China's Neocolonialism in the Political Economy of A.I. Surveillance[1]

Sharma, Ishan[2]

The result of neocolonialism is that foreign capital is used for the exploitation rather than for the development of the less developed parts of the world.
Kwame Nkrumah
Neo-Colonialism: The Last Stage of Imperialism[3]

The Enlightenment started with essentially philosophical insights spread by a new technology. Our period is moving in the opposite direction. It has generated a potentially dominating technology in search of a guiding philosophy.
Henry A. Kissinger[4]

I think we don't even quite understand the full scale of the problem that we are dealing with when it comes to Chinese surveillance technology when it is exported.
Samantha Hoffman (2019)
Australian Strategic Policy Institute[5]

---

[2] Ishan Sharma is a recent graduate of Cornell University and Fall 2020 Herbert Scoville Jr. Peace Fellow where he will be writing on issues related to international peace and security. His specific research interests lie in the field of emerging technology and geopolitics, including resurgent digital authoritarianism, global data and Internet governance, and the strategic A.I. power struggle between China and the United States.

[3] Kwame Nkrumah, *Neo-Colonialism: The Last Stage of Imperialism* (London: Thomas Nelson & Sons, 1965), 1.

[4] Henry A. Kissinger, "How the Enlightenment Ends," *The Atlantic,* June 2018, https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/

[5] Arjun Kharpal, "China's Surveillance Tech is Spreading Globally, Raising Concerns About Beijing's Influence," *CNBC,* October 8, 2019, https://www.cnbc.com/2019/10/08/china-is-exporting-surveillance-tech-like-facial-recognition-globally.html

INTRODUCTION

In the Fourth Industrial Revolution of data, artificial intelligence, and the Internet of Things, exploitation will manifest itself in new ways. While the United States dominates the artificial intelligence marketplace, China occupies a close second place. This analysis focuses on China's strategic decision to specialize in artificially intelligent surveillance systems (AISS) for geopolitical aims. This paper reviews characteristics of 19th century British and French colonial enterprises, identifying shared practices of exploitation and providing a framework for analyzing modern day examples in our rapidly developing technological environment.

China's State Council has declared that it will become the world leader in artificial intelligence by 2030.[6] Aside from its volume of data, China actually lags far behind the United States in the artificial intelligence race.[7] However, China is optimistic that its massive data repositories will usher in technological primacy. China's access to data has allowed it to become a leader in exporting AISS, a technology that can quantify and dismantle budding political opposition, closely monitor extremism, and provide critical information infrastructure. In short, AISS meets a critical security and stability demand of almost all countries today. In the past year alone, the reported number of countries implementing China's AISS increased from eighteen to sixty-three.[8] Furthermore, with the world awestruck by the rapid spread of COVID-19, demand for AISS is likely to only increase as East Asian countries demonstrate the technology's application for the current and future outbreaks.[9]

While China does export AISS to developed, liberal democracies, most of its exports are delivered to developing countries. In turn, China uses its network of importing countries for strategic purposes. A "foreign policy

[6] Jeffrey Ding, "Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI" (report, Future of Humanity Institute, Oxford University, March 2018), 10, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

[7] Ibid., 29

[8] Steven Feldstein, "The Global Expansion of AI Surveillance," (working paper, Carnegie Endowment for International Peace, Washington DC, September 17, 2019), 1, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

[9] Nicholas D. Wright, "Coronavirus and the Future of Surveillance: Democracies Must Offer an Alternative to Authoritarian Solutions," *Foreign Affairs,* April 6, 2020, https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance

aimed at cyberspace dominance," China's export-specialization in AISS grants unparalleled access to data resources and markets, while also shaping favorable international norms. [10] China further exploits this asymmetric exchange by convincing importing countries that their best interests are dutifully considered by its surveillance systems. Such practices can and should be considered part of a new form of exploitation.

The following literature review stresses the connection between literature on China's historical relationship to the neocolonialist tradition, the importance of data in modern artificially intelligent systems, and China's current AISS exportation practices. While the literature on China's neocolonialism primarily focuses on its historical engagement with Africa, this section will also indicate how such neocolonialist practices have been updated to conform to international normative constraints.

The third section of the paper will build the theoretical foundation of the neocolonialist claim. The paper qualifies this framework in China's case, noting that its neocolonialist engagements remain largely constrained by international norms of sovereignty. Nevertheless, this paper contends that the presence of some mutual benefits in the interaction between China and its import-empire should not acquit China of the neocolonialist label. Next, it will investigate the present linkages drawn between China's Belt and Road Initiative (BRI) and accounts of 19th century British and French colonialism. From these associations, this section will distill four key elements of colonialism: extraction of resources, pursuit of unsaturated markets, desire for global prestige, and altruistic rhetoric. Finally, these characteristics will be mapped onto China's present modern-day exportation of AISS.

The paper will conclude by calling for a more comprehensive conception of neocolonialism in the digital world. It will also recommend the use of the United States as a comparative case to contextualize normative forms of exploitation in the geopolitical, artificial intelligence marketplace.

LITERATURE REVIEW

To date, literature on the topic of China and AISS has been sparse, and

[10] Arthur E. Gwagwa, "How China's Artificial Intelligence is Shaping Geopolitical and Geoeconomic Global Order," *Medium,* April 2, 2019, https://medium.com/@arthurgwagwa/how-chinas-artificial-intelligence-is-shaping-geopolitical-and-geoeconomic-global-order-fb7fa341bd3c

most falls into one of two categories. On the one hand, China's actions are framed as an effort to exert global political influence and establish regional security, since the exportation of AISS encourages countries to fall in line with China's own authoritarian tendencies and preferred international norms. On the other hand, China's actions are perceived as driven by market-based incentives to export AISS, given the ongoing battle with the United States for global market hegemony. Existing literature thus fails to adequately draw a nexus linking the political and economic incentives behind China's AISS exportation. As a result, neocolonialist literature largely neglects to identify modes of Chinese exploitation beyond foreign direct and trade investments in Africa. When viewed from the perspective of the international political economy, China's AISS exportation emerges as a profoundly global, neocolonialist narrative.

Chinese Neocolonialism

Neocolonialist literature surrounding China almost entirely focuses on its development in Africa, and is generally divided into two schools—Sino-pessimism and Sino-optimism. Sino-pessimists, such as Lee, contend that China's investments in Africa largely exploit natural resources and undermine democracy.[11] They point to literature indicating that the degree of Chinese foreign direct investment in services is correlated with recipient countries' natural resources.[12] Zhao, for example, notes that "the Chinese government worked with any government that could help secure its investments in mining and drilling rights, including those accused of rampant corruption or severe human rights violations."[13]

Sino-optimists, in contrast, view Chinese engagement in Africa as welcome.[14] In fact, calling Chinese investments in Africa 'neocolonialist' may be viewed as quite ironic, since China has deliberately sought to distinguish itself

---

[11] Margaret C. Lee, "The 21st Century Scramble for Africa," *Journal of Contemporary African Studies* 24.3 (2006): 303-330, https://doi.org/10.1080/02589000600976570; Chibuzo N. Nwoke, "The Scramble for Africa: a Strategic Policy Framework," *Nigerian Journal of International Affairs* 33. 2 (2007): 31-55.

[12] Chen Wenjie, David Dollar, and Tang Heiwai, "Why is China Investing in Africa? Evidence from the Firm Level," *The World Bank Economic Review,* 32.3 (2018): 610, 612, 628, https://doi.org/10.1093/wber/lhw049

[13] Zhao Suisheng, "A Neo-Colonialist Predator or Development Partner? China's Engagement and Rebalance in Africa," *Journal of Contemporary China* 23.90 (2014): 1039, https://doi.org/10.1080/10670564.2014.898893

[14] Li Anshan, "China and Africa: Policy and Challenges," *China Security* 3.3 (2007): 68-94, http://cpfd.cnki.com.cn/Article/CPFDTOTAL-BDFZ201305003010.htm

from the West as a non-interventionist deal-maker.[15] As Lim argues, unlike the history of Western investments, China's devotion to infrastructure projects fills an important development gap in Africa.[16] It also perpetuates the narrative that China represents a trustworthy actor with "no history of enslavement, colonization, financing coups against unfriendly African regimes or deploying military forces in support of its foreign policies."[17] Instead, China's infrastructure investments are exchanged for resources, largely mirroring its own positive, oil-exchange experiences with Japan in the 1970s.[18] Moreover, China's investments are especially attractive to African nations, according to some scholars, because the deals, unlike those with the West, are claimed to come without strings attached.[19] China's recent decisions to establish special economic zones in several African countries and move growth-stimulating manufacturing facilities to sub-Saharan Africa are allegedly suggestive of long-term regional interests, as opposed to quick-fix, short-term projects evident in the post-colonial period.[20]

However, despite China's propagandistic non-interventionism principle—its purported willingness to conduct business without involving itself in the internal affairs of countries—reality tells a different story. In times of crisis, when investments are threatened, China has shown that it will interfere. For example, China provided weapons to Sudan for use against Darfur rebels, deployed the first Chinese battalion in Africa in South Sudan, and most recently acquired a military base in Djibouti.[21] Likewise, China's historical practices have

---

[15] Zhao, "A Neo-Colonialist Predator or Development Partner?," 1036-37; Alvin C-H. Lim, "Africa and China's 21st Century Maritime Silk Road," *Asia-Pacific Journal* 13.11.3 (2015): 5-6, https://apjjf.org/-Alvin-Cheng-Hin-Lim/4296/article.pdf

[16] Lim, "Africa and China's 21st Century Maritime Silk Road," 6.

[17] Zhao, "A Neo-Colonialist Predator or Development Partner?," 1036.

[18] Lim, "Africa and China's 21st Century Maritime Silk Road," 3.

[19] Richard Aidoo and Steven Hess, "Non-Interference 2.0: China's Evolving Foreign Policy towards a Changing Africa," *Journal of Current Chinese Affairs* 44.1 (2015): 108, 118, https://doi.org/10.1177/186810261504400105

[20] Zhao, "A Neo-Colonialist Predator or Development Partner?," 1036-37; Lim, "Africa and China's 21st Century Maritime Silk Road," 3; Timothy S. Rich and Sterling Recker, "Understanding Sino-African Relations: Neocolonialism or a New Era?" *Journal of International and Area Studies* 20.1 (2013): 62, https://www.jstor.org/stable/43111515

[21] Osman Antiwi-Boateng, "New World Order Neo-Colonialism: A Contextual Comparison of Contemporary China and European Colonization in Africa," *Africology: The Journal of Pan African Studies* 10.2 (2017): 186, https://www.jpanafrican.org/docs/vol10no2/10.2-13-Antwi-Boateng.pdf; Karen Allen, "What China Hopes to Achieve with First Peacekeeping Mission," *BBC News,* December 2, 2015, https://www.bbc.com/news/world-africa-34976580

revealed a similar pattern of intervention. China has intervened by providing military equipment and training to the FNLA and UNITA liberation movements in Angola and southern Africa and to Mozambique's government during its civil war in 1977.[22] The paradox of conflicting, recent accounts of China's (non) interventionism are suggestive of a complex, but disingenuous commitment to the development of its host countries.

Artificially Intelligent Surveillance Systems

As Wright argues, artificial intelligence involves the "the analysis of data to model some aspect of the world, where inferences from these models are then used to predict and anticipate possible future events"—essentially, systems that "learn from data in order to respond intelligently to new data."[23] Known as the "deep learning revolution," two 2012 AI breakthroughs in particular have enabled the rapid capacity for computers to learn independently and effectively.[24] First, using the Imagenet data set, a repository of over 1.2 million images, neural networks were able to classify images with a significantly lower error rate compared to previous technology.[25] Second, neural network algorithms built off a large set of pixels and game scores data sets from Atari computer games were able to successfully operate as well as professional human gamers.[26] These advances eventually culminated in the world-famous victory of AlphaGo over a world-class human Go player, a feat only possible after AlphaGo studied some 100 million game types.[27] Data, then, is

[22] Indira Campos and Alex Vines, "Angola and China: A Pragmatic Partnership" (paper, Center for Strategic and International Studies Conference on "Prospects for Improving U.S.-China-Africa Cooperation," Washington DC, December 5, 2007, published March 2008), 2, https://www.csis. org/analysis/angola-and-china-pragmatic-partnership; Paula C. Roque, "China in Mozambique: A Cautious Approach Country Case Study," (report, SAIIA Occasional Paper 23, South African Institute of International Affairs, Braamfontein, South Africa, January 2009), 2, https://media. africaportal.org/documents/SAIIA_Occasional_Paper_no_23.pdf

[23] Nicholas D. Wright, "The Technologies: What Specifically is New?," in Shazeda Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," ed. Nicholas D. Wright (white paper, Strategic Multilayer Assessment Periodic Publication, U.S. Department of Defense, Washington DC, December 2018), 2, https:// nsiteam.com/social/wp-content/uploads/2019/03/AI-China-Russia-Global-WP_FINAL2_ fromMariah8mar2019_ndw11mar2019.pdf

[24] Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy," (report, American Civil Liberties Union, New York, June 17, 2019), 6-8, https://www.aclu.org/sites/ default/files/field_document/061819-robot_surveillance.pdf

[25] Wright, "The Technologies," 3-4.

[26] Ibid.

[27] Ibid.

crucial to the ability of such systems to learn and operate.

AISS is the result of a technological intersection between the rapid global deployment of surveillance cameras and developments in AI data analytics.[28] The former provides an endless supply of progressively powerful, ultra-high-resolution footage, whereas the latter automatically scans troves of such data to learn correct and incorrect recognition of objects and people.[29] Surveillance cameras are therefore an integral part of AISS. China, for example, has increased the number of domestic surveillance cameras by 70% in the past three years alone. Furthermore, market analytics predict that by the end of 2021, over 1 billion cameras will be in use worldwide.[30] However, an average of only 2% of footage collected by surveillance cameras is observed, and even less is analyzed.[31]

AI data analytics thus represents a paradigm shift, since surveillance cameras are increasingly becoming augmented with the algorithmic ability to intelligently detect loiterers, trespassers, missing objects, and demographic features.[32] While "complex background clutters, varying illumination conditions, uncontrollable camera settings, severe occlusions and large pose variation,"[33] remain complications for AI data analytics, it still provides a revolutionary breakthrough in processing "oceans of data," compared to manual analysis of digital content.[34] Presently, the universe of data doubles every two years—an "information Big Bang."[35] Data analytics algorithms have subsequently been enabled with the capacity to draw linkages from real-time surveillance footage to individual identities. As more data continues to be collected, a "wealth of personal data," such as online searches and purchases, as well as social media

---

[28] Michael Kwet, "The Rise of Smart Camera Networks, and Why We Should Ban Them," *The Intercept*, January 26, 2020, https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/

[29] Stanley, "The Dawn of Robot Surveillance," 3, 6-8.

[30] Kwet, "The Rise of Smart Camera Networks."

[31] David Tang et al., "Seeing What Matters: A New Paradigm for Public Safety Powered by Responsible AI," (report, Accenture Strategy and Western Digital Corporation, 2018), 4. https://www.accenture.com/_acnmedia/pdf-94/accenture-value-data-seeing-what-matters.pdf

[32] Stanley, "The Dawn of Robot Surveillance," 5-9.

[33] Xu Jing et al., "Attention-Aware Compositional Network for Person Re-Identification," (paper, 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, June 18-22, 2018), 2119. https://doi.org/10.1109/CVPR.2018.00226

[34] Stanley, "The Dawn of Robot Surveillance," 7-9.

[35] Cameron F. Kerry, "Protecting Privacy in an AI-Driven World," *Brookings Institution*, February 10, 2020, https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

communications, could be brought into the AI data analytics fold. [36] While in 2018, only 5% of cameras were equipped with data analytics capabilities, by 2025, over 70% of surveillance cameras worldwide are projected to possess the capacity to interpret behavior in real-time.[37]

Though such huge data reservoirs are necessary for algorithmic development, a fundamental bottleneck of AISS is the availability of *labeled* training data. Such "ground truth" data trains the deep learning neural network to distinguish between and recognize relevant objects accurately.[38] For example, training an AISS system to differentiate between a child's face and an adult's face requires a dataset of images or videos for each category and labeled as such (e.g. Child Faces vs. Adult Faces). The labeling of datasets has proven to be "laborious and expensive," which is why ground truth data is a "vital currency in the computer vision field."[39] However, AISS ground truth data—the property records, birthdates, and medical records of citizens—is usually in the hands of governments, not companies designing the technology.[40] International access to governments' citizen ground truth data thus proves especially lucrative for exporting AISS around the world.

At present, over 75 countries are known to be utilizing AISS in one of three forms: smart cities, facial recognition systems, and smart policing. Smart cities exist in 56 countries, and have been described by the World Bank as technological urban centers responding to information collected from "thousands of interconnected devices."[41] While the term has been used ambiguously to define a range of infrastructure, smart cities are becoming "spaces of systematic data collection…[that] have been increasingly surveilled."[42] In the Australian city of Darwin, a network of "smart" devices—from street lights to environmental sensors and video cameras—consistently collect information on the residents.[43]

---

[36] Stanley, "The Dawn of Robot Surveillance," 19-21.
[37] Tang et al., "Seeing What Matters," 10.
[38] Wright, "The Technologies," 5.
[39] Stanley, "The Dawn of Robot Surveillance," 8.
[40] Wright, "The Technologies," 5.
[41] Feldstein, "The Global Expansion of AI Surveillance," 1; Victor Mulas, Eva Clemente, and Arturo Muente-Kunigami, "Smart Cities," *World Bank*, January 8, 2015, https://www.worldbank.org/en/topic/digitaldevelopment/brief/smart-cities
[42] "Smart Cities: Utopian Vision, Dystopian Reality," (report, Privacy International, October 31, 2017), 19, http://www.privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality
[43] Jathan Sadowski, Anna Carlson, and Natalie Osborne, "Darwin's 'Smart City' Project is About Surveillance and Control," *The Conversation,* February 4, 2020, https://theconversation.com/darwins-smart-city-project-is-about-surveillance-and-control-127118

Sadowski et. al explain that the "vision" of smart cities—a world of convenience, information efficiencies, and security—ignores the deep nexus to "older practices of colonial control," like the targeting of minority communities.[44] They describe citizens of such cities as "'captured,' both by surveillance that collects data and by authorities who control territory."[45]

Facial recognition systems which combine still-image datasets of human faces with real-time footage of citizens to find a biometric match are used in at least sixty-four countries, and are already "actively incorporating facial recognition systems in their AI surveillance programs."[46] The infrastructure of exports provided by China involves the deployment of thousands of high-definition cameras across a city.[47] For example, these are used in Malaysia by security officials equipped with facial recognition body cameras, and in Kenya to process the inflow of data at a centralized police facility.[48]

Smart policing relies on training artificial intelligence systems with large quantities of data including information on "geographic location, historic arrest levels, types of committed crimes, biometric data, [and] social media feeds" to respond to and even predict criminal activity.[49] In short, it is the application of data for powerful, systematic enforcement. In the United States, 60 police departments use PredPol, an artificially intelligent system trained on continuously updated crime data sets, including the times and locations of past crimes, to predict in which neighborhoods serious crimes are anticipated within a given time frame.[50] Given the racial and socioeconomic bias inherent in historical incarceration datasets, such algorithms could be used to target minority communities. Indeed, as Rieland argues, a tool like PredPol could enable presumptive judgements on the likelihood of crime in a given neighborhood, creating a reason for more surveillance and police monitoring.[51]

---

[44] Ibid.
[45] Ibid.
[46] Feldstein, "The Global Expansion of AI Surveillance," 23.
[47] "Video Surveillance as the Foundation of 'Safe City' in Kenya," *Huawei,* https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya
[48] Feldstein, "The Global Expansion of AI Surveillance," 23.
[49] Ibid.
[50] Randy Rieland, "Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?" *Smithsonian Magazine*, March 5, 2018, https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-usedpredict-crime-is-it-biased-180968337/
[51] Ibid.

In China, enforcement is even more intensive. The Integrated Joint Operations Platform operates at the data intersection of "CCTV cameras, facial recognition devices, and Wi-Fi sniffers" (devices that eavesdrop on activities or communications within wireless networks).[52] IJOP procures additional data from license plates and identification cards scanned at checkpoints, as well as health, banking, and legal records."[53] As a result, China has been able to systematically target Muslim Uighur populations, who were tracked, arrested, and placed within internment camps for purported "re-education."[54]

Empowered by ground-truth data, facial recognition AISS can categorically alter the power of governments. It could be applied to stay abreast of popular discontent, control mass protests with heat maps, delegitimize electoral opponents with automated, highly personalized disinformation campaigns, and adopt social credit registration systems to reward state support. For the authoritarian, it provides a critical update. When AISS allows for dissent to be quantified, budding uprisings dismantled, and political opposition precluded, there is no longer a costly reliance on the unstable use of military force for repression. For example, civilians, aware that Wi-Fi sniffers may be tracking the amount of time spent on a certain website, in a chat group, or at a location, are likely to avoid any trouble altogether. For context, Schneier writes that, "the exceptionally paranoid East German government had 102,000 Stasi surveilling a population of 17 million: that's one spy for every 166 citizens."[55] But through AI surveillance, the activities of billions of people may be monitored through only a few thousand individuals.[56]

For liberal democracies, AISS also meets the post-9/11 world demands for security. Bush-era policies like Stellarwind have normalized the digital use of surveillance, and with recent terrorist attacks, liberal democracies like France, Germany, and Spain have bought into China's surveillance solutions. In a broader sense, new AI technology offers an elegant alternative to the normative, costly, and labor-intensive forms of surveillance, providing stability and security for almost all regime types.

---

[52] Feldstein, "The Global Expansion of AI Surveillance," 20.

[53] Feldstein, "The Global Expansion of AI Surveillance," 25.

[54] "Data Leak Reveals How China 'Brainwashes' Uighurs in Prison Camps," *BBC News,* November 24, 2019, https://www.bbc.com/news/world-asia-china-50511063

[55] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, United States: W.W. Norton, 2015, 20.

[56] Greg Allen and Taniel Chan, "Artificial Intelligence and National Security" (report, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, MA, July 2017), 93, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

The COVID-19 global pandemic represents the latest iteration of AISS applicability. In China, surveillance cameras are pointed at the apartment doors of those under quarantine, while other surveillance devices are equipped to recognize high-body temperatures in individuals.[57] Recently, the Ministry of Public Security implemented a surveillance tool to account for a mask-wearing public with a facial recognition success rate of 95%.[58] The deployment of numerous technologies to track the spread of the virus could very well become a "catalyst" for normalizing even stricter mass surveillance measures in China and beyond, as a set of countries are already applying technology to enhance COVID-19 containment.[59]

STATUS QUO

China's Relative (Dis)advantage

AI development is expected to add USD 15.7 trillion to global GDP by 2030, a 14% increase.[60] Largely, though, the competition over AI is between the United States and China. AI will critically shape both countries' "interaction in the political, economic, and security arenas," defining the relative "balance of power between them."[61] With a forecasted 26% boost to its GDP from AI developments, China has been clear about its strategy to prioritize the AI industry.[62] China's 2017 Artificial Intelligence Development Plan stipulates that "AI has become a new focus of international competition."[63] Further, by 2025,

---

[57] Arjun Kharpal, "Use of Surveillance to Fight Coronavirus Raises Concerns About Government Power After Pandemic Ends," *CNBC,* March 26, 2020, https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html; "AI and Control of COVID-19 Coronavirus," *Council of Europe*, https://www.coe.int/en/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus

[58] Martin Pollard, "Even Mask-Wearers Can Be ID'd, China Facial Recognition Firm Says," *Reuters,* March 9, 2020, https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL

[59] Arjun Kharpal, "Coronavirus Could Be a 'Catalyst' for China to Boost Its Mass Surveillance Machine, Experts Say," *CNBC,* February 4, 2020, https://www.cnbc.com/2020/02/25/coronavirus-china-to-boost-mass-surveillance-machine-experts-say.html

[60] Jeffrey Ding, "Deciphering China's AI Dream," 33.

[61] Wang You and Chen Dingding, "Rising Sino-US Competition in Artificial Intelligence," *China Quarterly of International Strategic Studies* 4.2 (2018): 242. https://doi.org/10.1142/S2377740018500148

[62] Ding, "Deciphering China's AI Dream," 32.

[63] Graham Webster et al., trans., "China's 'New Generation Artificial Intelligence Development

China expects to reach "world-leading" status with gross output exceeding USD 60.3 billion, and by 2030 to become the "world's primary AI innovation center" at gross output exceeding USD 1.5 trillion.[64]

However, China must hurdle a large, technological deficit to overcome the United States. Wang and Chen write that "U.S. superiority over China in talent reserve, innovation systems, and related hardware development is first and foremost manifested in its leading position in developing computer algorithms."[65] For example, open source platforms like TensorFlow and Caffe, which enable the more complex algorithmic abilities of AI, are American academic and company creations. Similarly, since China's top ten chip-making companies are specialized in less flexible ASIC chips and have not expanded into the production of graphics processing units, China depends on international companies for GPUs, the predominant computer chip option for training AI algorithms.[66] Moreover, China's AI talent pool in 2018 was only one-fifth that of the United States, according to the China Institute for Science and Technology Policy at Tsinghua University.[67]

But China is aggressively playing catch up. China's State Council has released a plan to integrate AI as an academic discipline, while researchers are frequently replicating and implementing advances in the field.[68] Moreover, China has increased its output of research to 15,199 AI papers published in 2017 compared to the United States' 10,287.[69] While the U.S. continues to enjoy an advantage in the field-weighted citation impact (FWCI) of its AI papers, since 1998, the United States' FWCI has only increased by 24%, while China's FWCI has increased by 154%.[70] Moreover, the U.S. share of the top 10% of most-cited AI papers has steadily declined from 49% in 1982 to 29% in 2018, whereas China's share has

Plan' (2017)," *New America,* August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[64] Ding, "Deciphering China's AI Dream," 7.

[65] Wang and Chen, "Rising Sino-US Competition in Artificial Intelligence, 246.

[66] Ding, "Deciphering China's AI Dream," 24.

[67] Xue Lan et al., "China AI Development Report 2018" (report, China Institute for Science and Technology Policy, Tsinghua University, Beijing, July 2018), 3-4, http://www.sppm.tsinghua.edu.cn/eWebEditor/UploadFile/China_AI_development_report_2018.pdf

[68] Daniel Castro, Michael McLaughlin, and Eline Chivot, "Who Is Winning the AI Race: China, the EU or the United States?" (report, Center for Data Innovation, Washington DC, August 2019), 19-20, http://www2.datainnovation.org/2019-china-eu-us-ai.pdf

[69] Ibid. 20

[70] Ibid., 21.

grown from 0% in 1982 to 26.5%.[71] Researchers suggest that China will surpass the U.S. in producing the top 10% and 1% of all AI papers by the end of 2020 and 2025, respectively.[72]

One larger point of disagreement, however, is whether China possesses a so-called data advantage. Demchak writes that "scale in demographic size multiplies the AI advantage when the large state's resources are able to employ it strategically" towards "acquiring the enormous volumes of data needed."[73] As a result, "no Westernized civil society alone has the scale to exploit AI…sufficiently enough to balance [China's] advantage."[74] Yet Lewis notes that while Chinese companies may have access to millions of Chinese users, this does not guarantee a data advantage.[75] Rather, he finds that Chinese companies are limited to China because of foreign markets' distrust of their services. By contrast, Western companies like Facebook and Google "service a global market and have access to twice as much data as Chinese companies."[76] Wright, on the other hand, argues that simply comparing data set quantities overlooks China's advantage based "in terms of combining breadth of data with ground truth data" for which "liberal democracies should not compete."[77] This advantage particularly enables China to construct a surveillance state and enable it for export.[78] Indeed, Ding highlights that a CCID Consulting report projects China to possess 30% of the world's data by 2030.[79]

China's AI Geopolitics

Deibert explains that world governments are largely divided into two camps: those that prefer a more open Internet and society, like the United States and Asian democracies, and those that prefer state-led governance like China,

---

[71] Ibid., 24.
[72] Ibid.
[73] Chris C. Demchak, "Four Horsemen of AI Conflict: Scale, Speed, Foreknowledge, and Strategic Coherence," in Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order," 101-102.
[74] Ibid., 102.
[75] James A. Lewis, "AI and China's Unstoppable Global Rise," in Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order," 96.
[76] Ibid.
[77] Wright, "The Technologies," 6-7.
[78] Ibid.
[79] Ding, "Deciphering China's AI Dream," 25.

Iran, and Russia.[80] Importantly, emerging-market countries—such as Brazil, India, and Indonesia—may align with either camp.[81]

China's specialization in AISS comes as a strategic response to the "growing impetus worldwide to adopt cybersecurity and antiterror policies."[82] The strategy is immensely top-down, as the Communist Party of China (CCP) officials influence the state-owned and private enterprises of AISS exportation. Weber defines these enterprises as comprising a "security-industrial complex": a network of state agencies, state-owned companies, and private companies.[83] State agencies utilize government officials to train Sri Lankan officials, install surveillance cameras in Phnom Penh, Cambodia, and share practices with Russia;[84] state-owned companies like the China National Electronics Import and Export Corporation (CEIEC) handle national security projects abroad, including managing Venezuela's Integrated Monitoring and Assistance System and facial recognition hardware and installation in Ecuador;[85] private companies like Huawei, ZTE, and Tencent contain CCP committees on high-level decision-making processes and comprise the bulk of filtering and surveillance technology exports to countries such as Iran, Zambia, and Zimbabwe.[86]

Furthermore, China maintains access to the data collected by companies and their technologies. Article 7 of the 2017 Chinese National Intelligence Law requires that "any organization or citizen shall support, assist and cooperate with the state intelligence work."[87] Likewise, the 2014 Counter-Espionage law stipulates that "when the state security organ investigates and understands the situation of espionage and collects relevant evidence, the relevant organizations and individuals shall provide it truthfully and may not refuse."[88] While Chinese technology companies claim they would never hand over data to the government, the legal structure and coordinated top-down effort of its technology export system

---

[80] Ron Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege," *Journal of Democracy* 26.3 (2015): 70, http://doi.org/10.1353/jod.2015.0051

[81] Ibid.

[82] Ibid., 71.

[83] Valentin Weber, "Understanding the Global Ramifications of China's Information Controls Model," in Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order," 72, 74-75.

[84] Ibid.

[85] Ibid.

[86] Ibid

[87] Arjun Kharpal, "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice," *CNBC,* March 4, 2019, https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

[88] Ibid.

suggests otherwise.

Consequently, companies become a proxy for the Chinese government to obtain data on an international scale. Cave et al. report that Internet and technology companies are believed to have the highest proportion of CCP committees in the private sector.[89] Similarly, Steckman reports that China's state dealings with companies often require review of the company's intellectual property, including their acquired data.[90] Such access is significant and widespread, as China's coordinated efforts have culminated in training sessions in over 36 countries, and the construction of "Chinese-style Internet surveillance systems" for 18 others.[91] In total, Feldstein finds that Chinese companies are exporting AISS to at least sixty four countries, including thirty six that are a part of the BRI.[92]

Scholars agree that China's export endeavors are an attempt to reshape international norms and thereby retain regional hegemony. In order to shield its domestic use of AISS from international influence,[93] China, according to McKune and Ahmed, has become the "primary norm entrepreneur," the leading international advocate of Internet sovereignty.[94] Internet sovereignty, according to Xi Jinping, is violated when countries "pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security."[95] According to McKune and Ahmed, Xi's view embodies "the absolute, exclusive right of the state to control its domestic Internet environment, and its citizens' interaction with that environment."[96] This norm-shaping effort can be most directly identified in

[89] Danielle Cave et al., "Mapping China's Technology Giants" (report, Issues Paper 15/2019, International Cyber Policy Centre, Australian Strategic Policy Institute, April 18, 2019), 3, 7, https://www.aspi.org.au/report/mapping-chinas-tech-giants

[90] Laura Steckman, "Pathways to Lead in Artificial Intelligence," in Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order," 82.

[91] Richard A. Clarke and Rob Knake, "The Internet Freedom League: How to Push Back Against the Authoritarian Assault on the Web," *Foreign Affairs* 98.5 (2019): 185.

[92] Feldstein, "The Global Expansion of AI Surveillance," 1.

[93] Refers to the creation of China's social credit scoring system that ranks residents on the basis for actions committed both online and offline, as well as the detention of 1-2 million Uighur Muslims in the Xinjiang province via facial recognition systems.

[94] Sarah McKune and Shazeda Ahmed, "The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda," *International Journal of Communication* 12 (2018): 3840, https://ijoc.org/index.php/ijoc/article/view/8540/2461

[95] Ibid., 3837.

[96] Ibid.

China's usage of the Shanghai Cooperation Organization (SCO), World Internet Conference, and Collective Security Treaty Organization (CSTO), which are "focused sites of learning and norm promotion where ideas, technologies, and 'best' practices are exchanged."[97] With meetings of "like-minded officials from neighboring authoritarian states," behind closed doors, Deibert argues that both the SCO and the CSTO are "venues where commercial platforms for both mass and targeted surveillance are sold" under the auspices of countering terrorism, separatism, and extremism.[98]

Through these institutions, China is embarking on coordinated and strategic efforts to promote the Internet sovereignty norm as beneficial to developing states in particular.[99] As Mueller argues, by incentivizing countries to internalize and adopt a model of Internet governance, the control of communications is realigned within national state boundaries, instead of wealthy democracies who hold the current concentration of infrastructural power.[100] The end goal for China appears to be "global recognition of the norm over the long term."[101]

But scholars debate the motives behind China's Internet sovereignty norm entrepreneurism in developing countries. Feldstein views it as an effort to erode democratic norms by providing fragile democracies with the means to quell discontent, and thereby accelerate authoritarianism or backsliding.[102] Economy sees a grander vision, with China exporting political values internationally to usher in its era of a "closed Internet."[103] However, Weiss contends China's export of AISS instead reflects "less a grand strategic effort to undermine democracy and spread autocracy than the Chinese leadership's desire to secure its position at home and abroad" and instead, simply makes it "easier for authoritarian states to coexist alongside democracies."[104] As this analysis will show, China's AISS export-specialization is not a total upheaval of the liberal world order nor solely

[97] Deibert, "Authoritarianism Goes Global," 71-72.
[98] Ibid.
[99] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3837.
[100] Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Malden, MA: Polity Press, 2017), 140 quoted in McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3837.
[101] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3835.
[102] Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression," *Journal of Democracy* 30.1 (2019): 42-43, https://doi.org/10.1353/jod.2019.0003
[103] Elizabeth C. Economy, "China's New Revolution: The Reign of Xi Jinping," *Foreign Affairs* 97.3 (2018): 66.
[104] Jessica C. Weiss, "A World Safe for Autocracy? China's Rise and the Future of Global Politics," *Foreign Affairs* 98.4 (2019): 93-94.

constrained to aims of regional security; instead, China's geopolitics can in part be explained by its neocolonialist exploitation of importing countries for gains in the global political economy.

Literature Takeaways

The Sino-optimist/pessimist divide selectively captures elements of China's neocolonialism at the expense of painting a representative picture. Sino-pessimists overlook the Sino-optimists' emphasis on China's engagement in long-term infrastructure projects throughout Africa, such as the establishment of special economic zones. Further, Sino-optimists importantly recognize China's particular interest in distinguishing itself as non-Western, an interest consistent with its normative practices of non-interventionism and Internet sovereignty. Meanwhile, Chinese investment—which is made irrespective of political instability, and at times, preferential toward corrupt states—suggests China considers little else other than the bottom line. Equally important, then, is the historic and recent deviance from these normative practices, like with Mozambique in 1977 and Sudan in 2015, ignored by Sino-optimists and captured by the Sino-pessimists.

The paradox between these two positions suggests that Nkrumah's condition of neocolonialism—that is, investment must increase rather than decrease the wealth gap between the rich and poor countries of the world—may be a sufficient but unnecessary indicator of neocolonialism. Indeed, an important takeaway from the literature is that neocolonialism today is complex. While China's long-term infrastructure projects may enrich African countries in one way, its engagement with such countries can extract resources and political leverage in another. When a new source of wealth is introduced, but international conventions of wealth remain, it is possible to extract this new wealth from developing countries while simultaneously enriching them in old wealth.

As literature on AI indicates, this new wealth is data. It is well understood that data is the backbone of AI—only when AlphaGo studied over 100 million game types did it successfully overcome a world-class human Go player.[105] Ground-truth data, especially, is crucial for unlocking the potential of AI.[106] This particular source of wealth, then, is routine access to another nation's ground-

---

[105] Brenden M. Lake et al., "Building Machines That Learn and Think like People," *Behavioral and Brain Sciences* 40 (2017): 22-23, https://doi.org/10.1017/S0140525X16001837
[106] Wright "The Technologies," 5.

truth data, further advantaging China in its development of all types of artificially intelligent systems.

The growing concern here is that Chinese technology enables state access to data. The legal and political climate behind China's security-industrial complex indicates that its powerful companies are access points to international data. This data extraction may occur directly, as most export partnerships are expected to grant China access to civilian ground-truth data.[107] In particular, China leverages the sale of its technology for access to biometric data on citizens—such as those in Zimbabwe, Angola, and Ethiopia.[108] Alternatively, backdoors within technological operations can provide another avenue to data for China. In addition to international concern over backdoors in China's 5G infrastructure, recent reports have also revealed that the cameras made by Dahua Technology, the world's second-largest CCTV manufacturer, have been, whether deliberately or not, engineered with vulnerable access points. [109] Moreover, China could potentially gain parallel access to systems' data by assisting surveillance operations, as it has done in Venezuela.[110]

As it faces an opportunity to grow its GDP significantly, China's full-scale use of its security-industrial complex is unsurprising.[111] The declaration of AI as the "new focus of international competition" further underscores China's perception of the ascendancy of AI as an international issue.[112] Yet, it is crucial to recognize that China is a lagging entity in aggressive pursuit of market supremacy.[113] Its use of its AISS exports secures unparalleled access to ground-truth data to upgrade algorithms, but also grants worldwide hegemony in an ever increasing AI world. While seemingly paradoxical, the global, coordinated effort of the Chinese security-industrial complex to build and train AISS models for other

---

[107] Steckman, "Pathways to Lead in Artificial Intelligence," 82.

[108] Gwagwa, "How China's Artificial Intelligence is Shaping Geopolitical and Geoeconomic Global Order."

[109] Bruce Schneier, "China Isn't the Only Problem With 5G," *Foreign Policy,* January 10, 2020, https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance; Zak Doffman, "Warning As Millions Of Chinese-Made Cameras Can Be Hacked To Spy On Users," *Forbes,* August 3, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/#301ed6c06bf2

[110] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters,* November 14, 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/

[111] Ding, "Deciphering China's AI Dream," 32.

[112] Nicholas D. Wright, "AI and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy," in Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order," 22-24.

[113] Wang and Chen, "Rising Sino-US Competition in Artificial Intelligence," 246.

countries remains consistent with China's view of Internet sovereignty norms.[114] Indeed, in light of developments at the SCO, the World Internet Conference, and the CSTO, China's international, norm entrepreneurial efforts appear to be aimed at establishing regional partnerships and securing China's domestic AI practices outside the ambit of Western regulation. Convincing developing countries of the benefits of realigning control over communications domestically plays an important role in achieving the "global recognition of the norm over the long term."[115] While most of the contemporaneous conceptions of China's norm entrepreneurialism focus on the acceleration of authoritarianism,[116] Weiss offers a comparatively benevolent conception of China as merely interested in authoritarian coexistence.[117]

However, these scholars ignore the larger stratagem, particularly as it relates to developing countries. China facially represents its ideology with benevolence, using such trust to gain entry into developing countries' security apparatuses and pragmatically pursue resource extraction. Indeed, supplying the networks and infrastructure to countries grants unique access for China to countries' citizen data and markets, while also providing a platform to shape favorable norms in the strategic global AI competition. China's AISS export model can then be understood both as a neocolonialist mechanism to both feed its ground-truth data advantage and influence Internet norms in a world of emerging-market countries.[118]

The Neocolonialist Tradition & the AISS Empire

In the Nanshan district of Shenzhen, a "growing new breed of Chinese technology companies specializing in surveillance and censorship equipment" is emerging.[119] China has used its natural access to facial data—troves of video surveillance footage on a massive population—to immensely enhance the

---

[114] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 74-75; McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3841-43.

[115] Mueller, *Will the Internet Fragment?*, 140; McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3835.

[116]

[117] Feldstein, "The Road to Digital Unfreedom," 60-74; see Weiss, "A World Safe for Autocracy?"

[118] Deibert, "Authoritarianism Goes Global," 70.

[119] Ryan Gallagher, "Export Laws," *Index on Censorship* 48.3 (2019): 37, https://doi.org/10.1177/0306422019876445

accuracy of its facial recognition software.[120] China has published over 900 facial recognition sector patents in 2017 alone, a stark contrast to the 150 patents filed in the US.[121] By developing an unparalleled ability to "link people's identities and activities" with real time assessments of individuals' location, activities, gender, clothing, and facial characteristics,[122] Wang argues that China's AISS is expected to attain "world leading" status.[123] From Algeria to Zimbabwe, China's export empire in AISS is expansive. By 2023, China is expected to dominate the facial recognition market with nearly a 45% market share—an increase from today's 29%.[124]

Admittedly, China's security-industrial complex has exported broadly to liberal democracies, such as Germany and France, who have both supplied—but also bought into—China's facial recognition expertise.[125] However, the conception of an AISS empire here refers specifically to the 50 developing countries importing China's technology.[126] The decision to focus on these countries is, in large part, to indicate the strength of a neocolonialist relationship in the export of AISS. Many of these countries are in pivotal positions for China to enhance its own position in the international AI market.

The following sections will lay the theoretical foundation behind the subsequent section's claims of Chinese AISS neocolonialism. First, the reality of Chinese neocolonialism in the international normative climate will be explored, concluding that the presence of mutually beneficial engagement should not acquit China from indictment for neocolonialist exploitation. Next, four elements of neocolonialist practice based on Antiwi-Boateng's research—derived from the

---

[120] Qiang Xiao, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30.1 (2019): 56-58, https://doi.org/10.1353/jod.2019.0004

[121] Jeffrey Ding, "China's AI Superpower Dream with Jeffrey Ding," interview by Lucas Perry, in *AI Alignment Podcast*, August 16, 2019, produced by the Future of Life Institute, podcast, MP3 audio, 1:12:20, https://futureoflife.org/2019/08/16/chinas-ai-superpower-dream-with-jeffrey-ding/

[122] Xiao, "The Road to Digital Unfreedom," 58, 64.

[123] Eudora Wang, "China To Take Nearly Half Of Global Face Recognition Device Market By 2023," *China Money Network*, August 23, 2018, https://www.chinamoneynetwork.com/2018/08/23/china-to-take-nearly-half-of-global-face-recognition-device-market-by-2023

[124] Ibid.

[125] Steven Feldstein, "The Global Expansion of AI Surveillance," 8.

[126] Ibid. e.g. Algeria, Argentina, Armenia, Bahrain, Bangladesh, Bolivia, Botswana, Brazil, Burma, Chile, Ecuador, Egypt, Ghana, Hong Kong, India, Indonesia, Iran, Iraq, Ivory Coast, Kazakhstan, Kenya, Krygzystan, Laos, Malaysia, Malta, Mauritius, Mexico, Mongolia, Morocco, Oman, Pakistan, Panama, Philippines, Qatar, Rwanda, Saudi Arabia, Serbia, Singapore, South Africa, Tajikistan, Thailand, Turkey, Uganda, Ukraine, United Arab Emirates, Uruguay, Uzbekistan, Venezuela, Zambia, and Zimbabwe

heritage of colonialism in 19th century British and French empires—will be identified and compared to China's modern exportation of AISS. The section will focus on developing countries' engagement with China's AISS exports, which highlights the nexus between traditional and modern elements of neocolonialism: 1) the extraction of data as a resource, 2) the pursuit and creation of exclusive markets, 3) the accumulation of global prestige to influence norms, and 4) the ulterior framing of China's AISS-export relationship with developing countries as altruistic. It should be noted, however, that such characteristics are only the most salient elements of colonialism—not an exhaustive account. Nonetheless, China's specialization in AISS should be viewed as a strategic decision on its path to global AI supremacy.

The Reality of China's Neocolonialism

  Before exploring the elements of China's engagement with Africa as a neocolonialist enterprise, it is important to first consider the complexities of China's modern interaction with African countries. In many cases, China's investments, while producing immense returns and access to new markets, have generated enormous benefits for the African countries it contracts with. For example, Chinese capital development funding for African infrastructure totaled about $328 billion from 2009 to 2014, and China has pledged about $1 trillion in aid for the following decade.[127] But evidence of mutual benefit should not vindicate neocolonialist aims. Rather, as this section will contend, all of China's displays of mutual beneficence can be explained by strategic attempts to distinguish itself from prior and current Western engagements.

  International norms changed the pragmatic calculus of industrialization for China. Antiwi-Boateng writes that:

> … the Chinese have had to engage African people under a completely different international political, economic, and legal framework … Chinese engagement in Africa is occurring at a period where the concept of statehood and sovereignty has been globally accepted and institutionalized …[128]

---

[127] Steve Johnson, "China By Far The Largest Investor In African Infrastructure," *Financial Times,* November 30, 2015, http://www.ft.com/intl/cms/s/3/716545c0-9529-11e5-ac15-0f7f7945adba.html

[128] Antiwi-Boateng, "New World Order Neo-Colonialism," 189.

Indeed, as Zhao argues, China learned its "lessons the hard way" and after engendering "local and international concern . . . of a zero-sum competition for finite resources," has "made efforts to adjust such sensitive business practices."[129] China's doctrine of non-interference and declaration of "Five Principles of Peaceful Coexistence" point towards the idea that, for neocolonialist enterprises, such careful balancing is required by international norms. [130] At the same time, the principles form a visibly sharp distinction from previously destabilizing Western colonial policies and post-independence Western conditionality of resources.[131] For example, unlike the manipulation of African elites by patronizing European elites, China has emphasized respectful and purportedly mutually-beneficial interactions when engaging African leaders. As Antiwi-Boateng argues, these relationships have "been driven by the need to reduce Western influence in Africa," a choice made easy for many African leaders now comparatively viewing the "burdensome and indifferent attitude from the West."[132]

China's refrain from a "civilizing mandate" of cultural assimilation, as European colonialists engaged in, is another example of China's careful balancing to satisfy international norms. Instead, as Antiwi-Boateng argues, China pursues strategic forms of cultural diplomacy to improve its image and leave the appearance of the West as inflexible and traditional.[133] China Central Television—"the most powerful soft power tool used by China"—broadcasts programming on positive trade relations to some 47 countries, strengthening its influence indirectly, as opposed to political or administrative control.[134] Similarly, China funds approximately 12,000 African students to study in China, far outpacing all other countries' scholarship programs for African students in an attempt to "shape and cultivate the next generation of African leaders who will be amenable to future

---

[129] Zhao Suisheng, "A Neo-Colonialist Predator or Development Partner?," 1033.
[130] "The Five Principles of Peaceful Coexistence: The Time-Tested Guideline of China's Policy With Neighbors," *Ministry of Foreign Affairs of the People's Republic of China,* July 30, 2014, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/t1179045.shtml; Refers to the following: mutual respect for each other's territorial integrity and sovereignty, mutual non-aggression, mutual non-interference in each other's internal affairs, equality and mutual benefit, and peaceful co-existence.
[131] Antiwi-Boateng, "New World Order Neo-Colonialism," 186.
[132] Ibid., 188.
[133] Ibid., 185.
[134] Ibid.

Chinese policies."[135] Even the massive developmental aid projects are stained by ulterior motives of expanding Chinese influence at the expense of supplanting the West. The over $75 billion of Chinese investments in aid and development projects is largely considered a "charm offensive"—a design to woo its recipients in order to establish political and economic influence in the region.[136]

China's choice to distinguish its operations from that of the West has granted it increased access to investments within Africa. Dreher and Fuchs have noted that African states were drawn to Chinese partners in large part to avoid the ideological and political remedies required from Western investors.[137] Given this framing, China's favorability has increased as investments have risen over the years. In 2011, China had a favorability polling of 50% in Kenya, Nigeria, Ghana, and South Africa, and by 2014, it was 60%.[138] As of 2015, African respondents have a significantly more positive view of China at 70% favorability, compared to Europe at 41%.[139]

While Sino-optimists and Sino-pessimists categorize China's neocolonialism as binary, the complexities of neocolonial traditions engender a modern scenario in which China's exploitation can both have mutually beneficial outcomes and still be manipulative. Rich and Recker suggest that the reality: China's engagement with developing countries "is somewhere in the middle" of Sino-optimist and Sino-pessimist perspectives, oscillating between neocolonialist exploitation and mutual beneficence.[140]

China's recent engagements, however, are more indicative of strategic conformity, rather than genuine adherence to non-interference. Verhoeven, for instance, found that China's growing material interests are "forcing it to

---

[135] Simon Allison, "Fixing China's Image in Africa, One Student at a Time," *Guardian*, July 5, 2013, https://www.theguardian.com/world/2013/jul/31/china-africa-students-scholarship-programme; Antiwi-Boateng, "New World Order Neo-Colonialism," 184.

[136] Claire Provost and Rich Harris, "China Commits Billions in Aid to Africa as Part of Charm Offensive," *Guardian*, April 29, 2013, https://www.theguardian.com/global-development/interactive/2013/apr/29/china-commits-billions-aid-africa-interactive

[137] Axel Dreher and Andrea Fuchs, "Rogue Aid? An Empirical Analysis of China's Aid Allocation," *Canadian Journal of Economics* 48.3 (2015): 993-995, https://doi.org/10.1111/caje.12166

[138] Chen Wenjie, "Chinese Investment in Africa Is More Diverse and Welcome than You Think," *Quartz Africa,* August 26, 2015, https://qz.com/africa/488589/chinese-investment-in-africa-is-more-diverse-and-welcomed-than-we-give-it-credit/

[139] Chen, Dollar, and Tang, "Why is China investing in Africa?," 2.

[140] Rich and Recker, "Understanding Sino African Relations," 72.

in practice abandon the principle of non-interference."[141] This is evidenced by examples in Sudan and Djibouti, as well as historical experiences in Angola and Mozambique.[142] Antiwi-Boateng thus argues that although it maintains itself internationally as non-interventionist, China is a "neo-colonialist entity" capable of resource extraction without the "unbridled territorial control" that 19th-century colonists relied upon.[143] When considering neocolonialist engagements, China's export of AISS must be evaluated in light of this complexity, especially with respect to China's strategic use of international norms for material gain.

ELEMENTS OF NEOCOLONIALISM

Resource Extraction: Harvesting Data

For Antiwi-Boateng, the core of the British and French colonial regimes was the search for sources of raw materials, like timber, ivory, and copper. [144] These materials served a higher order goal of industrialization, largely spurred by a competitive international dynamic.[145] It appears that, in the present day, China views Africa as a central piece in its international grand strategy. While Africa is a large buyer of manufactured products like machinery and textiles, and import resources like crude oil and copper that are of little value to Africa, China's engagements have largely been spurred by Chinese efforts to compete internationally. [146] For example, China is the world's largest user of copper and eighth largest exporter of refined copper products.[147] Thus, Zhao finds that China's renewed interests in Africa does resemble European colonial powers' natural resource expeditions.[148]

In the AISS context, China's State Council, in its 2017 "New Generation Artificial Intelligence Development Plan," outlined the importance of AI for "supply side structural reform[s]" and the "great rejuvenation of the Chinese nation."[149]

[141] Harry Verhoeven, "Is Beijing's Non-Interference Policy History? How Africa is Changing China," *The Washington Quarterly* 37.2 (2014): 66, https://doi.org/10.1080/0163660X.2014.926209
[142] See Antiwi-Boateng, "New World Order Neo-Colonialism," 186; Allen, "What China Hopes to Achieve With First Peacekeeping Mission"; Campos and Vines, "Angola and China," 2-3; Roque, "China in Mozambique," 2.
[143] Antiwi-Boateng, "New World Order Neo-Colonialism," 177.
[144] Ibid., 181-82.
[145] Ibid.
[146] Zhao, "A Neo-Colonialist Predator or Development Partner?," 1042.
[147] Ibid., 1043.
[148] Ibid., 1035-36.
[149] Webster et al., "China's 'New Generation Artificial Intelligence Development Plan.'"

Considering that the integration of AI systems could boost Chinese GDP by 26%, AISS is a crucial element of China's future industrialization plans.[150] A report by the China Industry Economy Research & Consulting group noted that China's facial recognition software is expected to maintain an average annual growth rate of 25%, hitting over $1.06 billion by 2022.[151]

Integral to such AI industrialization, however, is ground-truth data, which AISS exportation grants tremendous access to. For example, Alibaba's CloudWalk Technology company contracted with Zimbabwe to install facial recognition software. According to a UN Special Rapporteur report, to read and differentiate African faces, Cloudwalk asked the Zimbabwean government to turn over massive amounts of biometric data.[152] Such datasets are incredibly valuable, as facial recognition software today largely struggles with differentiating faces that are not white.[153] In written testimony to the House Committee on Oversight and Government Reform, Cook explained that datasets of millions of sub-Saharan African faces enable Chinese developers to overcome pervasive, race-related software errors—an immense market share advantage for China.[154] The operation of such technology in a majority black population like Zimbabwe's creates an algorithmic advantage over American and European developers.[155] But the situation in Zimbabwe is not unique. In Uganda, there is a lack of transparency over the regulation of information flows in what appears to be a "policy to hand over the country's entire communications infrastructure," according to an official

---

[150] Ding, "Deciphering China's AI Dream," 32.

[151] Zhang Hongpei, "Chinese Facial ID Tech To Land In Africa," *Global Times*, May 17, 2018, http://www.globaltimes.cn/content/1102797.shtml

[152] "MISA Zimbabwe's Submission on the Surveillance Industry and Human Rights in Zimbabwe" (report, United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Media Institute of Southern Africa, Harare, Zimbabwe, February 15, 2019), 1, https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/MISA%20ZIMBABWE.pdf

[153] Steve Lohr, "Facial Recognition Is Accurate, If You're a White Guy," *New York Times*, February 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[154] Sarah Cook, "China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses," *Freedom House,* September 26, 2018, https://freedomhouse.org/article/chinas-cyber-superpower-strategy-implementation-Internet-freedom-implications-and-us#Ftn31

[155] Lynsey Chutel, "China Is Exporting Facial Recognition Software To Africa, Expanding Its Vast Database," *Quartz Africa*, May 25, 2018, https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

in the Ugandan Parliament.[156] Similar deals were struck in Angola and Ethiopia, and China's export partnerships are expected to include requirements that grant Chinese access to a civilian ground-truth data.[157] In effect, China's AISS accuracy will improve against international competition.

However, as Chutel writes, the CloudWalk example is only one method by which China's security industrial complex circumvents ethical and legal concerns to access countries' data cheaply.[158] Another method involves inputting backdoors within the infrastructure of AISS, which then less visibly siphon data. Recently, the African Union Headquarters' computers, imported from China, were discovered to have been sending information to mainland China for years without consent or awareness.[159] Such backdoors can be expected in the over 18 countries where China has internally constructed surveillance infrastructure.[160] For example, the state-owned enterprise China National Electronics Import & Export Corporation (CEIEC) built the facial recognition hardware for Ecuador, while ZTE, a private Chinese company, embedded employees into Venezuela's telecommunications systems to assist in managing information databases and building centralized video surveillance systems.[161] ZTE's Venezuelan database contains details such as birthdays, family information, employment income, medical history, property owned, presence on social media, and political affiliation.[162] Moreover, China's Transsion has taken over Africa's mobile market, surpassing Samsung along the way.[163] It has recently introduced the Tecno Camon X Pro, which will enable the facial recognition data collection of millions of customers.[164] Like the export-

---

[156] Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy—Chinese Giant's Staff Aided Cybersecurity Forces' Snooping On Opposition," *Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

[157] Gwagwa, "How China's Artificial Intelligence is Shaping Geopolitical and Geoeconomic Global Order"; Steckman, "Pathways to Lead in Artificial Intelligence," 82.

[158] Ibid., 79.

[159] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 73-74.

[160] Clarke and Knake, "The Internet Freedom League," 187-88.

[161] Jun Mai, "Ecuador Is Fighting Crime Using Chinese Surveillance Technology," *South China Morning Post*. Jan 22, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2129912/ecuador-fighting-crime-using-chinese-surveillance; Berwick, "How ZTE Helps Venezuela Create China-Style Social Control."

[162] Ibid.

[163] Chutel "China Is Exporting Facial Recognition Software To Africa"

[164] Ibid.

partnership deals granting China explicit access to data, information backdoors in Chinese cyber infrastructure projects should be expected as a means of data collection.[165] Indeed, the frequency of such backdoors has led Australia and the U.S. to avoid purchasing infrastructure from companies like Huawei and ZTE, and have caused public concern in Ghana over a Chinese digital television infrastructure project.[166]

China's theft of developing countries' data should thus be viewed as a deliberate extraction of resources. In 2017, the *Economist* wrote that "the world's most valuable resource is no longer oil, but data."[167] But even that comparison underplays the importance of data. Data can be replicated and transported with little limitation, and, unlike energy, its utility increases with use.[168]

As the world turns more and more towards artificial intelligence, the demand for data can only be expected to increase. However, in the internationally competitive environment of artificial intelligence, "it's not just the volume of data that's important . . . [but] the kind of data and where they originate."[169] A country with access to numerous other countries' data will be able to develop more universally applicable AI products, since merely having data on "Spanish speech patterns will not make a system robust at identifying Mandarin characters."[170] If China is able to acquire numerous countries datasets, then the competitive advantage they will gain in providing technologies to these countries will remain unparalleled. Sacks and Sherman point out just precisely what is at stake:

> In a world increasingly underpinned and powered by AI, those looking to develop globally competitive AI systems—algorithms that will be precise and accurate in many parts of the world, across many demographics—will need access to data on those

---

[165] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 73-74.
[166] Ibid.
[167] "The World's Most Valuable Resource Is No Longer Oil, But Data," *Economist*, May 6, 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
[168] Bernard Marr, "Here's Why Data Is Not The New Oil," *Forbes*, March 5, 2018, https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#16c01a773aa9
[169] Samm Sacks and Justin Sherman, "The Global Data War Heats Up," *Atlantic*, June 26, 2019, https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/
[170] Ibid.

different demographics, from those different regions.[171]

Increasingly, data especially makes all the difference for gaining a competitive market advantage in the realm of AI.[172]

Pursuit of Unsaturated Markets: Security and Stability

Antiwi-Boateng argues that the second archetypal feature of 19th century colonialism was the search for markets. The British and French, for instance, used infrastructure projects—such as roads and railways—to establish expanded markets for products and economies. China, through state financing, has similarly provided "billions in loans to African governments to fund infrastructure projects which are usually contingent on the use of Chinese labor, technology and raw materials."[173] China emulates colonial heritage presently by tapping into Africa's "*unsaturated market[s]*" (emphasis added).[174] Indeed, as Herrero argues, the bulk of China's investment and project finance within Africa is "directed towards China's strategic objectives, namely securing access to resources and using [its] excess capacity in construction and transportation."[175]

AISS, by nature, is a technology offering a paradigm shift for guaranteeing security and stability, and recipient countries are likely to grow more and more reliant on its capabilities. Even more telling is that China's specialization in AISS arrives at the intersection of two trends: a reverse wave of authoritarianism and a rapidly digitizing global South. Over the past two centuries, according to Huntington, the emerging diversity of regime types can largely be organized in terms of three "waves" of democratization, each wave followed by a "reverse wave" of authoritarianism: 1820s democracy, 1920s fascism; 1940s allied victory, 1960s bureaucratic authoritarianism; and the 1970s democracies.[176] Presently, the

---

[171] Ibid.

[172] Kai-Fu Lee, "Kai-Fu Lee's Perspectives On Two Global Leaders In Artificial Intelligence: China and the United States," interview by Michael Chui, *McKinsey Global Institute*, June 14, 2018, https://www.mckinsey.com/featured-insights/artificial-intelligence/kai-fu-lees-perspectives-on-two-global-leaders-in-artificial-intelligence-china-and-the-united-states

[173] Antiwi-Boateng, "New World Order Neo-Colonialism," 182.

[174] Zhao, "A Neo-Colonialist Predator or Development Partner?," 1033-1052.

[175] Alicia-Garcia Herrero, "China's Investments In Africa: What The Data Really Say, and the Implications For Europe*,*" *Forbes,* July 24, 2019, https://www.forbes.com/sites/aliciagarciaherrero/2019/07/24/chinas-investments-in-africa-what-the-data-really-says-and-the-implications-for-europe/#a723dc8661f9

[176]Samuel P. Huntington, "Democracy's Third Wave," *Journal of Democracy* 2.2 (1991): 12-13, 18, https://doi.org/10.1353/jod.1991.0016

world finds itself in its third, reverse wave of authoritarianism—over 2.5 billion people now live in countries affected by the "global autocratization trend."[177] At the same time, an explosive growth of digital connectivity has taken place in the global South, particularly among authoritarian regimes, weak states, and flawed democracies.[178] As Deibert reported, "In Indonesia, the number of Internet users increases each month by 800,000," while "the Internet-penetration rate in Cambodia rose a staggering 414 percent from January 2014 to January 2015."[179] Overall, "the steepest rates of growth in mobile-data traffic will be found in the Middle East and Africa."[180] With the advent of the "dual use" apparatus of smartphones and digital assistants in even non-authoritarian government systems, the barriers to the adoption of AISS systems are at their lowest point ever.[181] Since crucial components of digital authoritarian monitoring are already in place in many developing countries, such as smart phones and Internet services, the rise in digital connectivity creates "security and governance pressure points" that regimes can squeeze.[182]

In fact, the political economy behind security represents the major demand behind AISS, and the resurgence of digital authoritarianism in many importing countries.[183] For the authoritarian, the gravest threats to state survival are no longer from coup d'états, but, as Feldstein puts it, "discontented publics on the streets or at the ballot box."[184] Governments who previously had strong-armed stability through coercion or cooptation now face fears of collapsing into a military state at the hands of emboldened police or encountering sustainability issues as resource demands increase among a more discontented populace.[185]

---

[177] Anna Lührman et al., "Democracy for All? V-Dem Annual Democracy Report 2018" (report, V-Dem Institute, University of Gothenburg, May 28, 2018), 19, https://doi.org/10.2139/ssrn.3345071 , quoted in Feldstein, "The Road to Digital Unfreedom," 43.
[178] Deibert, "Authoritarianism Goes Global," 73.
[179] Ibid.
[180] Ibid.
[181] Jeffrey Ding, "The Interests Behind China's AI Dream," in Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," 38.
[182] Jacob Poushter, "Smartphone Ownership Rates Skyrocket in Many Emerging Economies, but Digital Divide Remains," *Pew Research Center*, February 22, 2016, https://www.pewresearch.org/global/2016/02/22/smartphone-ownership-rates-skyrocket-in-many-emerging-economies-but-digital-divide-remains; Deibert, "Authoritarianism Goes Global," 73.
[183] Ibid., 74.
[184] Feldstein, "The Road to Digital Unfreedom," 43.
[185] Ibid., 42-43.

But AISS contains none of these drawbacks. Instead, according to Feldstein, it "requires considerably fewer human actors than conventional repression, entails less physical harassment, and comes at a lower cost."[186] Chinese companies are thus in the business of providing state solutions to many developing countries' problems of governance and political instability.[187]

For the digitizing global South—countries like Laos, Kenya, and Indonesia—stability now has an affordable price, as product pitches are often accompanied by loans which encourage equipment purchases.[188] China has used its burgeoning market dominance in AISS and state-backed loans to open AISS to countries that previously could not afford it. The surveillance-solution multiplies the value of increasingly prevalent Internet connectivity and mobile devices, which are used to deliver critical and often lacking information infrastructure. Its facial recognition technology therefore exploits the need for social stability in developing countries.[189] The result is that, on the condition of contracting with Chinese firms, countries like Mauritius gain long-term financing from the Chinese government and companies like Huawei assume sole proprietorship over AISS installations. Zimbabwe is the first example of China entering Africa with AISS, but it has been far from the last.[190]

Already, via partnerships forged in its Belt and Road Initiative, China has supplied surveillance systems to nearly half of the 86 countries enrolled in the project.[191] Xi Jinping may have publicly stated China is not exporting a particular model nor asking for others to copy it, but this matters little. [192] Feldstein argues that as countries integrate Chinese systems into their governance practices, they develop a greater reliance on the infrastructure, software, and technical expertise of such systems and subsequently face "increasing pressure to align their policies with the PRC's strategic interests."[193] Similarly, Benaim and Gilman surmise that ambitions of AISS exports may very well be long term and resemble "algorithmic authoritarianism," where China's exportation of domestic surveillance methods contributes to a greater need for additional, similarly functional technology.[194]

[186] Ibid.
[187] Cave et al., "Mapping China's Technology Giants," 4.
[188] Feldstein, "The Global Expansion of AI Surveillance," 2.
[189] Zhang, "Chinese Facial ID Tech to Land in Africa."
[190] Gallagher, "Export Laws," 35-37.
[191] Feldstein, "The Global Expansion of AI Surveillance," 1.
[192] Weiss, "A World Safe for Autocracy?," 94-96.
[193] Feldstein, "The Road to Digital Unfreedom," 49.
[194] Daniel Benaim and Hollie R. Gilman, "China's Aggressive Surveillance Technology Will

For example, in 2008, during his presidency, Hugo Chavez visited Shenzhen and learned of the power of surveillance mechanisms.[195] By 2013, Venezuela had contracted with CEIEC to install over 30,000 security cameras in what current President Maduro called the Integrated Monitoring and Assistance System.[196] In 2018, ZTE was hired by Venezuela on a $70 million national security project constructing a "Fatherland Card" database that closely resembles China's own Social Credit Registry method of rewarding and punishing citizens through technology.[197]

At the intersection of global authoritarianism and digitization, China has successfully opened access to its specialized market. Feeding on pressing and unsaturated needs for security and stability, China cultivates an increasing dependence among these countries for its state-solutions. In what can best be described as an exploitative vicious cycle, China's AISS export regime stokes greater demand within its empire for its product and provides for ever-increasing influence and access to data.[198] In turn, with greater access to data, especially on citizens within recently digitizing developing countries where citizen digital data has seldom, if ever, been systematically acquired, China will gain a marked advantage for developing country-specific AI products, even beyond AI surveillance.

Desire for Global Prestige: Achieving Internet Sovereignty

The third key marker of neocolonialism, according to Antiwi-Boateng, is power projecting with the intent of securing the ability to pursue national interests "unhindered by other great powers."[199] In the colonial heritage of the 19th and 20th centuries, European naval superiority functioned to protect and pursue British and French national interests.[200] China presently shares with European

---

Spread Beyond Its Borders," *Slate,* August 9, 2018, https://slate.com/technology/2018/08/chinas-export-of-cutting-edge-surveillance-and-facial-recognition-technology-will-empower-authoritarians-worldwide.html

[195] Berwick, "How ZTE Helps Venezuela Create China-Style Social Control."

[196] Ryan Mallett-Outtrim, "30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets," *Venezuela Analysis*, November 27, 2013, https://venezuelanalysis.com/news/10198

[197] Berwick, "How ZTE Helps Venezuela Create China-Style Social Control."

[198] Steckman, "Pathways to Lead in Artificial Intelligence," 82-83.

[199] Antiwi-Boateng, "New World Order Neo-Colonialism," 182.

[200] Ibid.

colonialists a similar strategic desire, as it views Africa as a part of a larger strategy for global influence.[201] The November 2006 Forum on China-Africa Cooperation (FOCAC) prompted deep anxieties in the West, as German Chancellor Angela Merkel responded by: "Europeans should not leave the continent of Africa to the People's Republic of China …We must take a stand in Africa."[202]

China is similarly using its AISS-export prestige—its relationships with developing countries—to influence global norms about the use of technology. According to Finnemore and Sikkink, the lifecycle of a norm occurs in three stages: norm emergence, facilitated by a norm entrepreneur; norm cascade, when countries begin to adopt the norm more rapidly; and norm internalization, where a norm gains widespread acceptance.[203] Presently, norms of Internet governance are in contest and are emerging. On one end, open governance espouses the global free flow of ideas and information exchanges, while on the other end, Internet sovereignty rejects the present Internet order in exchange for a more localized and sovereign approach. McKune and Ahmed write that China has been the state most dedicated to a coordinated and strategic effort to promote Internet sovereignty globally—the primary norm entrepreneur of "Internet sovereignty."[204] As this section will argue, China has strategically used its empire of developing countries to bring about Internet sovereignty norms and protect its ability to pursue further exploitative AISS practices.

The importance of Internet sovereignty for China should not be understated. First and foremost, it is an attempt to craft information borders. Chen Xueshi, from the PLA-affiliated National University of Defense Technology, writes that information borders can be defined as the "national security relevant virtual space (and corresponding physical carriers) stored on electronic devices used by a state's infrastructure systems, government, and extra-governmental institutions and individuals."[205] According to the Chinese government, states that abide by Internet sovereignty 1) "must participate in international Internet governance on

---

[201] Daniel Large, "Beyond 'Dragon in the Bush': The Study of China-Africa Relations," *African Affairs* 107.426 (2008): 56-58, https://doi.org/10.1093/afraf/adm069

[202] Jilio Godoy, "China Swaggers into Europe's Backyard," *Asia Times,* November 17, 2006, http://www.atimes.com/atimes/China_Business/HK17Cb03.html, quoted in Horace Campbell, "China in Africa: Challenging US Global Hegemony," *Third World Quarterly* 29.1 (2008): 92, https://doi.org/10.1080/01436590701726517

[203] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52.4 (1998): 894, https://doi.org/10.1162/002081898550789

[204] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3840.

[205] Ibid., 3837.

an equal footing" 2) shall not "engage in, condone, or support cyber activities that undermine the national security of others states" and 3) shall have the "right to choose their own paths of cyber development, their models for Internet regulation and their public Internet policies" without interference from other states.[206]

Given its centralized, authoritarian structure, China views a potential open Internet as a threat. Information borders are key to the survival of its mode of governance.[207] In one of the most prominent CCP journals, top officials wrote that the Party's ideas must become the "strongest voice in cyberspace," for "if our party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term."[208] By contrast, a hallmark of Internet sovereignty has been to conceptualize it in the same domain as sovereignty over national airspace and maritime zones.[209] Thus, by constructing linkages to established legal norms of state sovereignty, China can protect domestic regime practices from Western-based human rights criticism.[210]

AISS forms a critical part of the effort to normalize Internet sovereignty on the global stage. Indeed, "China's Cyber Superpower Strategy" emphasizes the importance of enhancing the "global influence of Internet companies like Alibaba, Tencent, Baidu [and] Huawei" in order to secure "international consensus" for Internet sovereignty.[211] In fact, China's "AI National Team" of Alibaba, Tencent, Baidu, and iFLYTEK operates with a mandate to invest heavily and export effectively.[212] Developed countries figure centrally in its plan. Its international claims on Internet sovereignty are made on behalf of the developing world, calling countries to refocus the control of information

---

[206] "International Cyberspace Cooperation Strategy," (policy document, no. CD/2092, Conference on Disarmament, Ministry of Foreign Affairs of the People's Republic of China and State Information Office, March 1, 2017), https://undocs.org/CD/2092, quoted in Ibid.

[207] Ibid., 3838.

[208] Webster et al., "China's 'New Generation Artificial Intelligence Development Plan.'"

[209] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3838.

[210] Webster et al., China's 'New Generation Artificial Intelligence Development Plan.'"

[211] . Sarah Cook, "China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses," *Freedom House,* September 26, 2018, https://freedomhouse. org/article/chinas-cyber-superpower-strategy-implementation-Internet-freedom-implications-and-us#Ftn31

[212] Gwagwa, "How China's Artificial Intelligence is Shaping Geopolitical and Geoeconomic Global Order," 1.

technologies within jurisdictional borders.[213] Moreover, thirteen of the top twenty "Digital Decider" states for the future openness of the Internet have imported China's AISS technology, including the top five—Brazil, Indonesia, Mexico, India, and Singapore.[214] Wright has therefore referred to China as using these companies' "market power" to "influence technical standards, 'normalize' domestic control and shape norms of behavior through international organizations."[215]

The interstate collaborations from Chinese companies exporting AISS ultimately legitimizes Internet sovereignty norms in multilateral settings.[216] In Ethiopia and Sudan, the CCP has led workshops on managing public opinion, adopting key legislation, and implementing surveillance technologies.[217] Further, in Cambodia, the National Police were trained in the use of surveillance cameras by China's Ministry of Public Security, while in Sri Lanka, PLA officials trained Sri Lankan officials on website filtration practices.[218] Overall, China appears to be leading a "charm offensive" by cultivating media and government elites in a network of countries sympathetic to Internet sovereignty norms.[219] It uses prior relationships to host sessions offering tools for monitoring and maintaining a "positive energy public-opinion guidance system."[220]

China also hosts conferences "to convince foreign officials and businesspeople of its view of the Internet."[221] In January 2018, the China Electronic Standardization Institute oversaw a joint effort by 30 academic and industry organizations to

---

[213] Mueller, W*ill the Internet Fragment?*, 18-19, quoted in McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3839.

[214] Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders: How a Group of Often Overlooked Countries Could Hold the Keys to the Future of the Global Internet," *New America*, October 23, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/

[215] Nicholas D. Wright, "Global Competition," in Ahmed et al., "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," 32.

[216] Marcus Michaelsen and Marlies Glasius, "Authoritarian Practices in the Digital Age—Introduction," *International Journal of Communication* 12.7 (2018): 3788, https://ijoc.org/index.php/ijoc/article/view/8536

[217] Economy, "China's New Revolution: The Reign of Xi Jinping," 66-68.

[218] Khuon Narim, "Chinese Police Start Placing Surveillance Cameras," *Cambodia Daily,* July 16, 2015, https://english.cambodiadaily.com/news/chinese-police-start-placing-surveillance-cameras-88535; Bandula Sirimanna, "Chinese Here for Cyber Censorship," *Sunday Times*, February 14, 2010, www.sundaytimes.lk/100214/News/nws_02.html

[219] Adrian Shabaz, "The Rise of Digital Authoritarianism," *Freedom House*, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

[220] Ibid.

[221] Economy, "China's New Revolution," 66.

produce a "White Paper on Artificial Intelligence Standardization."[222] Such efforts promote Chinese AI companies' global competitiveness and set the rules in a strategically competitive, international environment. Meanwhile, regional security forums like the Shanghai Cooperation Organization (SCO) are focused sites of learning best practices and provide a platform to disseminate digital norms to the international community.[223] Discussions at these conferences are normally kept behind closed doors and disclosures are rarely, if ever, released in English.[224] Indeed, the SCO is composed of shared interests of maintaining regime stability; ergo, the propensity to view and identify ethnic groups and political opposition as a security threat is streamlined through the SCO framework.[225] McKune and Ahmed argue that the fact that both India—the world's largest democracy—and Pakistan have joined the SCO "demonstrates the significant potential for the diffusion of authoritarian norms and practices."[226]

The role China's security-industrial complex plays in setting international standards at the UN's International Telecommunication Union (ITU) is especially telling. The ITU, a crucial multilateral body of nearly 200 member states, "is a space where companies outside of North America and Europe tend to shape and drive standard development."[227] Ratified standards on facial recognition, video monitoring, and city and vehicle surveillance are "increasingly being authored by companies" like ZTE, Dahua, and China Telecom, and are commonly adopted by developing ITU member nations in the global South—who may often lack the capacity to design standards themselves.[228] Reflecting the strategic access to data resources and development of China's AISS sector, one global human rights expert remarked that "there are virtually no human rights, consumer protection,

---

[222] Jeffrey Ding, trans., "Excerpts from China's 'White Paper on Artificial Intelligence Standardization,'" ed. Paul Triolo, *New America*, June 20, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-excerpts-chinas-white-paper-artificial-intelligence-standardization/
[223] Deibert, "Authoritarianism Goes Global," 72; McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3842-3843.
[224] Deibert, "Authoritarianism Goes Global," 72.
[225] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3842.
[226] Ibid., 3843.
[227] Anna Gross, Madhumita Murgia, and Yuan Yang, "Chinese Tech Groups Shaping UN Facial Recognition Standards," *Financial Times*, December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67
[228] Ibid.

or data protection experts present in ITU standards meetings."[229] The result, for example, is that facial recognition draft standards on smart street light services are written to advantage the particular design of ZTE product's "back-end architecture and functionality."[230] Overall, Chinese companies have been responsible for "every submission to the UN for international standards on surveillance technology in the past three years…[and] half of the standards have already been approved."[231]

The June 2019 G20 Summit in Osaka placed China in opposition to Japan, the U.S., and the EU for the world governance over data, suggesting China will continue to be the primary norm entrepreneur for Internet sovereignty. Indeed, summit debates highlighted China's contrast from Japanese Prime Minister Shinzo Abe's "free flow of data with trust," a principle to promote cross-border data flows with protection.[232] However, China's resistance lies beyond sacrificing its ability to extract the data of importing countries from unprotected backdoors, as the present U.S. administration might solely assume.[233] Rather, China views multilateral settings as avenues to protest the current western-biased Internet order. As the *Economist* points out, data flows have largely concentrated where data is "most efficiently crunched"—the United States, which offers "the biggest and most innovative tech companies, but [also] plenty of potential customers, fibre optic cables, cheap power and land to build cavernous data centres[sic]."[234] Data localization practices are the antithesis, and China's encouragement of such practices strategically and subversively undermines the default network benefits accruing in the West. Accordingly, China's signature on the Osaka Declaration on the Digital Economy should not be viewed as conciliation, but rather the next step in the long game to convince other nations to limit the free flow of data and move

---

[229] Ibid.

[230] Ibid.

[231] Anna Gross and Madhumita Murgia, "China Shows Its Dominance in Surveillance Technology." *Financial Times*. December 27, 2019. https://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96

[232] Masumi Koizumi, "Japan's Pitch For Free Data Flows 'With Trust' Faces Uphill Battle At G20 Amid 'Splinternet' Fears," *Japan Times,* June 27, 2019, https://www.japantimes.co.jp/news/2019/06/27/business/tech/japans-pitch-free-data-flows-trust-faces-uphill-battle-g20-amid-splinternet-fears/

[233] Shubhajit Roy, "G-20 Osaka Summit: India Refuses To Sign Declaration On Free Flow Of Data Across Borders," *Indian Express,* June 29, 2019, https://indianexpress.com/article/india/g-20-osaka-summit-narendra-mod-india-declaration-on-free-flow-of-data-across-borders-shinzo-abe-5805846/

[234] "Governments Are Erecting Borders For Data," *Economist,* February 20, 2020, https://www.economist.com/special-report/2020/02/20/governments-are-erecting-borders-for-data

away from the western Internet. Indeed, the Declaration is merely an agreement for continued discussions. Already, several G20 countries have indicated their desire to keep data internally, as Indonesia, Egypt, South Africa, and India, which specifically cited the importance of data localization, elected not to sign the Declaration.[235] As Sacks and Sherman argue, the solidified norms over the global governance of data will, in turn, "influence AI competition, because not getting these data could limit how well tailored products are to different people."[236]

However, China's AISS empire grants it an alarmingly advantageous game-theoretic position for ushering in data localization and Internet sovereignty. Ironically, much of the modern data localization practices in place were initially prompted by a knee-jerk reaction to the 2013 Snowden revelations on foreign surveillance.[237] Since then, more and more countries have adopted data localization practices to keep data within their respective borders, like how China denies its citizens access to Wikipedia, Facebook, and large portions of Google or Iran established its 'Halal net' free from any western architecture.[238] At present, about 45 countries have adopted policies preventing data from leaving their geographic borders, a trend not limited to authoritarian states but one that includes Australia, South Korea, India, Philippines, Russia, and India.[239] China's AISS exports, on the one hand, left unfettered, enable the raw extraction of data from developing countries, which continues to feed the Chinese security-industrial complex with increasingly diverse, international data. On the other hand, as data becomes more recognized as an industrial resource, the scale and ease by which China's siphoning of countries citizen data is occurring may prompt a similar reaction seen in 2013 and further accelerate the data localization trend globally. This time, a data localization surge, will likely become a permanent shift in the future of the open Internet, since thirteen of the top twenty "Digital

---

[235] "G20 Summit: India Does Not Sign Osaka Declaration On Cross-Border Data Flow," *Scroll. in,* June 29, 2019, https://scroll.in/latest/928811/g20-summit-india-does-not-sign-osaka-declaration-on-cross-border-data-flow

[236] Sacks and Sherman, "The Global Data War Heats Up."

[237] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (report, Information Technology and Innovation Foundation, Washington DC, May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf

[238] Akash Kapur, "The Rising Threat of Digital Nationalism," *Wall Street Journal,* November 1, 2019, wsj.com/articles/the-rising-threat-of-digital-nationalism-11572620577

[239] Ibid.

Decider" states have imported China's AISS technology.[240]

The global pandemic world of COVID-19 represents another vehicle of strategic import for AISS and Internet sovereignty norm-setting. The virus has arrived when democracy is already in a geopolitically fragile state, "and it risks exacerbating democratic backsliding . . . and potentially reset[ting] the terms of the global debate on the merits of authoritarianism versus democracy."[241] It has accelerated the use of new surveillance technologies, as governments from Israel to Hong Kong attempt to flatten the curve with locational tracking and contact tracing efforts.[242] Indeed, perhaps one of the "most significant legacies" of the global pandemic world is its increased reliance on AISS, "prompted by the public health need to more closely monitor citizens."[243] Wright's contention that Western democracies design, implement, and export its own surveillance model "as the world rebuilds in the wake of the pandemic" further underscores the geopolitically strategic importance of AISS and the capriciousness of international AI norms.[244] However, under pressure to control the pandemic, even ostensibly liberal democracies may be inclined to experiment and implement antidemocratic surveillance measures. For example, the Indian government has "pressured local media to maintain positive coverage" on its responses to the virus,[245] while states like Karnataka and Telangana are requiring the submission of selfies geo-tagged to periodically confirm the location of citizens.[246]

Without permanently accepted global standards for ethical, legal, and practical implications of AI, key players like China have a special incentive to shape norms that favor their needs. For instance, one prominent PLA scholar, Ye Zheng, described the "logic of Internet sovereignty as a starting point" for

---

[240] Morgus, Woolbright and Sherman, "The Digital Deciders."

[241] Frances Z. Brown, Saskia Brechenmacher, and Thomas Carothers, "How Will the Coronavirus Reshape Democracy and Governance Globally?" *Carnegie Endowment for International Peace,* April 6, 2020, https://carnegieendowment.org/2020/04/06/how-will-coronavirus-reshape-democracy-and-governance-globally-pub-81470

[242] Ibid.

[243] Wright, "Coronavirus and the Future of Surveillance."

[244] Ibid.

[245] Brown, Brechenmacher, and Carothers, "How Will the Coronavirus Reshape Democracy and Governance Globally?"

[246] Venkat Ananth, "As Covid-19 Cases Rise In India, "Covtech" Based Surveillance Intensifies," *Economic Times,* March 30, 2020, https://economictimes.indiatimes.com/news/politics-and-nation/as-covid-19-cases-rise-in-india-covtech-based-surveillance-intensifies/articleshow/74876078.cms

control over cyberspace.[247] The more countries the PRC can bring under its model of governance, the lesser the threat to Internet sovereignty. The market of AISS should thus be viewed as an "active shaper of the preferences, practices, and policies" of those who partake, as the services provided by China create critical solutions to state problems.[248] As Feldstein argues, such technology concentrates power in the hands of the few, furnishing even the heads of ostensibly democratic governments the strong incentive to "arm security forces with intrusive technology, monitor the activities of political opponents and civil society, and take preemptive action against potential challenges to their authority."[249] The dangers are greatest for backsliding regimes, the most common contemporaneous route to authoritarianism, as illiberal governments may find natural interest in such tools enabling protection from mass discontent.[250] The increased global propensity to adopt Chinese practices is heightened with each successive government integration, which is likely to induce others to follow. For example, replicas of Ecuador's ECU-911 system were sold to Venezuela, Bolivia, and Angola.[251] Laura Steckman therefore concludes that China's "dual-pronged" approach of outreach partnerships and export agreements grant it:

> …access to the world's cutting-edge researchers to develop AI faster, and the ability to export its internally-developed technologies, whether developed entirely domestically or in collaboration with partners, to (re)shape the world through AI. In the process, China may influence educational curricula, set international standards for AI, selectively highlight or impede the spread of news and other information, gain access to extensive personal data, and use the technologies to disseminate its ideological perspective.[252]

The breadth of China's AISS empire has helped ensure norms of Internet sovereignty are a viable alternative to the U.S. dominated open Internet norms.

---

[247] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3837.
[248] Deibert, "Authoritarianism Goes Global," 73.
[249] Feldstein, "The Road to Digital Unfreedom," 48.
[250] Ibid., 42-43.
[251] Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *New York Times,* April 19, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html
[252] Steckman, "Pathways to Lead in Artificial Intelligence," 82.

Rhetoric of Altruism: Paying for Harm

  The last relevant indicator of neocolonialism in the colonialist heritage is the framing of self-serving engagements with developing countries as benevolent. As Antiwi-Boateng argues, the rhetoric of altruism cloaked European colonialism as a civilizing mission to remedy the perceived "ignorance and cultural backwardness" of Africa.[253] Similarly, China uses carefully selected phrases of common prosperity to convey a "win-win" relationship.[254] For example, on the Belt and Road Initiative, Chinese Foreign Minister Wang Yi said the following:

> Africa faces challenges of maintaining peace and security, and of promoting development and revitalization. In response to the needs, China will step up mediation in regional hotspots as well as cooperation with African countries on unconventional security threats such as terrorism, piracy and natural disaster…China welcomes our African brothers and sisters in getting on board of [sic] the fast train of development.[255]

Antiwi-Boateng contends that this rhetoric accomplishes a distinction from previous Western practices, and therefore hides the "self-seeking results of economic extraction and unbridled opportunism" beneath its words.[256] As he argues, the framing of a win-win relationship should therefore be viewed more as a "pragmatic response to a new world order shaped by international norms and institutions."[257]

  Through the exportation of AISS, China gains data for industrialization purposes, renders countries dependent on its surveillance markets, and protects its regime's domestic Internet practices. In effect, these ramifications pose a serious risk to these countries' sovereignty and stability. However, this asymmetrical exchange is largely masked by its framing of the interaction as altruistic. Freedom House has reported that many countries are shifting to the "China Model" of surveillance control, because China has convinced such countries that its AISS systems are particularly advantageous for ideas of state sovereignty.[258] Companies like Huawei

---

[253] Antiwi-Boateng, "New World Order Neo-Colonialism," 183.
[254] Ibid.
[255] Li Xiang, "China to Boost Ties, Advance Belt and Road Initiative in Africa," *China Daily,* March 3, 2018. http://www.chinadaily.com.cn/a/201803/08/WS5aa0d6b3a3106e7dcc140675.html
[256] Osman Antiwi-Boateng, "New World Order Neo-Colonialism," 183.
[257] Ibid., 178.
[258] Gallagher, "Export Laws," 35-37.

market their products to the Middle East as an extremism prevention tool, and to Latin America as a weapon for crime prevention.[259] In February 2011, Ecuador, financed by Chinese loans, received an AISS system in exchange for oil; soon after, it had signed away over $19 billion in exchange for credit facilities towards a variety of Chinese infrastructure projects like hydroelectric dams.[260] In July 2018, Xi Jinping publicly called for the Arab world to import its "social stability" systems for around $150 million.[261] Most notably, in the deal with Zimbabwe, China claimed it as an example of win-win diplomacy. Former Zimbabwean Ambassador to China, Christopher Mutsvangwa, agreed: "China has proved to be our all-weather friend and this time around, we have approached them to spearhead our AI revolution in Zimbabwe."[262]

Similarly, Internet sovereignty is strategically framed as a new model of international relations that better represents the interests of the developing world.[263] At regional security forums, China has attempted to convince developing nations that Internet sovereignty is in their best interests. Arguing that the present Internet infrastructure system was established by the West, China frames Internet sovereignty as preferable since the present core infrastructure concentrates benefits in wealthy democracies while the majority of Internet users hail from developing countries.[264]

Violating Internet Sovereignty

According to President Xi Jinping, "no country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security."[265] Despite calls for international balance, China has failed to heed its own words. In April 2018, President Xi Jinping announced at the National Cyber Security

[259] Feldstein, "The Global Expansion of AI Surveillance," 17.
[260] Mozur, Kessel, and Chan, "Made in China, Exported to the World."
[261] Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China," *Foreign Policy*, August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/
[262] Problem Masau, "Zimbabwe: Chinese Tech Revolution Comes to Zimbabwe," *AllAfrica,* October 9, 2019, https://allafrica.com/stories/201910090185.html
[263] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3835, 3837, 3839.
[264] Ibid., 3839-40.
[265] Xi Jinping, "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference" (speech, Second World Internet Conference, Wuzhen, China, December 16, 2015), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/ zyjh_665391/t1327570.shtml

and Informationization Work Conference that he will move forward with "the construction of China as a cyber superpower."[266] Given that AI has become the driver of a new industrial revolution and international markets, China has formulated long term strategies to enhance its AI development sectors, increasingly the main battlefield of competition with the United States.[267] China has set up barriers for the entry of foreign AI companies and complicates international firms' ability to have data flow outside its borders.[268] Meanwhile, domestic artificial intelligence companies are expected to control 80% of the domestic market by 2025.[269] In the long term, China aims to exert influence on the global Internet, while exploiting the presently fragmented Internet norms for personal gain. China's extraction of countries' data, pursuit of unsaturated markets, and desire for global prestige further attest to the aims of Chinese AI supremacy.

China has also routinely violated Internet sovereignty norms through pervasive digital intrusion and espionage of extraterritorial targets.[270] In addition to the unauthorized siphoning of information from the African Union,[271] analysis of AISS projects within the BRI by Cave et al. show "serious concerns about the erosion of sovereignty for host nations, such as when a recipient government doesn't have full control of the operations, management, digital infrastructure or data being generated through those projects."[272] Co-located within its Great Firewall, which limits access to online materials deemed inappropriate by the CCP, an offensive weapon "inserts malicious content in unencrypted Web traffic to overseas users."[273]

Moreover, China's specialization in AISS and market dominance grant it a high degree of control over the user experience of such technology. Unfairly trained AI or imbalanced data sets create the opportunity for bias, which poses significant issues for exporting AI technologies abroad. The exporter possesses the power to shape norms of implementation for recipients of its technology. Through its AISS technology, China may have an opportunity to shape global privacy norms. In

---

[266] Gallagher, "Export Laws," 35.
[267] Wang and Chen, "Rising Sino-US Competition in Artificial Intelligence," 241.
[268] Ibid.
[269] Economy, "China's New Revolution," 65.
[270] See Bill Marczak et al., "China's Great Cannon" (brief, Citizen Lab, Munk School of Global Affairs, University of Toronto, April 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon/
[271] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 73-74.
[272] Cave et al., "Mapping China's Technology Giants," 9.
[273] McKune and Ahmed, "The Contestation and Shaping of Cyber Norms," 3843.

some cases, AISS is exported to support authoritarian-leaning leaders, in others it is done to undermine international law and threaten sovereignty.[274] However, the "right to choose" Internet policies and practices without international interference appears to be largely absent from such instances of China's engagement.

Entrenching Corruption

The most pernicious Chinese engagement with its empire, however, has been its impact on clients' corruption and state-sponsored abuse. Cheeseman, Lynch, and Willis describe how digital technologies like AISS may simply be too powerful to resist, as "the failure of digital checks and balances often renders an electoral process even more vulnerable to rigging than it was before."[275] In Zimbabwe, facial recognition is operated at political rallies to monitor and track opponents of the regime.[276] Amid hyperinflation and widespread shortages of food and medicine from economic meltdown, Venezuela's Fatherland Card has been used to curb discontent and allocate resources towards loyalists.[277] During the 2018 elections, Venezuela voters were asked to scan their Fatherland Cards to register for a prize and those who did received a message thanking them for supporting Maduro.[278]

Chinese companies operate with little scrutiny and consideration for corporate social responsibility, according to Mozur.[279] Indeed, when interviewed, Su Qingfeng, head of ZTE's Venezuela unit simply remarked: "we are just developing our market."[280] In Zimbabwe's telecommunications sector, Huawei has played a central role, continuing multimillion-dollar contracts with companies like NetOne, which has been the subject of a number of corruption allegations.[281] For Ecuador, one former legislator commented that they lack the capacity to demand information from China on systems like ECU-911.[282] In

---

[274] Economy, "China's New Revolution," 69.

[275] Nic Cheeseman, Gabrielle Lynch, and Justin Willis, "Digital Dilemmas: The Unintended Consequences of Election Technology," *Democratization* 25.8 (2018): 1397, 1400, 1405-08, https://doi.org/10.1080/13510347.2018.1470165

[276] Gallagher, "Export Laws," 35-37.

[277] Berwick, "How ZTE Helps Venezuela Create China-Style Social Control."

[278] Ibid.

[279] Mozur, Kessel, and Chan, "Made in China, Exported to the World."

[280] Berwick, "How ZTE Helps Venezuela Create China-Style Social Control."

[281] Cave et al., "Mapping China's Technology Giants," 11-12.

[282] Mozur, Kessel, and Chan, "Made in China, Exported to the World."

Uganda and Zambia, the effects of Chinese involvement were even more salient. Huawei aided government officials in spying on political opponents, including intercepting "encrypted communications and social media, and using cell data to track their whereabouts."[283] Ugandan security officials were encouraged to travel to Algeria to study Huawei's operations in Algiers, and shortly after, Uganda imported a Huawei AISS system for $126 million.[284] Moreover, China's company Semptian viewed regimes with a record of detaining and torturing critics as potential clients, including Saudi Arabia, Belarus, and Sudan.[285] Hikvision similarly provided Iran with facial recognition and smart policing software.[286] In this way, China is cementing the fate of authoritarianism within such countries. As Feldstein argues, the potential of AI to repress and weather discontent for an illiberal regime is all too enticing, leading to even steeper deterioration into authoritarian governance.[287]

While China's AISS exports may be welcomed by these countries, the consequences in terms of governance and human rights is ultimately negative, particularly for those with records of abuse.[288] Privacy norms may be altered universally as intensive, ubiquitous surveillance is instead normalized. China's maintenance of the win-win narrative behind exporting AISS, and disregard for its social and governmental impact on host countries largely resembles the neocolonialist tradition. Indeed, digitization is being pursued by countries that "lack the political will and institutional framework necessary for it to function effectively."[289] Rather than a 'civilizing' mission, at the expense of such countries, China has embarked on a 'securitization' mission, with the added effect of materially exploiting and normatively shaping their clients in favor of Chinese geopolitical interests.

Conclusion

With a projected 14% increase in Global GDP due to AI, the development of AI has become a recognized manifestation of a country's comprehensive

---

[283] Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

[284] Ibid.

[285] Gallagher, "Export Laws," 37.

[286] Feldstein, "The Global Expansion of AI Surveillance," Appendix 1.

[287] Feldstein, "The Road to Digital Unfreedom," 42-43.

[288] Gwagwa, "How China's Artificial Intelligence is shaping Geopolitical and Geoeconomic Global Order Summary."

[289] Cheeseman, Lynch, and Willis, "Digital Dilemmas: The Unintended Consequences of Election Technology," 1400.

power.[290] In this newfound international, technological environment, China's AISS exportation is one method of acquiring and enhancing control. Much like 19th century European colonialists imposed sovereignty over water or land, China's pursuit of global primacy in cyberspace is a similar assertion of authority.

However, China recognizes it is currently losing the race for the position of world AI leader. In fact, China is lagging when compared to the U.S. in every single indicator besides data.[291] In response, China has resolved to pursue specialization in the one field it has a relative advantage in: AISS. In one year alone, China has sought over 900 patents in the domain of facial recognition, outpacing a mere 150 patents from the U.S.[292]

China feeds and protects such specialization initiatives through the exertion of neocolonialist influence over its empire of importers: over 50 countries have received Chinese AISS technologies. China extracts unique data resources from these countries for the purposes of its industrialization. China certainly recognizes the potential of data, particularly as it endeavors to leapfrog the United States' AI position. Indeed, ground-truth data, like tax returns or medical records, is mostly in the hands of governments, but it is precisely that data which is crucial for developing AI surveillance states. Thus, data exchange requirements, like those of Zimbabwe's AISS contract—where massive troves of Zimbabwean biometric data were harnessed to enhance China's algorithms— are to be expected from China's AISS export partnerships. Even without such contracts, merely possessing China's infrastructure leads a country to be susceptible to backdoors of information—and China has already constructed AISS systems in over 18 countries.[293]

Similarly, China's specialization in AISS during the digitization of the global South, as well as the reverse wave of authoritarianism in developing countries, suggests a strategic manipulation of interests for market gain. Purporting to provide state solutions to developing countries' problems, China has categorically enhanced the capacity of nations to weather discontented publics—the key threat to regime survival today. In making such technology

---

[290] Wang and Chen, "Rising Sino-US Competition in Artificial Intelligence," 242-243.
[291] Ding, "Deciphering China's AI Dream." 27.
[292] Jeffrey Ding, "Is China Taking the Lead in AI?" Interview by Frieda Klotz, *MIT Sloan Management Review*, April 30, 2020, https://sloanreview.mit.edu/article/is-china-taking-the-lead-in-ai/
[293] Clarke and Knake, "The Internet Freedom League," 184-192.

available through financing measures, China has ultimately created a market-based reliance on its AISS political solutions: its customers always want more methods of control. As with Venezuela, this is likely to result in further purchases of AISS upgrades from China, locking in an unsaturated market for AISS exportation.

In the colonial past, the British and French empires exerted influence beyond regional spheres to pursue national interests without external interference. Likewise, China pursues countries in Africa and beyond with a similar platform and has pursued protections for its rise to AI power. Holding training sessions on the application of its technology in 36 countries and using international conferences to diffuse favorable norms to recipients of its technology, China has secured Internet sovereignty as a successful alternative to the present normative consensus. In the international contest for Internet norms, China has become the champion of Internet sovereignty and has used the market power of its companies—Alibaba, Tencent, Baidu, and Huawei—to recruit developing countries into its fold. The end result is the creation of a normative protectorate of countries, who enable AISS practices to continue unhindered by Western, rights-based criticisms.

Overall, China has used its position to gain asymmetrically from the countries to which it exports AISS. But, just as European powers once did with their 'civilizing' mission, China uses similar altruistic rhetoric. China effectively sells countries on the idea that AISS and Internet sovereignty norms are key for developing countries' interests while hiding more pernicious effects from the limelight. Describing its data extraction from Zimbabwe as "win-win" is particularly telling, but so is China's routine violation of Internet sovereignty norms. As China aspires for cyber hegemony, it pervasively intrudes on nations' sovereignty to information, and embeds its own national values within the technology it exports. Moreover, it feigns ignorance when it directly, as in the case of Uganda and Zambia, or indirectly undermines nations' political processes with its technologies. Seeking out clientele with records of state-sponsored human rights abuses and corruption only further deepens the dive into authoritarianism presently taking place. The net effect is negative, as China's technology increasingly becomes a conduit for human rights abuses and backwards progress.

Such elements—resource extraction, pursuit of unsaturated markets, desire for global prestige, and altruistic rhetoric—are indicative of neocolonialist exchange between China and the recipient countries. However, constrained by a set of international norms prohibiting explicit exploitation, China has been forced to add substance to its rhetorical 'win-win' framing. In this context, it appears

that China still contributes to the wealth gap, satisfying Nkrumah's condition of neocolonialism. Its heedless extraction of developing countries' data is applied to improve its algorithms far beyond what may be capable in the countries it pulls; its tapping into the heartstrings of countries' desires for security and stability creates a tangible reliance on AISS; its adoption of Internet sovereignty norms enable a more oppressive domestic censorship operation, a geopolitical lottery for China; and its exportation of AISS to countries with sub-par human rights records suggest the entrenchment of deleterious corruption. Such consequences do not echo the positive win-win rhetoric underlying China's AISS exports.

Earlier it was also argued that the presence of mutual beneficence should not acquit China's exportation of AISS as neocolonialist, because, in large part, China's mutual beneficence emerged solely out of conformity to international standards. But a key shortcoming of this paper is its failure to address two questions: If countries are seeking and implementing AISS as intended, why should China's intentions matter? Moreover, could not any mutually-beneficial, strategic partnership between a wealthier and less-wealthy country be explained away as neocolonialism 'boxed in' by international normative constraints?

One avenue to addressing such questions might involve a comparative case with U.S. AI geopolitical market policy. Future scholarship could contextualize the neocolonialist nature of the AI international marketplace with such comparison. Indeed, an analysis of how the U.S. interacts with its own set of international Internet norms, along with an evaluation of the dynamics between the U.S. and its recipient countries would prove useful for understanding the norms of AI superpower's market operations.

Nonetheless, since China exerts its position as a specialist in AISS to set the rules of engagement with the countries who import its technology, China's specialization in AISS should be viewed as a strategic foreign policy decision for cyberspace domination. COVID-19 is but the latest example highlighting the crucial importance of AISS and testing the Western democratic model of governance. Undoubtedly, more instances will follow as the technology evolves and proves its capacity to solve crises, from extremism to epidemics. In this way, China's abuse of developing countries' resources, markets, soft power, and trust on its path to AISS domination can and should be discerned as neocolonialism. But the questions above highlight the lack of clarity in what precisely qualifies as neocolonialism today. Future research would therefore also benefit from an

updated conception of neocolonialism that adequately factors in international normative constraints in its calculus of exploitation.

References

Ahmed, Shazeda, Natasha E. Bajema, and Samuel Bendett et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright. White paper, Strategic Multilayer Assessment Periodic Publication, U.S. Department of Defense, Washington DC, December 2018. https://nsiteam.com/social/wp-content/uploads/2019/03/AI-China-Russia-Global-WP_FINAL2_fromMariah8mar2019_ndw11mar2019.pdf

"AI and Control of COVID-19 Coronavirus." *Council of Europe.* https://www.coe.int/en/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus

Aidoo, Richard, and Steven Hess. "Non-Interference 2.0: China's Evolving Foreign Policy towards a Changing Africa." *Journal of Current Chinese Affairs* 44.1 (2015): 107-139. https://doi.org/10.1177/186810261504400105

Allen, Greg, and Taniel Chan. "Artificial Intelligence and National Security." Report, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, MA, July 2017. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Allen, Karen. "What China Hopes to Achieve with First Peacekeeping Mission." *BBC News.* December 2, 2015. https://www.bbc.com/news/world-africa-34976580

Allison, Simon. "Fixing China's Image in Africa, One Student at a Time." *Guardian.* July 5, 2013. https://www.theguardian.com/world/2013/jul/31/china-africa-students-scholarship-programme

Ananth, Venkat. "As Covid-19 Cases Rise In India, "Covtech" Based Surveillance Intensifies." *Economic Times.* March 30, 2020. https://economictimes.indiatimes.com/news/politics-and-nation/as-covid-19-cases-rise-in-india-covtech-based-surveillance-intensifies/articleshow/74876078.cms

Antiwi-Boateng, Osman. "New World Order Neo-Colonialism: A Contextual Comparison of Contemporary China and European Colonization in

Africa." *Africology: The Journal of Pan African Studies* 10.2 (2017): 177-195. https://www.jpanafrican.org/docs/vol10no2/10.2-13-Antwi-Boateng.pdf

Benaim, Daniel, and Hollie R. Gilman. "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders." *Slate,* August 9, 2018. https://slate.com/technology/2018/08/chinas-export-of-cutting-edge-surveillance-and-facial-recognition-technology-will-empower-authoritarians-worldwide.html

Berwick, Angus. "How ZTE Helps Venezuela Create China-Style Social Control." *Reuters*. November 14, 2018. https://www.reuters.com/investigates/special-report/venezuela-zte/

Brown, Frances Z., Saskia Brechenmacher, and Thomas Carothers. "How Will the Coronavirus Reshape Democracy and Governance Globally?" *Carnegie Endowment for International Peace.* April 6, 2020. https://carnegieendowment.org/2020/04/06/how-will-coronavirus-reshape-democracy-and-governance-globally-pub-81470

Campbell, Horace. "China in Africa: Challenging US Global Hegemony." *Third World Quarterly* 29.1 (2008): 89-105. https://doi.org/10.1080/01436590701726517

Campos, Indira, and Alex Vines. "Angola and China: A Pragmatic Partnership." Paper presented at the Center for Strategic and International Studies Conference on "Prospects for Improving U.S.-China-Africa Cooperation," Washington DC, December 5, 2007. Published March 2008. https://www.csis.org/analysis/angola-and-china-pragmatic-partnership

Castro, Daniel, Michael McLaughlin, and Eline Chivot. "Who Is Winning the AI Race: China, the EU or the United States?" Report, Center for Data Innovation, Washington DC, August 2019. http://www2.datainnovation.org/2019-china-eu-us-ai.pdf

Cave, Danielle, Samantha Hoffman, and Alex Joske et al. "Mapping China's Technology Giants." Report, Issues Paper 15/2019, International Cyber Policy Centre, Australian Strategic Policy Institute, April 18, 2019. https://www.aspi.org.au/report/mapping-chinas-tech-giants

Cheeseman, Nic, Gabrielle Lynch, and Justin Willis. "Digital Dilemmas: The Unintended Consequences of Election Technology." *Democratization* 25.8 (2018): 1397-1418. https://doi.org/10.1080/13510347.2018.1470165

Chen Wenjie. "Chinese Investment in Africa Is More Diverse and Welcome than You Think," *Quartz Africa*. August 26, 2015. https://qz.com/africa/488589/chinese-investment-in-africa-is-more-diverse-and-welcomed-than-we-give-it-credit/

———, David Dollar, and Tang Heiwai. "Why is China Investing in Africa? Evidence from the Firm Level." *Brookings Institute.* August 2015. https://www.brookings.edu/wp-content/uploads/2016/06/Why-is-China-investing-in-Africa.pdf

Chutel, Lynsey. "China Is Exporting Facial Recognition Software To Africa, Expanding Its Vast Database." *Quartz Africa*. May 25, 2018. https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

Clarke, Richard A., and Rob Knake. "The Internet Freedom League: How to Push Back Against the Authoritarian Assault on the Web." Foreign Affairs 98.5 (2019): 184-192.

Cook, Sarah. "China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and U.S. Responses." *Freedom House.* September 26, 2018. https://freedomhouse.org/article/chinas-cyber-superpower-strategy-implementation-Internet-freedom-implications-and-us#Ftn31

Cordesman, Anthony H., Ashley Hess, and Nicholas S. Yarosh. *Chinese Military Modernization and Force Development: A Western Perspective.* Lanham, MD: Rowman & Littlefield, 2013. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130930_Cordesman_ChineseMilitaryModernization_Web.pdf

Cory, Nigel. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Report, Information Technology and Innovation Foundation, Washington DC, May 2017. http://www2.itif.org/2017-cross-border-data-flows.pdf

"Data Leak Reveals How China 'Brainwashes' Uighurs in Prison Camps." *BBC*

News. November 24, 2019. https://www.bbc.com/news/world-asia-china-50511063

Deibert, Ron. "Authoritarianism Goes Global: Cyberspace Under Siege." *Journal of Democracy* 26.3 (2015): 64-78. http://doi.org/10.1353/jod.2015.0051

Demchak, Chris C. "Four Horsemen of AI Conflict: Scale, Speed, Foreknowledge, and Strategic Coherence." In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 100-106.

Ding, Jeffrey. "China's AI Superpower Dream with Jeffrey Ding." Interview by Lucas Perry in *AI Alignment Podcast,* August 16, 2019. Produced by the Future of Life Institute. Podcast, MP3 audio, 1:12:20. https://futureoflife.org/2019/08/16/chinas-ai-superpower-dream-with-jeffrey-ding/

———. "Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI." Report, Future of Humanity Institute, Oxford University, March 2018. https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

———, trans. "Excerpts from China's 'White Paper on Artificial Intelligence Standardization.'" Edited by Paul Triolo. *New America*. June 20, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-excerpts-chinas-white-paper-artificial-intelligence-standardization/

———. "The Interests Behind China's AI Dream." In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 37-41.

Doffman, Zak. "Warning As Millions Of Chinese-Made Cameras Can Be Hacked To Spy On Users." *Forbes*. August 3, 2019. https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/#301ed6c06bf2

Dreher, Axel, and Andrea Fuchs. "Rogue Aid? An Empirical Analysis of China's Aid Allocation." *Canadian Journal of Economics* 48.3 (2015): 988-1023. https://doi.org/10.1111/caje.12166

Economy, Elizabeth C. "China's New Revolution: The Reign of Xi Jinping." *Foreign Affairs* 97.3 (2018): 60-74.

Feldstein, Steven. "The Global Expansion of AI Surveillance." Working paper, Carnegie Endowment for International Peace, Washington DC, September 17, 2019. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

———. "The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression." *Journal of Democracy* 30.1 (2019): 40-52. https://doi.org/10.1353/jod.2019.0003

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52.4 (1998): 887-917. https://doi.org/10.1162/002081898550789

"G20 Summit: India Does Not Sign Osaka Declaration On Cross-Border Data Flow." *Scroll.in.* June 29, 2019. https://scroll.in/latest/928811/g20-summit-india-does-not-sign-osaka-declaration-on-cross-border-data-flow

Gallagher, Ryan. "Export Laws." *Index on Censorship* 48.3 (2019): 35-37. https://doi.org/10.1177/0306422019876445

Godoy, Jilio. "China Swaggers into Europe's Backyard." *Asia Times.* November 17, 2006. http://www.atimes.com/atimes/China_Business/HK17Cb03.html

"Governments Are Erecting Borders For Data." *Economist.* February 20, 2020. https://www.economist.com/special-report/2020/02/20/governments-are-erecting-borders-for-data

Gross, Anna, Madhumita Murgia, and Yang Yuan, "Chinese Tech Groups Shaping UN Facial Recognition Standards." *Financial Times.* December 1, 2019. https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67

Gwagwa, Arthur E. "How China's Artificial Intelligence is Shaping Geopolitical and Geoeconomic Global Order." *Medium.* April 2, 2019. https://medium.com/@arthurgwagwa/how-chinas-artificial-intelligence-is-shaping-

geopolitical-and-geoeconomic-global-order-fb7fa341bd3c

Herrero, Alicia-Garcia. "China's Investments In Africa: What The Data Really Say, and the Implications For Europe." *Forbes*. July 24, 2019. https://www.forbes.com/sites/aliciagarciaherrero/2019/07/24/chinas-investments-in-africa-what-the-data-really-says-and-the-implications-for-europe/#a723dc8661f9

Hess, Steve, and Richard Aidoo, "Beyond the Rhetoric: Noninterference in China's African Policy." *African and Asian Studies* 9.3 (2010): 356-383. https://doi.org/10.1163/156921010X516003

Huntington, Samuel P. "Democracy's Third Wave." *Journal of Democracy* 2.2 (1991): 12-34. https://doi.org/10.1353/jod.1991.0016

"International Cyberspace Cooperation Strategy." Policy document no. CD/2092, Conference on Disarmament, Ministry of Foreign Affairs of the People's Republic of China and State Information Office, March 1, 2017. https://undocs.org/CD/2092

Johnson, Steve. "China By Far The Largest Investor In African Infrastructure." *Financial Times*. November 30, 2015. http://www.ft.com/intl/cms/s/3/716545c0-9529-11e5-ac15-0f7f7945adba.html

Kapur, Akash. "The Rising Threat of Digital Nationalism." *Wall Street Journal*. November 1, 2019. wsj.com/articles/the-rising-threat-of-digital-nationalism-11572620577

Kerry, Cameron F. "Protecting Privacy in an AI-Driven World." *Brookings Institution*. February 10, 2020. https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

Kharpal, Arjun. "China's Surveillance Tech is Spreading Globally, Raising Concerns About Beijing's Influence." *CNBC*. October 8, 2019. https://www.cnbc.com/2019/10/08/china-is-exporting-surveillance-tech-like-facial-recognition-globally.html

———. "Coronavirus Could Be a 'Catalyst' for China to Boost Its Mass Surveillance Machine, Experts Say." *CNBC*. February 4, 2020. https://www.cnbc.com/2020/02/25/coronavirus-china-to-boost-mass-

surveillance-machine-experts-say.html

———. "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice." *CNBC*. March 4, 2019. https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

———. "Use of Surveillance to Fight Coronavirus Raises Concerns About Government Power After Pandemic Ends." *CNBC*. March 26, 2020. https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html

Kissinger, Henry A. "How the Enlightenment Ends." *The Atlantic.* June 2018. https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/

Koizumi, Masumi. "Japan's Pitch For Free Data Flows 'With Trust' Faces Uphill Battle At G20 Amid 'Splinternet' Fears." *Japan Times.* June 27, 2019. https://www.japantimes.co.jp/news/2019/06/27/business/tech/japans-pitch-free-data-flows-trust-faces-uphill-battle-g20-amid-splinternet-fears/

Kwet, Michael. "The Rise of Smart Camera Networks, and Why We Should Ban Them." *The Intercept*. January 26, 2020. https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks/

Lake, Brenden M., Tomer D. Ullman, and Joshua B. Tenenbaum et al. "Building Machines That Learn and Think like People." *Behavioral and Brain Sciences* 40 (2017): 1-72. https://doi.org/10.1017/S0140525X16001837

Large, Daniel. "Beyond 'Dragon in the Bush': The Study of China-Africa Relations." *African Affairs* 107.426 (2008): 45-61. https://doi.org/10.1093/afraf/adm069

Lee, Kai-Fu. "Kai-Fu Lee's Perspectives On Two Global Leaders In Artificial Intelligence: China and the United States." Interview by Michael Chui, *McKinsey Global Institute,* June 14, 2018. https://www.mckinsey.com/featured-insights/artificial-intelligence/kai-fu-lees-perspectives-on-two-global-leaders-in-artificial-intelligence-china-and-the-united-states

Lee, Margaret C. "The 21st Century Scramble for Africa." *Journal of Contemporary African Studies* 24.3 (2006): 303-330. https://doi.

org/10.1080/02589000600976570

Lewis, James A. "AI and China's Unstoppable Global Rise." In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 94-99.

Li Anshan. "China and Africa: Policy and Challenges." *China Security* 3.3 (2007): 68-94. http://cpfd.cnki.com.cn/Article/CPFDTOTAL-BDFZ201305003010.htm

Li Xiang. "China to Boost Ties, Advance Belt and Road Initiative in Africa." *China Daily.* March 3, 2018. http://www.chinadaily.com.cn/a/201803/08/WS5aa0d6b3a3106e7dcc140675.html

Lim, Alvin C-H. "Africa and China's 21st Century Maritime Silk Road." *Asia-Pacific Journal* 13.11.3 (2015): 1-14. https://apjjf.org/-Alvin-Cheng-Hin-Lim/4296/article.pdf

Lohr, Steve. "Facial Recognition Is Accurate, If You're a White Guy." *New York Times.* February 9, 2018. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Lührman, Anna, Sirianne Dahlum, and Staffan I. Lindberg et al. "Democracy for All? V-Dem Annual Democracy Report 2018." Report, V-Dem Institute, University of Gothenburg, May 28, 2018. https://doi.org/10.2139/ssrn.3345071

Mai Jun. "Ecuador Is Fighting Crime Using Chinese Surveillance Technology." *South China Morning Post.* Jan 22, 2018. https://www.scmp.com/news/china/diplomacy-defence/article/2129912/ecuador-fighting-crime-using-chinese-surveillance

Mallett-Outtrim, Ryan. "30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets." *Venezuela Analysis.* November 27, 2013. https://venezuelanalysis.com/news/10198

Marczak, Bill, Nicolas Weaver, and Jakub Dalek et al. "China's Great Cannon." Brief, Citizen Lab, Munk School of Global Affairs, University of Toronto, April 10, 2015. https://citizenlab.ca/2015/04/chinas-great-cannon/

Marr, Bernard. "Here's Why Data Is Not The New Oil." *Forbes*. March 5, 2018. https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#16c01a773aa9

Masau, Problem. "Zimbabwe: Chinese Tech Revolution Comes to Zimbabwe." *AllAfrica*. October 9, 2019. https://allafrica.com/stories/201910090185.html

McKune, Sarah, and Shazeda Ahmed. "The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda." *International Journal of Communication* 12 (2018): 3835-3855. https://ijoc.org/index.php/ijoc/article/view/8540/2461

Michaelsen, Marcus, and Marlies Glasius. "Authoritarian Practices in the Digital Age—Introduction." *International Journal of Communication* 12 (2018): 2788-3794. https://ijoc.org/index.php/ijoc/article/view/8536

"MISA Zimbabwe's Submission on the Surveillance Industry and Human Rights in Zimbabwe." Report submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Media Institute of Southern Africa, Harare, Zimbabwe, February 15, 2019. https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/MISA%20ZIMBABWE.pdf

Morgus, Robert, Jocelyn Woolbright, and Justin Sherman. "The Digital Deciders: How a Group of Often Overlooked Countries Could Hold the Keys to the Future of the Global Internet." *New America*. October 23, 2018. https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/

Mozur, Paul, Jonah M. Kessel, and Melissa Chan. "Made in China, Exported to the World: The Surveillance State." *New York Times*. April 19, 2019. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Mueller, Milton. *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Malden, MA: Polity Press, 2017.

Mulas, Victor, Eva Clemente, and Arturo Muente-Kunigami. "Smart Cities." *World Bank*. January 8, 2015. https://www.worldbank.org/en/topic/digitaldevelopment/brief/smart-cities

Narim, Khuon. "Chinese Police Start Placing Surveillance Cameras." *Cambodia Daily.* July 16, 2015. https://english.cambodiadaily.com/news/chinese-police-start-placing-surveillance-cameras-88535

Nkrumah, Kwame. *Neo-Colonialism: The Last Stage of Imperialism.* London: Thomas Nelson & Sons, 1965.

Nwoke, Chibuzo N. "The Scramble for Africa: a Strategic Policy Framework," *Nigerian Journal of International Affairs* 33. 2 (2007): 31-55.

Parkinson, Joe, Nicholas Bariyo, and Josh Chin. "Huawei Technicians Helped African Governments Spy—Chinese Giant's Staff Aided Cybersecurity Forces' Snooping On Opposition." *Wall Street Journal.* August 15, 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

Pollard, Martin. "Even Mask-Wearers Can Be ID'd, China Facial Recognition Firm Says." *Reuters.* March 9, 2020. https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL

Poushter, Jacob. "Smartphone Ownership Rates Skyrocket in Many Emerging Economies, but Digital Divide Remains." *Pew Research Center.* February 22, 2016. https://www.pewresearch.org/global/2016/02/22/smartphone-ownership-rates-skyrocket-in-many-emerging-economies-but-digital-divide-remains

Provost, Claire, and Rich Harris. "China Commits Billions in Aid to Africa as Part of Charm Offensive." *Guardian.* April 29, 2013. https://www.theguardian.com/global-development/interactive/2013/apr/29/china-commits-billions-aid-africa-interactive

Qiang Xiao. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30.1 (2019): 53-67. https://doi.org/10.1353/jod.2019.0004

Rich, Timothy S., and Sterling Recker. "Understanding Sino-African Relations: Neocolonialism or a New Era?" *Journal of International and Area Studies* 20.1 (2013): 61-76. https://www.jstor.org/stable/43111515

Rieland, Randy. "Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?" *Smithsonian Magazine*. March 5, 2018. https://www. smithsonianmag.com/innovation/artificial-intelligence-is-now-usedpredict-crime-is-it-biased-180968337/

Rollet, Charles. "Ecuador's All-Seeing Eye Is Made in China." *Foreign Policy*. August 9, 2018. https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/

Roque, Paula C. "China in Mozambique: A Cautious Approach Country Case Study." Report, SAIIA Occasional Paper 23, South African Institute of International Affairs, Braamfontein, South Africa, January 2009. https://media.africaportal.org/documents/SAIIA_Occasional_Paper_no_23.pdf

Roy, Shubhajit. "G-20 Osaka Summit: India Refuses To Sign Declaration On Free Flow Of Data Across Borders." *Indian Express*. June 29, 2019. https://indianexpress.com/article/india/g-20-osaka-summit-narendra-mod-india-declaration-on-free-flow-of-data-across-borders-shinzo-abe-5805846/

Sacks, Samm, and Justin Sherman. "The Global Data War Heats Up." *Atlantic*. June 26, 2019. https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/

Sadowski, Jathan, Anna Carlson, and Natalie Osborne. "Darwin's 'Smart City' Project is About Surveillance and Control." *Conversation*. February 4, 2020. https://theconversation.com/darwins-smart-city-project-is-about-surveillance-and-control-127118

Schneier, Bruce. "China Isn't the Only Problem With 5G." *Foreign Policy*. January 10, 2020. https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance

Shabaz, Adrian. "The Rise of Digital Authoritarianism." *Freedom House*. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Sirimanna, Bandula. "Chinese Here for Cyber Censorship." *Sunday Times*. February 14, 2010. www.sundaytimes.lk/100214/News/nws_02.html

"Smart Cities: Utopian Vision, Dystopian Reality." Report, Privacy International, October 31, 2017. http://www.privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality

Stanley, Jay. "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy," Report, American Civil Liberties Union, New York, June 17, 2019. https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf

Steckman, Laura. "Pathways to Lead in Artificial Intelligence." In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 78-84.

Tang, David, Esther Colwill, and Judy Fujii-Hwang et al. "Seeing What Matters: A New Paradigm for Public Safety Powered by Responsible AI." Report, Accenture Strategy and Western Digital Corporation, 2018. https://www.accenture.com/_acnmedia/pdf-94/accenture-value-data-seeing-what-matters.pdf

"The Five Principles of Peaceful Coexistence: The Time-Tested Guideline of China's Policy With Neighbors." *Ministry of Foreign Affairs of the People's Republic of China*. July 30, 2014. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/t1179045.shtml

"The World's Most Valuable Resource Is No Longer Oil, But Data." *Economist*. May 6, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Verhoeven, Harry. "Is Beijing's Non-Interference Policy History? How Africa is Changing China." *The Washington Quarterly* 37.2 (2014): 55-70. https://doi.org/10.1080/0163660X.2014.926209

"Video Surveillance as the Foundation of 'Safe City' in Kenya." *Huawei.* https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya

Wang You and Chen Dingding. "Rising Sino-US Competition in Artificial Intelligence." *China Quarterly of International Strategic Studies* 4.2 (2018): 241-258. https://doi.org/10.1142/S2377740018500148

Wang, Eudora. "China To Take Nearly Half Of Global Face Recognition Device

Market By 2023." *China Money Network*. August 23, 2018. https://www. chinamoneynetwork.com/2018/08/23/china-to-take-nearly-half-of-global-face-recognition-device-market-by-2023

Weber, Valentin. "Understanding the Global Ramifications of China's Information Controls Model." In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 72-77.

Webster, Graham, Rogier Creemers, and Paul Triolo et al., trans. "China's 'New Generation Artificial Intelligence Development Plan' (2017)." *New America.* August 1, 2017. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

Weiss, Jessica C. "A World Safe for Autocracy? China's Rise and the Future of Global Politics." *Foreign Affairs* 98.4 (2019): 92-102.

Wright, Nicholas D. "AI and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy." In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 16-29.

———. "Coronavirus and the Future of Surveillance: Democracies Must Offer an Alternative to Authoritarian Solutions." *Foreign Affairs*. April 6, 2020. https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance

———. "Global Competition." In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 30-36.

———. "The Technologies: What Specifically is New?" In Ahmed et al. "Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," edited by Nicholas D. Wright, 1-9.

Xi Jinping. "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference." Speech, Second World Internet Conference, Wuzhen, China, December 16, 2015. http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/

zyjh_665391/t1327570.shtml

Xu Jing, Zhao Rui, and Zhu Feng et al. "Attention-Aware Compositional Network for Person Re-Identification." Paper presented at the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, June 18-22, 2018.

Xue Lan, Liang Zheng, and Yu Zhen et al., "China AI Development Report 2018." Report, China Institute for Science and Technology Policy, Tsinghua University, Beijing, July 2018. http://www.sppm.tsinghua.edu.cn/eWebEditor/UploadFile/China_AI_development_report_2018.pdf

Zhang Hongpei. "Chinese Facial ID Tech To Land In Africa." *Global Times.* May 17, 2018. http://www.globaltimes.cn/content/1102797.shtml

Zhao Suisheng. "A Neo-Colonialist Predator or Development Partner? China's Engagement and Rebalance in Africa." *Journal of Contemporary China* 23.90 (2014): 1033-1052. https://doi.org/10.1080/10670564.2014.898893