language Council) has established 59 Confucius Institutes in Africa which inculcate the Chinese language and culture.[89]

---

80 Dahir (n 79). See also J Eisenman & J Kurlantzick 'China's Africa strategy' (2006) *Current History* 219-224.

81 However, according to supporters 'China has brought expertise on important development issues and has a much better sense than Western nations of the challenges involved in raising standards of living'. A Roussi 'China's bridge to Africa' 569 *Nature* 16 May 2019 326.

82 Roussi (n 81) 326. For a more detailed exposition of the geopolitical implication of the BRI, see A Chatzky & J McBride 'China's massive belt and road initiative' *Council on Foreign Relations* 28 January 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative (accessed 23 March 2020).

83 Thus far 39 African countries and the African Union Commission have entered into BRI cooperation agreements, with others expected to follow suit. Roussi (n 81) 325.

84 China funds one in five infrastructure projects on the continent. Roussi (n 81). See also B Gill, C Huang & JS Morrison 'Assessing China's growing influence in Africa' (2007) 3 *China Security* 9; B Sautman & Y Hairong 'Friends and interests: China's distinctive links with Africa' (2007) 50 *African Studies Review* 80.

85 Roussi (n 81) 325; Gill et al (n 84) 6.

86 Dahir (n 78); Gill et al (n 84) 6.

87 Mohamed Hassan, president of the World Academy of Sciences and a Sudanese mathematician, as cited in Roussi (n 81) 326. Hassan continued: 'When it comes to training a new generation of African scholars, [the Chinese] are doing a marvellous job. They are doing better than any other country for Africa.' As quoted in Roussi (n 81) 326.

88 Eg, China hosted almost 62 000 African university and post-graduate students in 2016, and in 2015 the Chinese government offered 8 470 scholarships to African students. Roussi (n 81) 326.

89 Roussi (n 81) 326; Eisenman & Kurlantzick (n 80) 221.

The BRI includes a major emphasis on information technology.[90] In relation to the promotion of technology in Africa Chinese ventures are unrivalled.[91] The extent of Chinese technological penetration of the African continent is encompassing;[92] vast numbers of the population rely fundamentally on Chinese companies for their telecommunications and digital services.[93]

China Telecom has plans to lay a 150 000 kilometre-long fibre optic network which will operate in 48 African states.[94] Transsion Holdings, a Shenzhen-based company, overtook Samsung to become the leading smart phone provider in Africa;[95] Huawei, the Chinese telecommunications giant, built 70 per cent of the 4G network and most of the 2G and 3G networks on the continent easily out-competing its European rivals.[96] The Kenyan government appointed Huawei as the principal advisor for its 'master plan' in respect of information and communication technologies.[97]

The Chinese telecommunications conglomerate ZTE provides the Ethiopian government with the infrastructure that enables it to monitor and exercise surveillance over the communications of opposition activists and journalists.[98] Another Chinese company, H3C, won the contract to construct a Nigerian airport's new telecommunications network.[99] Hikvision established an office in Johannesburg[100] and through a local video surveillance provider

90 M Abramowitz & M Chertoff 'The global threat of China's digital authoritarianism' *The Washington Post* 1 November 2018, 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 (n 20).
91 Roussi (n 81) 326.
92 See D Gershgorn 'Africa is building and AI industry that doesn't look like silicon valley' *Medium* 25 September 2019, https://onezero.medium.com/africa-is-building-an-a-i-industry-that-doesnt-look-like-silicon-valley-72198eba706d (accessed 2 March 2020).
93 A Hawkins 'Beijing's Big Brother tech needs African faces' *Foreign Policy* 24 July 2018, 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' *The Washington Post* 29 November 2017, https://www.washingtonpost.com/opinions/china-has-a-plan-to-rule-the-world/2017/11/28/214299aa-d472-11e7-a986-d0a9770d9a3e_story.html (accessed 5 March 2020).
95 Hawkins (n 93); L Chutel 'China is exporting facial recognition software to Africa, expanding its vast database' *Quartz Africa* 25 May 2018, https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/ (accessed 18 February 2020). Also, two of the three most popular smartphone brands are Chinese. Roussi (n 81) 326.
96 MacKinnon (n 18).
97 Abramowitz & Chertoff (n 90).
98 Hawkins (n 93); Polyakova & Meserole (n 4).
99 Freedom House (n 20).
100 Hawkins (n 93).

in 2019 rolled out 15 000 cameras throughout the Johannesburg metropolitan area.[101]

Despite the warning by the United States not to contract with Huawei because of alarm about cyber-security, the company has had great success in Africa indicating that governments consider imperative greater internet access.[102] Huawei's popularity is enhanced by the inducement that its construction of 4G networks usually is funded by Chinese banks through so-called 'soft loans' offering below market rates of interest and longer repayment periods than loans from international financial institutions.[103] The fact that through its proxies the Chinese government is the only eager provider of finance for internet connectivity on the continent gifts it significant leverage over African governments.[104]

5 The Chinese model of 'internet sovereignty' in Africa

As stated, China continues to develop and to fine-tune its internal censorship apparatus as well as exporting this model around the world. The Chinese notion of 'internet sovereignty' perhaps unsurprisingly offers an alluring prospect for many governments, including in Africa, that seek to combat the potentially-destabilising effects of a free internet and to stifle freedom of expression instead of embracing a notion of the internet that eliminates borders. To an increasing extent these African countries implement rules and erect obstacles that hinder its working in the name of national sovereignty but with the purpose of allowing governments to inspect and control their citizens' data at will.[105]

By means of seminars and through official visits the Chinese government actively advises the media elite and government officials in countries in the path of the BRI to accept its lead in adopting internet sovereignty. According to Freedom House in 2018 'increased activity by Chinese companies and officials in Africa preceded the passage of restrictive cybercrime and media laws in Uganda and Tanzania' (China is these countries' largest trading partner.[106]

101 Swart (n 44).
102 MacKinnon (n 18).
103 As above.
104 '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 (n 18).
105 Freedom House (n 20).
106 As above; Woodhams (n 15).

At an event sponsored by the government of Tanzania and the CAC of China, the Tanzanian deputy minister of communication stated:[107]

> Our Chinese friends have managed to block such media in their country and replaced them with their home-grown sites that are safe, constructive and popular. We aren't there yet, but while we are still using these platforms we should guard against their misuse.

He went on to declare that 'the government must find ways to ensure that while a person is free to say anything there are mechanisms to hold them accountable for what they say'.[108] The suggestion in this formulation is that internet sovereignty is compatible with the acceptance of freedom of expression but in a modified form in the limits of the law.

Woodhams points out that it is impossible not to conclude that internet sovereignty is the very 'antithesis of freedom of expression, particularly if the law strictly [proscribes] what can and cannot be said'.[109] As a case in point, the leader of the opposition in Tanzania, who had accused security forces of murdering dozens of herders in a violent skirmish, was arrested in October 2018. It is entirely comprehensible that internet sovereignty is available as a policy tool to silence criticism of a government whose intent is to keep a firm grip on power.[110]

Tanzania has a history of harassing critics of the government and recently introduced a statute governing internet content that relies heavily on the Chinese model.[111] In Tanzania the posting of 'false content' is prohibited; a phrase redolent of the terminology in Chinese law of a prohibition on 'making falsehoods'.[112] The nebulous notion of 'content that causes annoyance' is proscribed in Tanzania in an echo of China's 'destroying the order of society'.[113] The Tanzanian government alleges that this law was propagated in order to crack down on 'moral decadence' similarly to the way 'decadent' material is banned from social media in China.[114] In December 2019 Amnesty International described the introduction by the government of Nigeria of the Protection from Internet Falsehoods, Manipulation and Other Related Matters Bill as a proposal to 'stifle the space for

107 Woodhams (n 15).
108 As quoted in Woodhams (n 15).
109 Woodhams (n 15).
110 As above.
111 Hawkins (n 93).
112 As above.
113 As above.
114 Hawkins (n 93).

critics, human rights reporting and accountability in the country'.[115] In a way that is similar to the sweeping provisions in China's Cyber-Security Law the Nigerian Bill proposes to prohibit statements online that are deemed 'likely to be prejudicial to national security' as well as 'those which may diminish public confidence' in Nigeria's government.[116]

The influence of the Chinese model of internet sovereignty is visible in Zimbabwe in the manner in which it looks to China to provide a model for managing aspects of society including social media and communications.[117] In 2016 President Mugabe heralded China as an exemplar in social media regulation which he hoped Zimbabwe could emulate.[118] The 2017 Cybercrime and Cyber-security Bill criminalises communicating falsehoods online in a copy of the legal rhetoric China uses to stifle dissent.[119] Post-Mugabe the Zimbabwean government shows greater determination to have dominion over all aspects of its digital and public spaces.[120] In January 2019, after days of protests as a result of a 100 per cent increase in fuel prices, the security forces launched a crackdown in which 12 people were killed and 600 were arrested. The Zimbabwe government ordered the first countrywide internet shutdown.[121] This assault on the internet is the government's latest attempt to impose its will on the citizens of Zimbabwe.[122]

Taking their cue from China's digital governance playbook, other African governments also have ordered internet shutdowns as well as the blocking of websites and social media platforms ahead of critical democratic instances such as elections and protests. Internet shutdowns and social media bans have been reported in Chad

115 D Tegegn 'African Union's Revised Declaration on Principles of Access to Information and Freedom of Expression' 13 December 2019 *Amnesty International USA*, https://medium.com/@amnestyusa/african-unions-revised-declaration-on-principles-of-access-to-information-and-freedom-of-2d7d636dddb2 (accessed 9 July 2020).

116 As above.

117 SN Romaniuk & T Burgers 'How China's AI technology exports are seeding surveillance societies globally' *The Diplomat* 18 October 2018, https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/ (accessed 27 January 2020).

118 Hawkins (n 93).

119 As above.

120 'The [new] government has shown zero political will to protect rights.' Jeffrey Smith of Vanguard Africa, as quoted in R Mwareya 'Zimbabwe drifts towards online darkness' *Coda* 26 February 2019, https://www.codastory.com/authoritarian-tech/zimbabwe-drifts-towards-online-darkness/ (accessed 31 March 2020).

121 Partial internet service was restored in February 2019, but social media applications and messaging services, such as Facebook, WhatsApp and Twitter, remained blocked for days longer. Mwareya (n 120).

122 Mwareya (n 120).

(2016), Togo (2017) and Cameroon (2018).[123] The *Financial Times* reports that in the first half of 2019 at least six governments in Africa shut down the internet,[124] and in the Sudan in June 2019, 'as soldiers from a government paramilitary force went on a killing spree in the capital Khartoum, the internet went dark, preventing protesters from documenting the violence on social media'.[125]

Some African governments initiated a method of stifling freedom of expression through the imposition of social media taxes. In 2018 the governments of Uganda, Zambia and Benin serially announced or imposed new taxes on mobile internet users, 'leaving millions of Africans struggling to cover the costs of getting online'.[126] In Uganda the government imposed a daily tax on the use of social media platforms such as Facebook, Twitter and WhatsApp in order to curb what it described as 'idle chatter'.[127] In his 2019 report the United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association stated that the social media tax in Uganda

> disproportionately and negatively impacts the ability of users to gain affordable access to the Internet, and thus unduly restricts their right to freedom of expression and their rights of peaceful assembly and association – particularly so for low-income citizens, for whom purchasing 1 GB of data per month will cost nearly 40 per cent of their average monthly income.[128]

In April 2018, in a blatant attempt to restrict freedom of expression online, the government of Tanzania introduced a so-called 'blogger tax' which requires Tanzanian bloggers, YouTube channel operators and independent website owners to register and pay the exorbitant sum of approximately US $900 per year to publish content online.[129]

In addition to its activities in Tanzania and Uganda, China has cemented trade partnerships with a number of other countries on

123 Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association HR Council UN Doc A/HRC/41/41 (2019) 13.
124 These countries were Chad, Ethiopia, the Democratic Republic of the Congo, Eritrea and Mauritania.
125 D Pilling 'The fight to control Africa's digital revolution' *Financial Times* 20 June 2019, https://www.ft.com/content/24b8b7b2-9272-11e9-aea1-2b1d33ac3271 (accessed 7 July 2020).
126 Only in Benin did protests result in a quick abandonment of the tax plan. Anonymous 'Taxing social media in Africa' *Internet Health Report* 2019 April 2019, https://internethealthreport.org/2019/taxing-social-media-in-africa/ (accessed 8 July 2020).
127 Pilling (n 125).
128 Report of the Special Rapporteur (n 123) 14.
129 'Taxing social media in Africa' (n 126). The Financial Times opined that 'Tanzania's authorities have sought to tax bloggers out of existence'. Pilling (n 12).

the continent, including Egypt, Ethiopia, Nigeria, South Africa and Sudan.[130] Alongside the established practice of providing African governments with the knowledge and technology that enables them to control content in what they declare to be a fight against so-called 'public threats', China in an effort to deflect public criticism equips these developing economies with affordable, dependable and cutting-edge technological infrastructure.[131]

For example, in 2017, as part of the BRI the Chinese artificial intelligence company, Percent Corporation, developed an intelligent system for information visualisation and data analysis to assist the government of Angola in its decision-making process.[132] This system accurately and dynamically records data about the full life cycle of birth, education, marriage and social security of every person, as well as a person's biometric information such as fingerprints and facial image.[133] The system's ostensible purpose is to 'manage population resources',[134] but clearly has great potential in terms of surveillance and as a tool for repression.

In many countries, in light of the costs of developing or acquiring these technologies, the Chinese offer is enticing.[135] For this reason and lured by the inducement of easy loans and investments many African countries have become almost entirely dependent on China for the provision of technology and services[136] and are susceptible to pressure to subscribe to the Chinese notion of 'internet sovereignty'. The grave danger is that as a consequence of the frail nature of democracy in these countries and their less than stellar history in defending human rights, they are open to more than economic lessons.[137]

6 Conclusion

China is active in recasting the global debate on security, freedom and openness through advocating its model of 'internet sovereignty'.[138]

130 Woodhams (n 15).
131 As above.
132 Anonymous 'China-designed big data system aids Angola's intelligent governance' *People's Daily* 24 August 2018, http://en.people.cn/n3/2018/0824/c90000-9493984.html (accessed 31 March 2020).
133 As above.
134 As above.
135 SN Romaniuk & T Burgers 'How China's AI technology exports are seeding surveillance societies globally' *The Diplomat* 18 October 2018, https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/ (accessed 27 January 2020).
136 Romaniuk & Burgers (n 135).
137 As above.
138 As above.

The rapid expansion across Africa of Chinese technology warrants vigilance on the part of democrats.[139] China's activities are conducive to creating a framework by which an increasing number of African countries follow the Chinese technology governance model.[140] This development raises the spectre that the Chinese attitude to state power becomes the dominant model to be followed in implementing security and surveillance in Africa.[141]

There are concerns that Africa could be 'left behind' in the global technology race and the consequent transformation of the economy,[142] but a greater danger is that the developing world runs the risk of becoming passive consumers of technology developed in China or elsewhere that is designed as a fit for different cultures and circumstances.[143]

Africa's nascent technology industry cannot compete globally with that of China or the United States but African countries have local leverage in setting policy. It is more important than ever in this situation that policy makers and legislators are involved in vigorously advocating improvements to the rule of law, transparency and accountability in governance and in the private sector.[144]

In order to enjoy a political discourse that is free and democratic, telecommunications and internet legislation and regulation must be transparent, accountable and open to reform.[145] In the absence of fundamental guarantees the forms of dissent and opposition and the activities of reform movements face increasing and crushing opposition reinforced by the progressively more ingenious and sophisticated forms of surveillance and censorship.[146]

Fortunately, in these circumstances there can be reliance on a well-established international human rights framework as well as access to a robust regional human rights system that is available as a bulwark against the tide of dependence on Chinese repressive systems built into technology. The African Union (AU) has taken proactive steps to develop rules and common practices on digital governance for the continent. In late 2019 the African Commission on Human and

139 See Qiang (n 7) 61.
140 Romaniuk & Burgers (n 135).
141 As above.
142 L Andersen et al 'Human rights in the age of artificial intelligence' *Access Now* November 2018, https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf (accessed 2 March 2020).
143 As above.
144 MacKinnon (n 21) 44.
145 As above.
146 As above.

Peoples' Rights (African Commission) published a revised Declaration of Principles on Freedom of Expression and Access to Information in Africa (Declaration).[147] Principles 37 to 42 of the Declaration specifically address the rights to freedom of expression and access to information in the digital age which had not been addressed in the 2002 Declaration on the Principles of Freedom of Expression in Africa.

The Declaration reaffirms the fundamental importance of freedom of expression and access to information to individual human rights and as cornerstones of democracy and a means to ensure respect for other human rights.[148] Principle 37 obligates states to facilitate these rights online and to adopt laws and policies to provide universal, equitable, affordable and meaningful access to the internet without discrimination to everyone, specifically including marginalised groups and children.[149]

Principle 38 of the Declaration speaks directly to domestic legislation that is based on the China model that restricts freedom of expression, as well as reflecting on the use of internet shutdowns and social media taxes. It prohibits states from interfering with the right of individuals to seek, receive and impart information by way of digital technologies through measures such as the removal, blocking or filtering of content unless interference is justifiable under international human rights law.[150] Principle 38 explicitly states that states may not engage in the disruption of access to the internet by segments of the public or an entire population.[151] In addition, states may impose only taxes, levies and duties on internet end users that do not undermine universal, equitable, affordable and meaningful access to the internet and which are justifiable under international human rights law.[152]

To discourage practices such as those favoured by the government of China to force international and domestic internet search engines and social media platforms to block certain content and otherwise

147 The Declaration was adopted by the African Commission at its 65th ordinary session held from 21 October to 10 November 2019 in Banjul, The Gambia, and replaces its 2002 Declaration of Principles on Freedom of Expression in Africa. The Declaration is a soft law instrument that interprets article 9 (right to receive information and free expression) of the African Charter on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019), https://www.achpr.org/presspublic/publication?id=80 (accessed 9 July 2020).
148 Preamble to the Declaration (n 147).
149 Principles 37(1), (3), (4) and (5) of the Declaration (n 147).
150 Principle 38(1) of the Declaration.
151 Principle 38(2) of the Declaration.
152 Principle 38(3) of the Declaration.

abide by domestic censorship laws, Principle 39 of the Declaration provides that states require that internet intermediaries enable access to all internet traffic equally without discrimination based on the type or origin of content.[153] States also shall require that internet intermediaries do not interfere with the free flow of information by blocking or giving preference to particular internet traffic.[154] States further may not require internet intermediaries to proactively monitor or filter content or, except under strict conditions, remove content.[155]

Under Principle 39(6) states may not demand that internet intermediaries develop search engines and chat rooms specifically to comply with domestic censorship laws such as Google proposed to do by means of Project Dragonfly, its secret search engine for the Chinese market:

> States shall ensure that the development, use and application of artificial intelligence, algorithms and other similar technologies by internet intermediaries are compatible with international human rights law and standards, and do not infringe on the rights to freedom of expression, access to information and other human rights.

In October 2019 a specialised technical committee on communication and information technologies of the AU held at Sharm El Sheikh, Egypt (2019 Sharm El Sheikh Declaration)[156] recognised that achieving digital transformation in Africa requires political commitment at the highest level with the intention of aligning policies and sector regulation and involving a massive scaling-up of investment and dedication of resources.[157] The specialised technical committee noted that the harmonisation of legal and regulatory frameworks is a prerequisite for the creation of a common digital single market, and that internet and digital infrastructure is an essential component in the development of Africa's digital ecosystem.[158]

The geopolitical reality is that with such large sections of the continent's telecommunications infrastructure under Chinese control, African states will find it difficult to disentangle themselves from China.[159] If African governments fail to advance values and interests in conformity to the wishes of their people, including freedom of expression, free enterprise and the rule of law, with boldness equal

153 Principle 39(1) of the Declaration.
154 As above.
155 Principles 39(2) & (4) of the Declaration.
156 AU/STC-CICT-3/MIN//Decl. https://au.int/en/decisions/2019-sharm-el-sheikh-declaration-stc-cict-3 (accessed 9 July 2020).
157 Preamble to the 2019 Sharm El Sheikh Declaration (n 156).
158 As above.
159 MacKinnon (n 18).

to the brazen attempt to impose others, the 'China model' of digital governance by default will become the 'Africa model', largely because of inaction and complacency.[160]

African countries are called upon to critically appraise the values, explicit and implicit, embedded in the technology they acquire from China.[161] African governments, policy makers and technology entrepreneurs must keep in mind considerations of the kind of society they desire in contrast to the kind of society driven by the technology they acquire from China.[162] Chinese investment and technological innovation should not result in the resurrection of the spectre of neo-colonial exploitation.[163] A people hoping to reap the benefit of the Fourth Industrial Revolution for the betterment of the quality of their life[164] creates the imperative that they play a central role in determining crucial technological issues for the continent.[165] Their voice must be prioritised at every step, from designing to developing to implementing technology, and – most importantly – in establishing the policy and legal framework within which these technologies operate.

160 See See D Curran 'Facial recognition will soon be everywhere. Are we prepared?' *The Guardian* 27 May 2019, https://www.theguardian.com/commentisfree/2019/may/21/facial-recognition-privacy-prepared-regulation (accessed 6 February 2020); Freedom House (n 17).
161 See A Birhane 'The algorithmic colonization of Africa' *Real Life* 18 July 2019, https://reallifemag.com/the-algorithmic-colonization-of-africa/ (accessed 2 March 2020).
162 As above.
163 Gershgorn (n 92).
164 Para 2 of 2019 Sharm El Sheikh Declaration (n 156).
165 Birhane (n 161).