Expanding Digital Authoritarianism?
The Effect of Chinese AI Surveillance Technology on Digital Repression in Africa

Candidate number: NDBQ6

Word count: 9,972

Dissertation submitted in part-fulfilment of the Masters Course in Security Studies, UCL, September 2021

Abstract

The rapid development of artificial intelligence (AI) is hailed as having the potential to advance society in transformative ways. Yet, a growing number of states are leveraging advanced AI surveillance technology (AIST) not only to surveil, but also to repress citizens. Journalists, think tanks and academics alike fear that China, in particular, is advancing authoritarianism abroad by exporting advanced AIST to regimes with poor human rights records or illiberal forms of governance. Existing literature fails, however, to systematically investigate the relationship between China's AIST exports and authoritarian practices in importing countries. This paper proposes a causal mechanism to investigate the effect of African governments' adoption of China's AIST on digital repression practices in Africa. Using two-way fixed effect regression, results demonstrate that adoption of Chinese AIST increases digital repression in Africa on only one of five digital repression indicators. Adoption of Chinese AIST is otherwise associated with a decrease of digital repression on the other four digital repression indicators. The findings suggest that AIST potentially reduces the need for digital repression, allowing us to critically assess the assumptions made in the causal mechanism as well as certain dynamics highlighted in the repression technology literature.

Table of Contents

List of Figures

Appendices

List of Abbreviations

2FE - Two-way fixed effect regression
AI - Artificial intelligence
AIST - Artificial intelligence surveillance technology
ATT - Average treatment effect on the treated group
BRI - Belt and Road Initiative
DSP - Digital Society Project
DSR - Digital Silk Road
DV - Dependent variable
ICT - Information and communication technology
IV - Independent variable
UNCTAD - United Nations Conference for Trade and Development

Introduction

The rapid development of artificial intelligence (AI) is lauded as advancing society in transformative ways. In the field of international security, there is an increasing focus on how AI can augment both offensive and defensive cyber capabilities (Johnson, 2019a, 2019b). Yet, an increasing tally of states are deploying advanced AI surveillance tools to surveil citizens to maintain political control (Feldstein, 2019). A prominent example is the vast network of advanced AI facial recognition technology used to track and control the Uyghurs, a large Muslim minority in northern China (Mozur, 2019).

In recent years, China has '[aggressively marketed] the transfer of advanced AI technology around the globe', particularly across the Middle East and North and Sub-Saharan Africa through the Digital Silk Road initiative (Crosston, 2020, p. 149). Chinese equipment is usually purchased using loans from China with the objective of enhancing public safety. However, these exports do not exclusively improve the cyberinfrastructure of developing nations. Think tanks, scholars and journalists assert that China is also advancing censorship, disinformation and public opinion-shaping tools that support regimes with poor human rights records or illiberal forms of governance (Hoffman, 2018, 2019; Chin, 2019; Lilkov, 2020).

This contributes to a wider policy debate concerning technological advancements that contribute to a rise of authoritarianism and a decline of democracy. In fact, there is a growing consensus that the world is experiencing a 'third wave of autocratization' (Lührmann and Lindberg, 2019). V-Dem estimates that 35 percent of the world's population are currently living through

autocratization, an inverse-democratization process whereby political rights and freedoms are increasingly limited (Alizada *et al.*, 2021). Digital tools such as AIST have the potential to enhance states' abilities to repress. Knowledge on the dynamics and trade-offs behind repression tactics remains scarce, but understanding their logic provides a crucial contribution to our understanding of authoritarianism and how such regimes may proliferate.

It is important to highlight that AI is not one single technology. Rather, AI 'incorporates information acquisition objectives, logical reasoning principles and self-correcting capacities' (Feldstein, 2019, p. 5). For example, machine learning, a subfield of AI, incorporates statistical processes to analyse massive amounts of data to discern patterns and predict future uses (ibid). Thus, AIST are surveillance technologies that integrate AI into their processing. AIST can be disaggregated into three main applications: smart city/safe city technologies; facial recognition systems; and smart policing (ibid).

This paper seeks to understand the effect of the adoption of Chinese AIST on digital repression in Africa. The paper presents the following hypothesis: African governments' adoption of China's AIST leads to an increase in digital repression practices in Africa. Digital repression is defined as 'the use of information and communications technology to surveil, coerce, or manipulate individuals or groups [to] deter specific activities or beliefs that challenge the state' (Feldstein, 2021, p. 25). This encompasses techniques related to monitoring; censorship; social manipulation and disinformation; internet shutdowns; and targeted persecution of online users (ibid).

This study aims to contribute to the literature in three ways. Though many case studies demonstrate China's hand in strengthening authoritarian tendencies abroad through AIST exports, they do not explicitly propose dynamics through which this pattern occurs. This paper proposes a causal mechanism for the relationship between China's AIST exports and digital repression based on a set of interlinked assumptions from the literature. Secondly, as the majority of scholarship at the intersection of China and digital technologies is qualitative, the paper fills a methodological gap in the literature by designing and conducting a quantitative study to test the empirical relationship between adoption of AIST and digital repression in Africa. Finally, the paper attempts to contribute to the budding field of emerging technology in international security by highlighting the effects of AI applications in surveillance technology.

The paper proceeds with a review of the literature on authoritarianism, information and communication technologies (ICTs) and China's digital authoritarianism. Next, the theoretical argument and methodology are presented. The paper proposes a causal mechanism and a quantitative research design to empirically test the hypothesis, utilising an original dataset compiled using public data. The subsequent section presents the results of the analysis before discussing the implications of the results, considering limitations and improvements and proposing avenues for further research. The paper concludes by summarizing its key contributions and considering policy implications.

Literature Review

This section presents the state of the literature on authoritarianism and ICTs, before reviewing the literature on China's digital authoritarianism specifically.

Authoritarianism and ICTs

Technological advancements have spurred the study of the role of digital technologies in phenomena such as political competition (Acemoglu and Robinson, 2006); violent and nonviolent conflict (Shapiro and Siegel, 2010; King, Pan and Roberts, 2013; Dafoe and Lyall, 2015; Shapiro and Weidmann, 2015); and authoritarian politics (Farrell, 2012; Reuter and Szakonyi, 2015; Rød and Weidmann, 2015; Weidmann and Rød, 2019).

Much of the literature on authoritarian politics and digital technologies is split into two camps: liberation versus repression technology. Those in the liberation camp argue for the emancipatory or democratizing potential of digital technologies, asserting that ICTs empower civil society by spreading democratic values, lowering mobilization costs, facilitating mobilised dissent and driving citizen capability to challenge state power (Diamond, 2010; Howard, 2010; Lynch, 2011; Hussain and Howard, 2013; Pierskalla and Hollenbach, 2013). Those in the repression camp, meanwhile, argue that ICTs strengthen authoritarian rule by buttressing regime repression capabilities (Rød and Weidmann, 2015; Groshek and Mays, 2017; Weidmann and Rød, 2019).

The internet and social media have traditionally been regarded as ‘liberation technologies’ that transform how information is produced, consumed and shared. In China, for example, citizens exposed to alternative online views evaluate government performance more negatively (Tang and Huhe, 2014). Generally, the internet undermines pro-authoritarian ideals by increasing information flow (Ruijgrok, 2017; Shahbaz, 2018). This exposes citizens to foreign values such as democracy and freedom (Diamond, 2010; Lynch, 2011; Pierskalla and Hollenbach, 2013) and

catalyses protest through reducing communication costs and informational uncertainty for potential protesters (Ruijgrok, 2017).

Social media similarly undermines authoritarian rule by facilitating collective mobilization (Shirky, 2009; Eltahawy, 2010; Castells, 2013). The Arab Spring, for example, has been popularly dubbed a 'Facebook/Twitter revolution' (Passini, 2012; Reardon, 2012; Al-Jenaibi, 2016). Anecdotal evidence and cross-national quantitative data from the 2010-11 Tunisian revolution support the liberation technology claims (Ruijgrok, 2017).

The successful application of ICTs to authoritarian contexts led to a shift in discourse, however. The repression technology perspective asserts that digital technologies challenge democratic politics (Tufekci, 2014; Bennett and Livingston, 2018), portraying authoritarian governments as savvy technology users that exploit technology to control information. Technological innovation particularly reinforces authoritarian governance, empowering authoritarian states by increasing their capacity to repress civil society and prevent the mobilisation of opposition (Frantz, Kendall-Taylor and Wright, 2020; Kendall-Taylor, Frantz and Wright, 2020; Dragu and Lupu, 2021). Consequently, we observe an increasing reliance on digital repression in dictatorships (Frantz, Kendall-Taylor and Wright, 2020).

The internet has also received significant attention in the 'repression technology' literature. Case studies of countries in separate regions suggest that the internet is not necessarily a threat to authoritarian regimes (Kalathil and Boas, 2003). One study suggests that some autocracies fare well under a level of internet diffusion that is neither too high nor too low (Chang and Lin,

2020). Although Milner (2006) demonstrates that internet expansion is more likely in democracies, other evidence suggests that certain pro-market, pro-growth autocratic states actually welcome internet expansion due to the economic payoffs it yields (Corrales and Westhoff, 2006). As states learn to control the internet's content, the tendency of authoritarian regimes to restrict internet use declines (ibid).

Recent large-N quantitative studies demonstrate that internet expansion in autocracies has no effect on regime change towards democracy or on the quality of political institutions, however (Groshek, 2010; Rød and Weidmann, 2015; Weidmann *et al.*, 2016; Groshek and Mays, 2017; Weidmann and Rød, 2019). Rapid internet adoption appears to strengthen authoritarian rule by facilitating the use of tools that benefit the regime, including sophisticated digital monitoring (Rød and Weidmann, 2015; Dragu and Lupu, 2021). Notwithstanding, internet technology can benefit citizens in the short term by nurturing episodes of unrest (Ruijgrok, 2017; Weidmann and Rød, 2019), especially when citizens leverage high-speed internet specifically for political ends (Stoycheff and Nisbet, 2014; Stoycheff, Nisbet and Epstein, 2016). Yet in the long-term, protest levels are kept low because control of the internet is asymmetrical (Weidmann and Rød, 2019; Chang and Lin, 2020). The regime controls internet expansion and provision. Thus, regimes can censor online information, networks and resources related to civil society (ibid). Further, internet provision allows for digital surveillance that enables targeted forms of repression, particularly in regions with loose government control (Gohdes, 2020).

Authoritarian regimes tend to *promote* ICTs whose content they can control (Corrales and Westhoff, 2006). This is because legitimation is key to their survival - many autocracies persist

by cultivating popular consent and societal approval of their application of power (Gerschewski, 2013; Feldstein, 2021). The Chinese government, for example, uses internet censorship to allow government criticism - albeit limited - while suppressing calls for collective action (King, Pan and Roberts, 2013). Moreover, when citizens have additional instruments for receiving information, the government-citizen information asymmetry decreases as citizens are able to obtain more information about the government (Ivanova, Yakovleva and Selenteva, 2020). This new alignment creates advantages for the state as many authoritarian regimes leverage the internet to provide pro-government information (Zeng, 2015).

Internet and social media surveillance also enable the collection of accurate mass opinion, allowing authoritarian regimes to create tailored policies (King, Pan and Roberts, 2013; Gunitsky, 2015; Singer and Brooking, 2018). Online surveillance creates information asymmetries between state and citizen, whereby obscure internet monitoring allows the state to observe patterns of behaviour unknown to the citizen (Robbins and Henschke, 2017). Governments have honed such surveillance tools for the identification and imprisonment of political dissidents to prevent social unrest (Diamond, 2010; MacKinnon, 2011; Xu, 2021). Consequently, surveillance reduces the need for authoritarian governments to resort to reactive, violent, state-led repression. Instead, they employ preventive repression to address threats before mass protests mobilise (Greitens, 2016; Xu, 2021).

Not only do states engage in preventive repression, but citizens restrict behaviour when being surveilled. Stoycheff *et al.* (2019) find that surveillance significantly deters individuals'

intentions to engage in illegal offences and that such restrictive effects are not limited to any specific online population or political context.

The expansion of surveillance tools is enabled by the development of data applications (Liang *et al.*, 2018). Today, the extensive use of AI and big data-enabled surveillance augments the state's capacity to predict citizen behaviour (van Dijck, 2014). Technologies such as facial recognition, automated text analysis and big data analysis open a host of new avenues for citizen control. Findings indicate that at least 77 out of 179 countries are actively using AI and big-data technology for public surveillance purposes (Feldstein, 2021, p. 227). Authoritarian regimes apply advanced surveillance technologies to neutralise potential dissidents through targeted repression and preventive arrests (Frantz, Kendall-Taylor and Wright, 2020; Xu, 2021). Despite the rapid pace of technological advancement, little has been written on how AI will affect surveillance and repression practices. To date, the only existing database on AI and big-data global surveillance was created by Feldstein (2019).

China's 'Digital Authoritarianism'

Despite the limited literature on the fusion of new technologies and repression, there is a notable focus on China in the discourse, especially China's application of AI to surveillance technologies and China's 'export' of digital authoritarianism.

In line with the repression technology perspective, China exploits digital technologies to maintain and strengthen the one-party system (Hoffman, 2017; Liang *et al.*, 2018; Cave *et al.*,

2019; Zeng, 2020). Some scholars have characterised the Chinese government's approach to online communications as 'networked authoritarianism' (MacKinnon, 2011), whereby the government uses the technology as an instrument to elicit, respond to and direct public opinion and more efficiently provide public services (Tsang, 2009; He and Warren, 2011). As a result, perceptions of regime performance are enhanced (Hoffman, 2019; Chen and Greitens, 2021).

According to Zeng (2016, 2020), China also uses technology to maintain coercive control, utilising big data and AI to move towards what Zeng (2016, p. 1452) describes as 'Big Brother 2.0'. For example, a vast network of advanced AI facial recognition technology is used to look for and track the activities of the Uyghurs, a large Muslim minority in Northern China (Daly, 2019; Mozur, 2019).

Zeng, however, argues that such use of massive digital data may undermine authoritarian governance by intensifying power struggles: if sensitive data is concentrated in the hands of a few powerful individuals or agencies and is misused, regime legitimacy and elite cohesion may suffer (2016). Accordingly, Pan (2017, p. 167) demonstrates that 'China's ability to censor social media rests on the dominance of domestic firms in China's market'.

Notwithstanding, the Chinese case suggests that AI-powered surveillance is becoming a powerful tool for digital repression (Feldstein, 2019; Qiang, 2019). Beijing's increasing exports of AI surveillance tools alongside its experience using digital tools for surveillance feeds a fear that China is driving a future of tech-enhanced authoritarianism, whereby AIST is being

strategically deployed to restrict civil society in foreign countries - especially in emerging markets with low human rights records (Gwagwa and Garbe, 2018; Crosston, 2020).

The inability of emerging markets to manage and analyse large amounts of data themselves has created an opportunity for private high-tech companies to support governments with data collection and analysis (Fuchs *et al.*, 2013; Kendall-Taylor, Frantz and Wright, 2020). In this vein, many authors claim that the global uptake of Chinese AI surveillance technology throughout the developing world is driven mainly by the Digital Silk Road (DSR), the technology component of China's Belt and Road Initiative (BRI) (Khalil, 2020). Programmes subsidised by the DSR have generated in the ballpark of US$17 billion in loans and investments in projects such as smart cities and big data initiatives (Artigas, 2017; Hillman and McCalpin, 2019; Yan, 2019; Khalil, 2020; Lilkov, 2020).

Expanding digital authoritarianism relies on exporting technologies that provide useful services (Hoffman, 2019). In many cases, the provision of technical infrastructure through the BRI builds the 'digital backbone' of recipient states, providing high-speed internet in deprived zones; lays fibre optic cables; commercialises smartphones with default Chinese apps; and promotes agreements with governments to use BeiDou (the Chinese GPS) for military and civilian purposes (Lilkov, 2020; Oreglia, Ren and Liao, 2021). 'Useful' technology exports also support governments' domestic surveillance programmes: at least 80 countries from Latin America, Asia and Africa have adopted Huawei's Safe City solutions or other Chinese surveillance platforms (Feldstein, 2019; Khalil, 2020) alongside training in 'public opinion guidance' - purportedly a euphemism for censorship (Mozur, Kessel and Chan, 2019).

Some authors assert that such private-public partnerships blur the line between public and private sectors, making it increasingly difficult to discern the primary actors responsible for the expansion of surveillance (Gates, 2011; Fuchs *et al.*, 2013). Notwithstanding, Chinese support for the repressive capabilities of AIST recipient states are demonstrated through case studies, focusing particularly on Africa (Gravett, 2020). For example, assisted by a US$240 million loan from China, Chinese startup CloudWalk began to supply Zimbabwe with facial recognition technology for a national surveillance programme (Chutel, 2018; Romaniuk and Burgers, 2018). Ethiopia also has a history of heavy surveillance and repression activities and its ICT sector has increasing involvement from high-tech Chinese firms such as Huawei and ZTE (Grinberg, 2017; Meester, 2021).

The literature on China's digital authoritarianism provides valuable insight into China's fusion of AI and surveillance technology. There is strong anecdotal evidence to support claims that China supports repressive practices abroad through AIST exports, illustrating how these technologies are being deployed abroad to support repressive practices in many countries (Chutel, 2018; Freyburg and Garbe, 2018; Shahbaz, 2018; Cave *et al.*, 2019; Hillman and McCalpin, 2019; Frantz, Kendall-Taylor and Wright, 2020; Khalil, 2020; Meester, 2021). Yet, though 'China is often cited as a prime example of how authoritarian regimes can retain control, [...] there has been limited research on whether China's online censorship practices can be replicated in other authoritarian regimes' at all (Pan, 2017, p. 167). Moreover, the specific *processes* by which advanced technologies lead to increased digital repression in recipient states are overlooked;

studies tend to focus on single states, thus findings cannot be generalised. To date, no quantitative studies have been conducted to assess qualitative claims or vice versa.

Summary

The literature on authoritarianism and ICTs demonstrates that 'liberation technology' scholars largely failed to account for the role of the state in controlling internet provision and expansion, thus controlling the flow of information to citizens and preventing high levels of social unrest in the long run. The 'repression technology' camp demonstrates that digital tools enable authoritarian governments to adapt policies according to precise, aggregated data on citizens (Xu, 2021). Though there is little recent study on how *new* technologies affect repression, there is a notable focus on China's 'export' of digital authoritarianism using AIST. Studies fail, however, to systematically investigate the relationship between China's AIST exports and authoritarianism in importing countries. This highlights a need to study whether China's technology transfers affect repression abroad, as purported by popular media (Romaniuk and Burgers, 2018; Chin, 2019); think tanks (Hoffman, 2017, 2018; Shahbaz, 2018; Cheney, 2019; Kendall-Taylor, Frantz and Wright, 2020; Lilkov, 2020; Sahin, 2020); and academia (MacKinnon, 2011; Liang *et al.*, 2018; Gravett, 2020; Zeng, 2020; Feldstein, 2021).

Theoretical Argument

Why African governments' adoption of China's AI surveillance technologies may lead to an increase in digital repression practices in Africa

Many scholars claim that China promotes authoritarianism abroad via exports of AIST, allowing existing repressive states to exploit the technology for political gain (Cheney, 2019; Khalil, 2020; Sahin, 2020; Feldstein, 2021; Gamso, 2021). To investigate the relationship between AIST and repression, this paper proposes a causal mechanism (summarised in figure 1) that rests on a set of interlinked assumptions drawn from existing work.

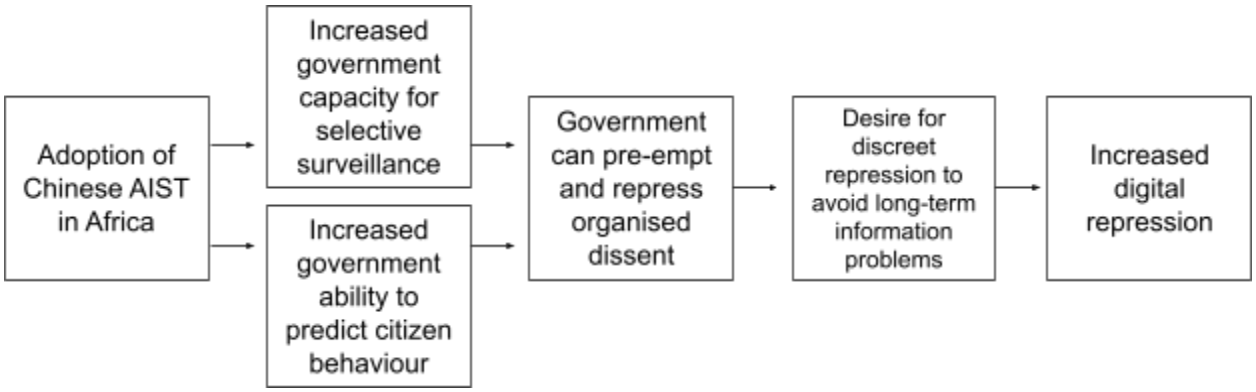


Figure 1. Chinese AIST adoption leading to increased digital repression in Africa

Academic literature and popular media purport that Chinese AIST are proliferating in emerging markets with poor human rights records (Gwagwa and Garbe, 2018; Crosston, 2020; Lilkov, 2020). This paper focuses particularly on Africa. Though many African states already have a

history of surveilling citizens (Breckenridge, 2014; Dwyer and Molony, 2019), financial loans and technical training via the DSR have made it possible for China's technology firms to supply African governments with advanced surveillance technologies integrating AI and big data applications (Hoffman, 2019; Gravett, 2020; Khalil, 2020). Thus, the starting assumption is that adopting AIST increases the recipient governments' surveillance capacity, by automating the data collection process and aggregating data from multiple sources to monitor individuals' whereabouts and behaviour (Andrejevic and Gates, 2014, p. 190; Feldstein, 2021, p. 216).

Previously, information asymmetries in government-citizen interactions were more balanced, neither side possessing a sufficiently realistic model of the counterparty (Ivanova, Yakovleva and Selenteva, 2020). As a result of government adoption of Chinese AIST, however, a large power differential between government and private citizens emerges (Tufekci, 2014; Robbins and Henschke, 2017). Governments can now discover new patterns on citizen behaviour that were formerly inaccessible, for example inferring citizens' past or future locations and actions (Lyon, 2014; van Dijck, 2014; Khalil, 2020). A myriad of studies concur that technological innovation benefits the government more than citizens by facilitating sophisticated digital monitoring (King, Pan and Roberts, 2013; Gunitsky, 2015; Rød and Weidmann, 2015; Singer and Brooking, 2018; Weidmann and Rød, 2019; Dragu and Lupu, 2021). Consequently, governments can more easily identify political dissidents and censor resources related to regime opposition, thereby making organised dissent more costly (Diamond, 2010; MacKinnon, 2011; Rød and Weidmann, 2015; Weidmann and Rød, 2019; Chang and Lin, 2020; Dragu and Lupu, 2021; Xu, 2021). Further, governments that deploy AIST can now undertake individualised and selective scrutiny to

oversee political and social activities that pose a threat to the regime and stifle them before they multiply (Andrejevic and Gates, 2014; Shorey and Howard, 2016; Liang *et al.*, 2018).

Governments can pre-empt political dissent and ensure regime maintenance using force, but such physical coercion is costly because it threatens to create a presumption of regime illegitimacy (DeMeritt, 2016). Regime legitimacy is crucial for the stability of autocracies as it ensures popular support for the government (Gerschewski, 2013; Morgenbesser, 2017), particularly in Africa (Letsa, 2017). Moreover, excessively violent or widespread physical repression resulting from government surveillance may shape behaviour over time, deterring citizens from revealing their 'true preferences' and 'exacerbating the authoritarian information problem in the long run' (Xu, 2021, p. 313). However, if governments employ less visible forms of repression, citizens are less likely to hide their regime preferences (Xu, 2021). Governments, therefore, are incentivized to make repression less visible to maintain uncertainty about their repression targets and avoid augmenting future information problems (ibid).

Pursuing digital strategies runs a lower risk of undermining regime legitimacy as they are less obtrusive than conventional, violent tactics (Feldstein, 2021). Digital repression is thereby less prone to domestic and international condemnation, while still allowing for the maintenance of political control (ibid). Digital repression, defined by Feldstein (2021, p. 25) is 'the use of information and communications technology to surveil, coerce, or manipulate individuals or groups [to] deter specific activities or beliefs that challenge the state'. This includes 'surveillance, censorship, social manipulation and disinformation, internet shutdowns and targeted persecution of online users' (ibid). Thus, in line with Weidmann and Rød (2019) and

Feldstein (2021), digital repression strategies are assumed to both partly substitute as well as enhance governments' abilities to carry out traditional, physical forms of repression.

Therefore, similar to how protest levels are kept low in the long-term because the regime controls internet expansion (Weidmann and Rød, 2019; Chang and Lin, 2020), governments can monopolise AIST to resolve information problems related to discerning citizen's true regime sentiments. Governments can use AIST to identify, monitor and track potential regime opponents and deploy preventive *digital* repression in place of physical coercion to neutralise them before they pose concrete threats to the government (Dragu and Lupu, 2021; Xu, 2021). This is particularly useful to control secluded religious or ethnic populations (Xu, 2021), particularly prevalent in Africa. Hence, African states also adopt new, anticipatory surveillance models, whereby surveillance is no longer used only to monitor specific actions, but to pre-empt them (Halper, 2010; Gravett, 2020; Khalil, 2020). Thus, the paper proposes the following hypothesis:

H: African governments' adoption of China's AI surveillance technologies leads to an increase in digital repression in Africa.

To summarise, the proposed causal mechanism is encapsulated as follows. Many African governments currently already employ surveillance, but financial loans and technical training via the DSR have made it possible for China's technology firms to supply African governments with advanced surveillance technologies integrating AI and big data applications. The potent analytical power of AI means that states that employ China's AIST will observe a substantial increase in domestic surveillance capacity by being able to predict patterns in citizen action.

These governments will begin to adopt anticipatory surveillance models as a result, to stifle dissent before it arises. However, as physical coercion is costly and may shape behavioural incentives in ways that are detrimental to the regime, governments will privilege digital over physical repression to stifle dissent. Thus, the adoption of China's AIST will lead to an increase in digital repression as governments can track potential regime dissidents and deploy preventive digital repression to neutralise them before they undermine the regime.

Research Design

Numerous case studies assert that China spreads its model of digital repression in African states through its export of AI surveillance technologies (Cave *et al.*, 2019; Hillman and McCalpin, 2019; Gravett, 2020; Lilkov, 2020; Sahin, 2020). Quantitative analysis, however, remains extremely scarce and digital repression remains particularly understudied. Thus, to fill a methodological gap in the literature and test the causal effect of China's exports of AIST on digital repression in Africa, this paper proposes a quantitative analysis using a two-way fixed effect (2FE) regression.

Data

This paper utilises a panel dataset compiled by the author using data drawn from publicly available sources (refer to appendix A for the full list of variables and sources). Panel data are used to observe the behaviour of different entities across time (e.g. Maness and Valeriano, 2016, pp. 309–317). Thus, the dataset records 1,092 observations for 52 African countries between

2000 to 2020. To facilitate data collection, the study utilised only countries coded as an African economy according to the United Nations Conference for Trade and Development (UNCTAD) online data centre (refer to appendix B for the full list of African countries included in the analysis).

Case studies in the literature and news articles focus on Africa, suggesting a natural focal point for this study (Cave *et al.*, 2019; Hillman and McCalpin, 2019; Gravett, 2020; Lilkov, 2020; Sahin, 2020). Further, Feldstein's AI global surveillance index (2019) specifies the origin country of AIST for adopting countries - specifically, whether the technology adopted by the country is Chinese- or US-made. African countries utilise only Chinese-made AIST. Comparatively, countries in Latin America and Eastern Europe with high rates of Chinese AIST adoption also utilise US AIST (ibid). Consequently, Africa is the best focus for this study because it reduces the likelihood of confounding. After controlling for the relevant variables, we can assume that any changes in digital repression observed can be attributed to the adoption of Chinese AIST.

The beginning of the time period was chosen because US-China trade relations were established in 2000, followed by China's formal accession to the WTO in 2001 (CFR, no date). Both events increased China's global economic outreach (ibid). The time period extends as recently as possible given the yet-emerging nature of AI technology; thus, the time period continues until 2020 according to availability of public data. Due to government opacity regarding surveillance use, the main issue for this study is the near impossibility of identifying the precise year AIST systems were deployed (Feldstein, 2019). Thus, the study assumes that each country in the

dataset adopted Chinese AIST in 2017 and continued utilising it until 2020. Hence the treatment years 2017-2020.

The study assumes that 2017 was the year in which most countries adopted AIST because of the lack of news coverage on the technology pre-2017, Feldstein (2019, p. 3) stating that 'the majority of sources referenced by the index occur between 2017 and 2019'. To ensure reliability, this date was cross-referenced with China's export data. UNCTAD's 'digital economy' data includes international trade in ICT services, defined as the 'wholesale of computers, computer peripheral equipment and software' (UNCTAD, 2009, p. 33). As AIST can be classified as software, we can assume that ICT services encompass trade in AIST. Indeed, we observe a steep uptick in China's ICT services exports from 2017: China's international trade in ICT services as a percentage of total trade in services soared from 12.17% in 2017 to 17.34% in 2018, continuing to rise thereafter (refer to appendix C for a visualisation). This seems coherent with the introduction of the DSR in 2015, when technologies integrating artificial intelligence, big data and smart cities began to be sold by Chinese tech firms in Africa (Oreglia et al., 2021; Greene and Triolo, 2020). It is reasonable, therefore, to assume 2017 as the year of African countries' Chinese AIST adoption as this was when China's trade in ICT services (including AIST) spiked following the establishment of the DSR.

Independent variable

The independent variable (IV) is the country's adoption of Chinese AIST (*ctech*), a binary variable coded as 1 if the country adopted Chinese AIST and 0 otherwise. As aforementioned, the treatment years are 2017 to 2020. Hence, the independent variable is coded as 1 for each year

from 2017-2020 and 0 otherwise. Therefore, the dataset includes a total of 36 countries in the control group (countries that did not adopt Chinese AIST); and 16 countries in the treatment group (countries that adopted Chinese AIST) (appendix B summarises the full list of African countries included in the analysis with indications of which countries adopted Chinese AIST).

Data on which countries utilise Chinese AIST is drawn from Feldstein's (2019) AI global surveillance index, the first and only existing database on the global expansion of AI surveillance. Index data was aggregated utilising open-source reporting, 'including news articles, websites, corporate documents, academic articles, NGO reports, expert submissions, and other public sources' (Feldstein, 2019, p. 6). Sources were categorised into tiered levels of reliability and accuracy and content analysis was then used to incorporate multiple sources to determine the presence of AIST and the corresponding companies (ibid). Consequently, a comprehensive database of countries that have adopted AIST is produced.

Dependent variable

The dependent variable (DV), digital repression, is operationalised using five digital repression indicators from the Digital Society Project (DSP) dataset (Mechkova *et al.*, 2020):

1. government domestic dissemination of false information (*smgovdom*);
2. government internet shutdown (*smgovshut*);
3. government social media shutdown (*smgovsm*);
4. government social media censorship (*smgovsmcenprc*);
5. arrests for posting political content online (*smarrest*).

The variables are ordinal, aggregating ratings provided by multiple country experts to provide a value ranging from -5 to 5 (Mechkova *et al.*, 2021). A value of -5 indicates that the government is extremely likely to engage in digitally repressive behaviour while 5 indicates that the government is extremely unlikely to do so.

The dependent variables were chosen using Feldstein's digital repression taxonomy (2021). Feldstein (2021, p. 25) categorises digital repression into five indicators and utilises DSP variables to measure each form of digital repression. However, Feldstein (2021) includes DSP variables that measure both government digital repression capacity and practice, whereas this study focuses only on digital repression practices. Therefore, for this study, only the DSP variables that measure government repression practices are maintained from Feldstein's taxonomy (2021).

Control variables

Digital factors

The study controls for several potential confounders that indicate the government's dominance in the digital sphere. Government digital dominance influences the IV by affecting a country's disposition towards utilising AIST, as well as the DV by affecting citizens' ability to organise political dissent and thus how often governments may engage in digital repression. Thus, the study utilises ordinal variables from the DSP database to control for the prevalence of social media platforms entirely controlled by the government (*smgovsmalt*); the surveillance of political content on social media by the government (*smgovsmmon*); the citizen consumption of domestic online media (*smonex*); the online media fractionalisation (*smmefra*); the average use of social

media to organise offline political action (*smorgavgact*); and the polarisation of society (*smpolsoc*) (Mechkova *et al.*, 2020). The percentage of households with internet access is also controlled, expressed nominally as *internet,* using ITU data (ITU, no date). This is because the internet is purported to benefit citizens in the short-term by nurturing episodes of unrest but benefits governments in the long-term by enhancing digital repression tools (Ruijgrok, 2017; Weidmann and Rød, 2019).

Military expenditure

A strong relationship exists between a country's military expenditure and its use of AIST (Feldstein, 2019). Military expenditure affects the DV and IV by affecting a country's ability to purchase AIST and its ability to carry out digital repression, hence it is controlled using the nominal variable *militaryexp* utilising SIPRI military expenditure data (SIPRI, 2015).

Regime type

As regime type is associated with both AIST and digital repression (Feldstein, 2021; cit), the Polity V Dataset (CSP, 2018) is used to control for regime polity score, expressed ordinally as *polity2*, and V-Dem data (Gerring *et al.*, 2021) is used to control for respect for civil and political liberties, expressed ordinally as *civlib* and *pollib*.

Other factors

Other variables that affect the government's ability to surveil and digitally repress citizens are included: GDP per capita (*gdppp*) and total and urban population (*pop* and *urbanpop*) using

UNCTAD data (UNCTAD, 2021a, 2021b); and the onset of new conflict using the binary indicator *newconf* from the UCDP Onset Dataset (Gleditsch *et al.*, 2002).

Model

Multiple tests were carried out, comparing bivariate and multivariate regressions with two-way fixed effect (2FE) regressions to ensure model adequacy. Robustness tests are then conducted to avoid miscalculation of standard errors. As this is an observational study, all confounders are impossible to observe. Thus, the 2FE model was found to be most suitable for panel data as it removes omitted variable bias by simultaneously controlling for unobserved unit-specific and time-specific confounders by including dummy variables for each group and time period. Specifically, unit fixed effects mean that only within-group variation is used in the outcome (digital repression score) to calculate the effect of the treatment (adoption of Chinese AIST). This removes any omitted variable bias that is constant over time, for example culture, major religion and regime type. Unit-dummies also create smaller standard errors on the treatment, which would not have been possible with repeated cross-section data as we would not have the same units in each time period. Meanwhile, time fixed effects mean that we remove the effect of any changes to the outcome variable that affect all units at the same time, for example elections and economic shocks.

The fundamental problem of causal inference, however, is that we cannot directly observe the counterfactual of our results: what would be the digital repression scores for countries that adopted Chinese AIST in the absence of the treatment? 2FE allows us to rectify this problem and calculate an average treatment effect on the treated group because it rests on the assumption of

parallel trends: if treated units did not receive the treatment (i.e., if countries that adopted Chinese AIST had not adopted it), they would have followed the same trend as the control units (the countries that had not adopted Chinese AIST), since selection bias is time-invariant.

The 2FE model is expressed as follows:

$$Y_{it} = \gamma_i + \alpha_t + \delta D_{it} + \epsilon_{it}$$

Whereby:

- Y_{it}: the observed outcome: the digital repression scores (*smgovdom, smgovshut, smgovsm, smgovsmcenprc, smarrest*).
- D_{it}: the binary treatment indicator for unit i at time t: the adoption of Chinese AIST (*ctech*), 1 for treated unit-period observations (2017-2020) and 0 otherwise.
- δ: the difference-in-difference estimate based on D_{it}.
- γ_i and α_t: unit and time fixed effects, respectively.
- ϵ_{it}: the error term.

Results

This paper uses 2FE regression to investigate the causal relationship between adopting Chinese AIST and digital repression practices in Africa. Findings indicate that the average treatment effect on the treated group (ATT) of Chinese AIST adoption increases for only one of five digital repression indicators, government internet shutdowns, by only 0.02 points with p-value 0.021.

This provides partial support for the hypothesis that African governments' adoption of Chinese AIST adoption increases digital repression in Africa. However, Chinese AIST adoption is associated with a decrease of digital repression as measured by the remaining four digital repression indicators. The implication is that Chinese AIST adoption largely decreases digital repression practices in Africa. The full regression outputs are recorded in appendix D. This section proceeds to describe the regression results and their significance. The implications of the results are dissected in the following section.

Government domestic dissemination of false information (*smgovdom*)

The results of the first analysis are summarised in appendix D, table 1. Models 1, 2 and 3, demonstrate bivariate, multivariate and 2FE regressions, respectively. The three models are compared to observe the association between adoption of Chinese AIST (*ctech*) and *smgovdom*. The coefficient of *ctech* in model 1 demonstrates that adoption of Chinese AIST is associated with a 0.014-point increase in government dissemination of false information. Controlling for potential confounders in model 2 demonstrates that adoption of Chinese AIST is associated with a 0.21-point increase in government dissemination of false information, which is a more substantial increase than model 1. The adjusted R^2 in model 2 also demonstrates that controlling for additional covariates explains 77% of the variation in *smgovdom*. However, neither the bivariate nor the multivariate coefficient can be interpreted causally as omitted variable bias is a problem in both cases.

Once unobserved unit-specific and time-specific confounders are controlled for in model 3, the 2FE model, government domestic dissemination of false information decreases drastically

compared to models 1 and 2: the coefficient of *ctech* in model 3 indicates an ATT of -0.22 points, significant at the 99.9% confidence interval. Substantively, the -0.22-point ATT is a significant decrease of the *smgovdom* score on the -5 to 5 interval. Moreover, the adjusted R^2 in model 3 illustrates that unobserved unit- and time-specific confounders account for 91% of the variation in *smgovdom*.

The p-value allows us to ascertain whether the null hypothesis is true, that is, whether adopting Chinese AIST does *not* affect government domestic dissemination of false information. A p-value of less than 0.05 informs us that there is less than 5% chance of seeing these results if the null hypothesis were true. Conducting a t-test derives a p-value of 0.92, meaning that there is a very high probability of achieving the same results even if the null hypothesis were true. Hence, we fail to reject the null hypothesis that adopting Chinese AIST does not affect government domestic dissemination of false information. In other words, the p-value provides evidence in favour of the null hypothesis of no effect.

Government internet shutdown (*smgovshut*)

The results of the second analysis are summarised in appendix D, table 2, illustrating the relationships between *ctech* and *smgovshut*. Results illustrate that the *ctech* coefficient is associated with a 0.12-point increase in *smgovshut* in bivariate model 4 and a 0.41-point increase in multivariate model 5. Though these are significant increases, we again cannot interpret them causally. The *ctech* coefficient in 2FE model 6, meanwhile, is associated with an ATT of 0.02 points, suggesting that adopting Chinese AIST increases government internet shutdowns in Africa, but only marginally. The adjusted R^2 increases from 84% in model 5 to 93% in model 6.

Unobserved confounders, thus, account for 93% of the variation in *smgovshut*. A t-test provides a p-value of 0.021, meaning we can reject the null hypothesis of no effect at 95% confidence and have additional evidence for our hypothesis that adopting Chinese AIST increases digital repression in Africa via internet shutdowns.

Government social media shutdown (*smgovsm*)

The results of the third analysis are summarised in appendix D, table 3, illustrating the relationship between *ctech* and *smgovsm*. Results illustrate that the *ctech* coefficient is associated with a 0.35-point increase in *smgovsm* in bivariate model 7 and a 0.70-point increase in multivariate model 8, both statistically significant at 99% confidence. Though these are even larger effects than the previous analysis, they are not causal due to omitted variable bias. In fact, 2FE model 9 is associated with an ATT of -0.06 points while the adjusted R^2 demonstrates that unobserved confounders account for 92% of the variation in *smgovsm*, suggesting an opposite effect: that adopting Chinese AIST decreases government social media shutdowns in Africa, though only minimally. However, a t-test provides a p-value of 0.46, suggesting evidence in favour of the null hypothesis of no effect.

Government social media censorship (*smgovsmcenprc*)

The results of the fourth analysis are summarised in appendix D, table 4, illustrating the relationship between *ctech* and *smgovsmcenprc*. Results are mixed, illustrating that the *ctech* coefficient is associated with a -0.06-point decrease in government social media censorship in bivariate model 10, increasing to a 0.38-point increase in *smgovsmcenprc* in multivariate model 11. However, 2FE model 12 is associated with an ATT of -0.22 points, which is a fairly large decrease compared to the 2FE results in the previous models, and statistically significant at the

99.9% confidence interval. Therefore, we cannot reject the null hypothesis that adoption of Chinese AIST does not affect government social media censorship. The 2FE model thus suggests that adopting Chinese AIST decreases government social media shutdowns in Africa. Additionally, the t-test provides a p-value of 0.69, which is far from significant, actually supporting the claim that we cannot reject the null hypothesis of no effect. Interestingly, the adjusted R^2in model 12 demonstrates that unobserved confounders account for 87% of the variation in *smgovsmcenprc,* which is noticeably less than in previous 2FE models.

Government arrests for posting political content online (*smarrest*)

The results of the fifth analysis are summarised in appendix D, table 5, illustrating the relationship between *ctech* and *smarrest*. The coefficients illustrate that the adoption of Chinese AIST is associated with a 0.16-point increase in *smarrest* in bivariate model 13 and a -0.40-point decrease in multivariate model 14. However, 2FE model 15 is associated with an ATT of -0.18 points. Similar to 2FE model 12 for social media censorship, this is a relatively large decrease, again suggesting that adopting Chinese AIST decreases government arrests for political content in Africa fairly significantly. The adjusted R^2in model 15 demonstrates that unobserved confounders account for 84% of the various in *smarrest*. However, a t-test provides a p-value of 0.33, suggesting evidence in favour of the null hypothesis of no effect.

Summary

To summarise the five analyses, we observe relatively large associations between Chinese AIST adoption and the outcomes in the bivariate and multivariate regression models. Yet these effects cannot be interpreted causally due to omitted variable bias. The 2FE models provide the most

credible estimates for the causal effect of Chinese AIST adoption on digital repression practices in Africa because they control for unobserved within states over time to reduce omitted variable bias; in fact, the associations observed in the bivariate and multivariate models largely disappear in the 2FE models.

In four of five cases, the 2FE coefficients associated with *ctech* are negative: adopting Chinese AIST seems to decrease government domestic dissemination of false information, social media shutdowns, social media censorship and arrests for political content. However, government social media shutdowns decrease the least. P-values for the four indicators provide evidence for the null hypothesis of no effect. However, the 2FE coefficient in model 6 demonstrates an increase in government internet shutdown, providing partial support for the hypothesis that adopting Chinese AIST increases digital repression practices in Africa. Though the effect is almost negligible (an increase of 0.02 points), the p-value allows us to reject the null hypothesis of no effect at 95% confidence.

Overall, there seems to be little evidence of a significant effect of Chinese AIST adoption increasing digital repression in Africa. Contrary to the hypothesis, the models suggest that Chinese AIST adoption decreases digital repression in Africa.

Robustness checks

Heteroscedasticity is a major concern in regression analysis. When calculating linear regression, standard errors are assumed to be homoscedastic: the variance of the error term is equal for all covariate values. When the homoscedasticity assumption is violated, the standard errors will be

miscalculated, leading to either upwards or downward bias in standard error estimates. Thus, heteroscedasticity-robust standard error calculations are conducted. The results are summarised in appendix D, table 6.

The standard errors in the corrected models (labelled *coeftest*) are larger after accounting for heteroscedasticity, illustrating that failures of the homoscedasticity assumption lead to a downward bias in standard error in the 2FE models. We observe that the statistical significance of the coefficient in 2FE model 1 decreases from 99.9% to 95% after correction in model 2. Similarly, the statistical significance in 2FE model 7 falls from 99.9% to no statistical significance in model 8 and from 99% in 2FE model 9 to no statistical significance in model 10.

Overall, however, the corrections do not make a large difference to the conclusions drawn. In four of five cases, we failed to reject the null hypothesis of no effect using the original standard errors. Hence, the corrections are not consequential and we do not change the conclusion of our hypothesis tests after correcting for heteroscedasticity.

The following section discusses the implications of the findings, limitations of the study and avenues forward, before concluding with a summary of the paper's key ideas and policy implications.

Discussion

Implications

The sample did not provide sufficient evidence to conclude that Chinese AIST adoption increases digital repression in Africa. Antithetically, the results suggest that Chinese AIST adoption *decreases* digital repression in Africa in four of five digital repression indicators: government domestic dissemination of false information, social media shutdown, social media censorship and arrests for political content. Digital repression only increases marginally in terms of government internet shutdowns. Nonetheless, as the 2FE model simultaneously controls for unobserved unit-specific and time-specific confounders, the parallel trends assumption is theoretically respected, giving the results high internal validity. This section proceeds to discuss the implications of the 2FE results in the context of the proposed causal mechanism and the existing literature.

Little support was found for the hypothesis. The only increase in digital repression concerned the internet shutdowns indicator. The 2FE model demonstrated that adoption of Chinese AIST is associated with a 0.02-point increase in internet shutdowns - an extremely small increase on the -5 to 5-point repression scale. However, we can be fairly confident in this result as the p-value 0.021 allows us to reject the null hypothesis at 95% confidence. This finding invites reflection upon assumptions made in the causal mechanism.

The causal mechanism assumes that governments have incentives to undertake digital repression, which is less visible and costly than physical coercion, to maintain uncertainty about repression

targets and ensure citizens' regime preferences remain fairly transparent in the long run. Although internet shutdowns are a form of digital repression (Feldstein, 2021), they may be similarly costly as physical repression. Compared to other forms of digital repression such as disseminating false information, internet shutdowns are relatively noticeable. If the government retains asymmetric control of the internet (Weidmann and Rød, 2019; Chang and Lin, 2020), citizens may be more likely to notice patterns of shutdowns that benefit the government.

Alternatively, internet shutdowns may be a difficult digital repression strategy to undertake due to power structures within the regime. Analyses of internet shutdowns in Uganda and the Republic of the Congo demonstrate that local internet companies backed by democratic states are less likely to succumb to government internet shutdown pressures; whereas domestic private companies with ties to the regime or internet companies connected to other authoritarian countries are more likely to adhere to shut down requests (Freyburg and Garbe, 2018). A promising path forward in this regard would be to investigate the viability of internet shutdowns as a digital repression strategy when internet access is not centrally controlled. Overall, the findings on internet shutdowns tentatively support the 'repression technology' literature, whereby technology reinforces authoritarian governance.

Adoption of Chinese AIST is associated with a 0.06-point decrease in social media shutdowns with p-value 0.46. Although this is a larger ATT than for internet shutdowns, it remains a substantively small effect on the -5 to 5-point repression scale. Similarly, social media shutdowns could be considered 'too obvious' of a digital repression strategy. In analysing results for social

media shutdowns, however, the covariate estimates in multivariate model 8 hint at initial reasons for the low ATT, explained hereafter (refer to appendix D, table 3).

Multivariate model 8 controls for social media platforms entirely controlled by the government (*smgovsmalt*). When holding all other variables constant, *ctech* is associated with a 0.48-point decrease in *smgovsmalt* at the 99.9% confidence interval. Though the multivariate model cannot be interpreted causally, it partly supports a dynamic outlined in the causal mechanism, whereby governments can utilise AIST to identify and monitor potential regime opponents. This potentially makes government-controlled social media redundant, hinting that AIST essentially replaces social media shutdowns as a repression tool - hence the 0.06-point decrease in social media shutdowns.

Adoption of Chinese AIST was associated with a substantial decrease in digital repression on the other three indicators: dissemination of false information (-0.22), social media censorship (-0.22) and arrests for posting political content (-0.18). The p-values were very high, at 0.92, 0.69 and 0.33, respectively. The causal mechanism assumes that adopting Chinese AIST increases the recipient government's surveillance capacity, allowing for individualised tracking and oversight over activities that threaten the regime. To maintain the regime, the government replaces physical repression with digital repression to stifle threats before they can multiply. However, the reality may not be as straightforward. The 'dictator's digital dilemma' highlights a trade-off between maintaining political control and sacrificing economic benefits from citizens' full use of digital technologies (Feldstein, 2021, p. 37). For example, in 2019 the Iraqi economy suffered over $2.3 billion in losses from an 11-day government internet shutdown that attempted to halt protests

(ibid). Thus, digital repression may have decreased significantly in terms of disseminating false information, censorship and arrests in part because it would have undesirable economic repercussions.

In sum, scant evidence is found for the hypothesis that African governments' adoption of Chinese AIST increases digital repression in Africa. Overall, Chinese AIST adoption seems to decrease digital repression in Africa. The findings nonetheless provide data to reassess the assumptions made in the causal mechanism and point towards avenues for further inquiry. The following subsection outlines the limitations of the research design before discussing ways forward for AIST research.

Limitations

The analysis is subject to several methodological and data-specific limitations. Concerning the prior, the assumption of 2017-2020 as the treatment years is a strong assumption, but given the impossibility of tracing the exact year of AIST adoption per country, this study attempted to strengthen the assumption by checking multiple references. Feldstein used public sources from 2017-2019 to compile the 2019 AI global surveillance index as little existed on AIST pre-2017. This matched UNCTAD export data, where we observed an uptick in China's trade in ICT services from 2017. This, in turn, matched qualitative knowledge on DSR trade patterns. This highlights the difficulty of analysing the impacts of AIST on digital repression as it is an emerging issue.

Another large limitation is that quantitative analysis lacks granularity. Because the deployment of AIST may only occur within sub-parts of nation-states, effects might cancel out at the national level. Moreover, it is difficult to assess which countries really deploy AIST and when. Thus, there may be certain effects that cancel out across states. It would be extremely valuable to systematically conduct comparative case studies to better grasp such dynamics.

Overall, the 2FE model is useful because it eliminates bias from unobserved factors that vary between countries but are constant within states over time (e.g. culture and economic shocks). To further strengthen the internal validity of the estimates, the study additionally controls for observable unit-fixed effects such as polity2 score and time-fixed effects such as GDP and new conflicts. Notwithstanding, there may be important variables that vary with a country over time that remain omitted. For example, policy measures related to the implementation of Chinese AIST systems that affect the relative ease of conducting digital repression compared to physical repression or coercion.

As the study is observational, the possibility of confounding nonetheless remains. Though 2FE ensures high internal validity, the trade-off is that the model has low external validity: the results are unlikely to be generalisable outside of the existing sample. They are nonetheless insightful, as they allow us to assess assumptions drawn from the literature. Randomly selecting a sample among all countries that utilise AIST, regardless of whether the AIST originated from China or not, would minimise confounding and increase generalisability by ensuring the sample reflects the true population distribution. Another alternative would be to compare digital repression outcomes pre- and post-2017 to verify whether Chinese AIST enhanced digital repression.

With regards to data collection, time constraints meant that not all relevant covariates were included in the analysis. For example, existing case studies of Thailand, Ethiopia and the Philippines demonstrate that ongoing levels of repression, leadership, state capacity and technological capabilities affect the degree to which governments use new digital tools for repressive purposes; ideally, these variables would be included (Feldstein, 2021, p. 24). Some public data used in the dataset contained large amounts of missing values, particularly for military expenditure and internet penetration, complicating the interpretation of results: missing data likely leads to coefficient estimates with larger standard errors, creating selection bias in the results. Missing data could be overcome by cross-referencing data sources when possible, though possible inconsistencies between data points may remain an issue.

As DSP data are generated by aggregating ratings from country experts, it is also possible that key DSP variables such as government domestic dissemination of false information provide an uncertain estimator. Particularly in authoritarian regimes, some experts may have incentives or be coerced into underreporting the true occurrence of false information dissemination. Similarly, Feldstein's AI surveillance index (2019) relied on open-source reporting. Some companies such as Huawei, however, have incentives to highlight new AIST capabilities, while other companies purposely keep business operations out of the public domain (Feldstein, 2019). This may lead to biased reporting, potentially affecting the validity of the index. Such issues are currently difficult to reconcile for the quantitative researcher of emerging technology in political science, even when following rigorous research procedures. Already, accurate data on the internal functioning of authoritarian regimes is difficult to access. In addition, there is a lack of public data on

government surveillance use, let alone on most AI applications. Relying on secondary sources and assessing their reliability, as Feldstein (2019) does, is a valuable way to gather information on AIST where it is otherwise difficult to gather precise data.

Avenues for further research

Methodologically, this paper aims to redress the lack of quantitative AIST scholarship. Yet the field also lacks rigorous qualitative scholarship. Further research could employ content tracing to identify an alternative causal mechanism. This may be a promising means to identify the effects of Chinese AIST on digital repression in Africa, as the discovery of mechanisms requires the reconstruction of processes, which may rectify the issue of identifying the precise year AIST systems were deployed in each country. Alternatively, further comparative case studies could be conducted. Felstein (2021) begins to fill this gap by comparing AIST in Thailand, Philippines and Ethiopia. Similar case studies could be conducted focusing on specific regions, such as Africa or Latin America.

Substantively, a myriad of valuable further research avenues exist. There is little disagreement that China is a leading supplier of AIST. Many claim that China supports digital authoritarianism through AIST exports (Sahin, 2020). If economic progress and technological innovation do not rely on democracy, China's non-democratic governance model may perpetuate globally (Meissner *et al.*, 2016; Crosston, 2020). Thus, as digital technologies become entangled with specific forms of governance, AIST may feed ideological clashes (Aho and Duffield, 2020). In this context, it would be valuable to better understand the appeal of China's AIST infrastructure for adopting countries (Peterson, 2020).

Yet China's digital landscape differs greatly from other authoritarian regimes. States with high technology capacity may be more likely to engage in digital surveillance (Xu, 2021). Nonetheless, it may not be possible to 'duplicate' China's model abroad, let alone its digital repression strategies such as media censorship (Pan, 2017). Digital repression may be more successful in countries that already possess high internal coercive capacity and weak government oversight (Feldstein, 2021). But not all countries with these characteristics carry out digital repression. What are the relevant factors that incline certain countries to adopt AIST and/or digital repression? Are AISTs then deployed throughout the country or only in specific areas or regions?

If one assumes the DSR encourages countries to take Chinese loans and import AIST, what role might the West play to counteract such expanding Chinese technological power? The European Commission recently proposed a draft AI Act, the first comprehensive AI regulation of its kind, setting boundaries for indiscriminate AIST such as social credit systems (European Commission, 2021). Further, the European Council is considering an ambitious infrastructure plan to rival the BRI (Lau, 2021). What impacts might such regulations and plans have on global technology standards and international balance of power?

Finally, this paper's causal mechanism assumes that surveillance deters individuals from engaging in illegal offences (Stoycheff *et al.*, 2019). If this holds true, we should observe fewer protests. Weidmann and Rød (2019) demonstrate that protests are kept low in the long-run due to government monopoly over internet expansion. Does a similar dynamic occur with AIST? The

difficulty is that AIST has not been utilised for long enough to understand long-term empirical effects with high confidence.

Conclusion

This paper has attempted to contribute to the literature at the intersection of authoritarianism, technology and digital repression, proposing a causal mechanism based on a set of assumptions from the literature. The paper hypothesised that African governments' adoption of China's AI surveillance technologies leads to an increase in digital repression practices in Africa. To investigate the causal relationship, the paper applied 2FE regression. Digital repression was measured using five indicators: government domestic dissemination of false information; government internet shut down; government social media shut down; government social media censorship; and government arrests for posting political content online (Mechkova *et al.*, 2020).

Overall, there is little evidence of a significant effect of Chinese AIST adoption increasing digital repression in Africa. On the contrary, the models suggest that African governments' adoption of Chinese AIST potentially decreases digital repression in Africa: results demonstrated that Chinese AIST adoption is associated with a marginal increase of government internet shutdowns, and a decrease of the remaining digital repression indicators.

The emergence of AIST as a tool to facilitate digital repression also raises scores of new questions, highlighted in the discussion. Why does China's digital infrastructure appeal to

adopting countries? What are the factors that incline countries to adopt AIST and digital repression and what are the long-term effects on contentious politics? What is the role of the West in countering expanding Chinese technological power? These are but a few avenues that merit further inquiry to better understand the implications of AIST on international security.

This analysis is subject to several methodological and data-specific limitations, however. Mainly, the results are unlikely generalisable outside of the sample. Nonetheless, the findings allow us to critically assess certain dynamics highlighted in the literature that informed assumptions in the causal mechanism. In line with the repression technology argument that technology reinforces authoritarian governance, results from this paper suggest that African governments can utilise AIST to affect dissent via internet shutdowns. However, in contrast to the literature on physical and digital coercion, the results suggest that AIST potentially reduces the need for digital repression. This finding nuances broad-stroke claims in discourse surrounding China 'exporting digital authoritarianism' (Sahin, 2020): though we still observe anecdotal cases where China's AIST exports are used by and to support illiberal regimes, it is important to disentangle exactly how this occurs to better understand policy-level implications.

New technologies do not always have obvious effects. This analysis can help policymakers better understand the effects of AI technology and repression in the digital age. Policymakers tend to hold strong positions about the transformative power of the internet, reflected for example in Hillary Clinton's 'Remarks on Internet Freedom' (2010). Yet, as Weidmann and Rød (2019) describe, we should be careful in drawing conclusions that assume that political protest entails beneficial consequences for citizens, as this is not necessarily the case in autocratic regimes. This

paper's findings demonstrate that when AIST is adopted in Africa, digital repression increases by means of internet shutdowns, implying that the internet remains a relevant tool for retaining control over a population. At face value, this speaks against prioritising expansion of AIST and the internet through policy, as they would further facilitate digital repression through government internet shutdowns.

It is rarely this simple, however. The way governments utilise AIST is a crucial factor to consider. If AIST adoption decreases digital repression overall, this might signal a shift in how autocratic regimes function. Is AIST predominantly used to repress potential regime dissidents, as traditionally expected, or is it used to better understand public opinion and provide useful services to citizens? If AIST can enable governments, even autocratic ones, to become more accountable, policies that favour technological expansion may be desirable.

Bibliography

Acemoglu, D. and Robinson, J.A. (2006) 'Economic Backwardness in Political Perspective', *American Political Science Review*, 100(1), pp. 115–131. doi:10.1017/S0003055406062046.

Aho, B. and Duffield, R. (2020) 'Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China', *Economy and Society*, 49(2), pp. 187–212. doi:10.1080/03085147.2019.1690275.

Alizada, N. *et al.* (2021) *Autocratization Turns Viral: Democracy Report 2021*. Gothenburg, Sweden: V-Dem Institute, University of Gothenburg. Available at: https://www.v-dem.net/files/25/DR%202021.pdf.

Al-Jenaibi, B. (2016) 'The Twitter Revolution in the Gulf Countries', *Journal of Creative Communications*, 11(1), pp. 61–83. doi:10.1177/0973258616630217.

Andrejevic, M. and Gates, K. (2014) 'Big Data Surveillance: Introduction', *Surveillance & Society*, 12(2), pp. 185–196. doi:10.24908/ss.v12i2.5242.

Artigas, Á. (2017) 'Surveillance, Smart technologies and the development of Safe City solutions: the case of Chinese ICT firms and their international expansion to emerging markets', p. 47.

Bennett, W.L. and Livingston, S. (2018) 'The disinformation order: Disruptive communication and the decline of democratic institutions', *European Journal of Communication*, 33(2), pp. 122–139. doi:10.1177/0267323118760317.

Breckenridge, K. (2014) *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge: Cambridge University Press. doi:10.1017/CBO9781139939546.

Castells, M. (2013) *Communication Power*. OUP Oxford.

Cave, D. *et al.* (2019) *Mapping China's Tech Giants*, *Australian Strategic Policy Institute*. Available at: https://www.aspi.org.au/report/mapping-chinas-tech-giants (Accessed: 6 July 2021).

CFR (no date) *What Happened When China Joined the WTO?*, *World101 From the Council on Foreign Relations*. Available at: https://world101.cfr.org/global-era-issues/trade/what-happened-when-china-joined-wto (Accessed: 8 September 2021).

Chang, C.-C. and Lin, T.-H. (2020) ‘Autocracy login: internet censorship and civil society in the digital age’, *Democratization*, 27(5), pp. 874–895. doi:10.1080/13510347.2020.1747051.

Chen, H. and Greitens, S.C. (2021) ‘Information capacity and social order: The local politics of information integration in China’, *Governance* [Preprint]. doi:10.1111/gove.12592.

Cheney, C. (2019) *China’s Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism*. Working Paper 8. Pacific Forum. Available at: https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf.

Chin, J.P., Nicholas Bariyo and Josh (2019) ‘Huawei Technicians Helped African Governments Spy on Political Opponents’, *Wall Street Journal*, 15 August. Available at: https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 (Accessed: 25 June 2021).

Chutel, L. (2018) *China is exporting facial recognition software to Africa, expanding its vast database*, *Quartz*. Available at: https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/ (Accessed: 4 August 2021).

Corrales, J. and Westhoff, F. (2006) ‘Information Technology Adoption and Political Regimes’, *International Studies Quarterly*, 50(4), pp. 911–933. doi:10.1111/j.1468-2478.2006.00431.x.

Crosston, M. (2020) ‘Cyber Colonization: The Dangerous Fusion of Artificial Intelligence and Authoritarian Regimes’, *Cyber, Intelligence, and Security*, 4(1), pp. 149–171.

CSP (2018) *Polity V: Political Regime Characteristics and Transitions, 1800-2018*. Electronic dataset. Center for Systemic Peace (CSP). Available at: https://www.systemicpeace.org/inscrdata.html.

Dafoe, A. and Lyall, J. (2015) ‘From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda’, *Journal of Peace Research*, 52(3), pp. 401–413. doi:10.1177/0022343314563653.

Daly, A. (2019) ‘Algorithmic oppression with Chinese characteristics : AI against Xinjiang’s Uyghurs’, in. APC, pp. 108–112. Available at: https://strathprints.strath.ac.uk/71586/ (Accessed: 14 August 2021).

DeMeritt, J.H.R. (2016) ‘The Strategic Use of State Repression and Political Violence’, *Oxford Research Encyclopedia of Politics* [Preprint]. doi:10.1093/acrefore/9780190228637.013.32.

Diamond, L. (2010) ‘Liberation Technology’, *Journal of Democracy*, 21(3), pp. 69–83. doi:10.1353/jod.0.0190.

van Dijck, J. (2014) ‘Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology’, *Surveillance & Society*, 12(2), pp. 197–208. doi:10.24908/ss.v12i2.4776.

Dragu, T. and Lupu, Y. (2021) ‘Digital Authoritarianism and the Future of Human Rights’, *International Organization*, pp. 1–27. doi:10.1017/S0020818320000624.

Dwyer, M. and Molony, T. (2019) *Social Media and Politics in Africa: Democracy, Censorship and Security*. London, UK: Zed Books Ltd.

Eltahawy, M. (2010) ‘Facebook, YouTube and Twitter are the new tools of protest in the Arab world’, *Washington Post*, 7 August. Available at: https://www.washingtonpost.com/wp-dyn/content/article/2010/08/06/AR2010080605094.html (Accessed: 16 August 2021).

European Commission (2021) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

Farrell, H. (2012) ‘The Consequences of the Internet for Politics’, *Annual Review of Political Science*, 15(1), pp. 35–52. doi:10.1146/annurev-polisci-030810-110815.

Feldstein, S. (2019) *The Global Expansion of AI Surveillance*, *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 (Accessed: 6 July 2021).

Feldstein, S. (2021) *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. Oxford University Press.

Frantz, E., Kendall-Taylor, A. and Wright, J. (2020) *Digital Repression in Autocracies*. V-Dem Institute, p. 54. Available at: https://www.v-dem.net/media/filer_public/18/d8/18d8fc9b-3ff3-44d6-a328-799dc0132043/digital-repression17mar.pdf.

Freyburg, T. and Garbe, L. (2018) ‘Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa’, *International Journal of Communication*, 12(0), p. 21.

Fuchs, C. *et al.* (eds) (2013) *Internet and Surveillance*. Routledge. Available at: https://learning.oreilly.com/library/view/-/9780415891608/ (Accessed: 11 August 2021).

Gamso, J. (2021) ‘Is China exporting media censorship? China’s rise, media freedoms, and democracy’, *European Journal of International Relations*, p. 13540661211015722. doi:10.1177/13540661211015722.

Gates, K.A. (2011) *Our Biometric Future*, *Our Biometric Future*. New York University Press. Available at: https://www.degruyter.com/document/doi/10.18574/9780814733035/html (Accessed: 11 August 2021).

Gerring, J. *et al.* (2021) *V-Dem [Country–Year/Country–Date] Dataset v11.1*. Electronic dataset. Varieties of Democracy (V-Dem) Project. Available at: https://www.v-dem.net/en/data/data/v-dem-dataset-v111/.

Gerschewski, J. (2013) ‘The three pillars of stability: legitimation, repression, and co-optation in autocratic regimes’, *Democratization*, 20(1), pp. 13–38. doi:10.1080/13510347.2013.738860.

Gleditsch, N.P. *et al.* (2002) ‘Armed Conflict 1946–2001: A New Dataset’, *Journal of Peace Research*, 39(5). Available at: https://ucdp.uu.se/downloads/index.html#onset.

Gohdes, A.R. (2020) ‘Repression Technology: Internet Accessibility and State Violence’, *American Journal of Political Science*, 64(3), pp. 488–503. doi:10.1111/ajps.12509.

Gravett, W.H. (2020) ‘Digital Coloniser? China and Artificial Intelligence in Africa’, *Survival*, 62(6), pp. 153–178. doi:10.1080/00396338.2020.1851098.

Grinberg, D. (2017) ‘Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia’, *Surveillance & Society*, 15(3/4), pp. 432–438. doi:10.24908/ss.v15i3/4.6623.

Groshek, J. (2010) ‘A Time-Series, Multinational Analysis of Democratic Forecasts and Internet Diffusion’, *International Journal of Communication*, 4(0), p. 33.

Groshek, J. and Mays, K. (2017) ‘A Time-Series, Multinational Analysis of Democratic Forecasts and Emerging Media Diffusion, 1994–2014’, *International Journal of Communication*,

11(0), p. 23.

Gunitsky, S. (2015) ‘Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability’, *Perspectives on Politics*, 13(1), pp. 42–54. doi:10.1017/S1537592714003120.

Gwagwa, A. and Garbe, L. (2018) *Exporting Repression? China’s Artificial Intelligence Push into Africa*, *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa (Accessed: 26 June 2021).

Halper, S. (2010) *The Beijing Consensus: How China’s Authoritarian Model Will Dominate the Twenty-First Century*. New York, USA: Basic Books.

He, B. and Warren, M.E. (2011) ‘Authoritarian Deliberation: The Deliberative Turn in Chinese Political Development’, *Perspectives on Politics*, 9(2), pp. 269–289. doi:10.1017/S1537592711000892.

Hillman, J.E. and McCalpin, M. (2019) *Watching Huawei’s “Safe Cities”*. Center for Strategic and International Studies. Available at: https://www.csis.org/analysis/watching-huaweis-safe-cities (Accessed: 3 July 2021).

Hoffman, S. (2017) ‘Managing the State: Social Credit, Surveillance and the CCP’s Plan for China’, *China Brief*, 17(11). Available at: https://jamestown.org/program/managing-the-state-social-credit-surveillance-and-the-ccps-plan-for-china/ (Accessed: 7 July 2021).

Hoffman, S. (2018) *Social Credit: Technology-enhanced authoritarian control with global consequences*. Policy Brief 6. Australian Strategic Policy Institute. Available at: https://www.aspi.org.au/report/social-credit (Accessed: 7 July 2021).

Hoffman, S. (2019) *Engineering global consent: the Chinese Communist Party’s data-driven power expansion*. Policy Brief 21. Australian Strategic Policy Institute, p. 36. Available at: https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

Howard, P.N. (2010) *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford University Press (Oxford Studies in Digital Politics). doi:10.1093/acprof:oso/9780199736416.001.0001.

Hussain, M.M. and Howard, P.N. (2013) ‘What Best Explains Successful Protest Cascades? ICTs

and the Fuzzy Causes of the Arab Spring', *International Studies Review*, 15(1), pp. 48–66. doi:10.1111/misr.12020.

ITU (no date) *Digital Development Dashboard*. Electronic dataset. International Telecommunication Union (ITU). Available at: https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx.

Ivanova, M., Yakovleva, T. and Selenteva, T. (2020) 'The Models of Information Asymmetry in the Context of Digitization of Government', in *Proceedings of the International Scientific Conference - Digital Transformation on Manufacturing, Infrastructure and Service*. New York, NY, USA: Association for Computing Machinery (DTMIS '20), pp. 1–6. doi:10.1145/3446434.3446512.

Johnson, J. (2019a) 'Artificial intelligence & future warfare: implications for international security', *Defense & Security Analysis*, 35(2), pp. 147–169. doi:10.1080/14751798.2019.1600800.

Johnson, J. (2019b) 'The AI-cyber nexus: implications for military escalation, deterrence and strategic stability', *Journal of Cyber Policy*, 4(3), pp. 442–460. doi:10.1080/23738871.2019.1701693.

Kalathil, S. and Boas, T.C. (2003) *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Carnegie Endowment for International Peace. Available at: https://www.jstor.org/stable/j.ctt6wpj9n (Accessed: 14 July 2021).

Kendall-Taylor, A., Frantz, E. and Wright, J. (2020) 'The Digital Dictators: How Technology Strengthens Autocracy Essays', *Foreign Affairs*, 99(2), pp. 103–115.

Khalil, L. (2020) *Digital Authoritarianism, China and COVID*, *Lowy Institute*. Available at: https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid (Accessed: 3 July 2021).

King, G., Pan, J. and Roberts, M.E. (2013) 'How Censorship in China Allows Government Criticism but Silences Collective Expression', *American Political Science Review*, 107(2), pp. 326–343. doi:10.1017/S0003055413000014.

Lau, S. (2021) *EU starts work on rival to China's Belt and Road Initiative*, *POLITICO*. Available at: https://www.politico.eu/article/eu-starts-work-on-rival-to-chinas-belt-and-road-project-network/ (Accessed: 7 August 2021).

Letsa, N.W. (2017) '"The people's choice": popular (il)legitimacy in autocratic Cameroon*', *The Journal of Modern African Studies*, 55(4), pp. 647–679. doi:10.1017/S0022278X17000428.

Liang, F. *et al.* (2018) 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure', *Policy & Internet*, 10(4), pp. 415–453. doi:https://doi.org/10.1002/poi3.183.

Lilkov, D. (2020) 'Made in China: Tackling Digital Authoritarianism', *European View*, 19(1), pp. 110–110. doi:10.1177/1781685820920121.

Lührmann, A. and Lindberg, S.I. (2019) 'A third wave of autocratization is here: what is new about it?', *Democratization*, 26(7), pp. 1095–1113. doi:10.1080/13510347.2019.1582029.

Lynch, M. (2011) 'After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State', *Perspectives on Politics*, 9(2), pp. 301–310. doi:10.1017/S1537592711000910.

Lyon, D. (2014) 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique', *Big Data & Society*, 1(2), p. 2053951714541861. doi:10.1177/2053951714541861.

MacKinnon, R. (2011) 'Liberation Technology: China's "Networked Authoritarianism"', *Journal of Democracy*, 22(2), pp. 32–46. doi:10.1353/jod.2011.0033.

Maness, R.C. and Valeriano, B. (2016) 'The Impact of Cyber Conflict on International Interactions', *Armed Forces & Society*, 42(2), pp. 301–323. doi:10.1177/0095327X15572997.

Mechkova, V. *et al.* (2020) *DSP [Country-Year] Dataset v3*. Electronic dataset. Digital Society Project (DSP). Available at: http://digitalsocietyproject.org/data/.

Mechkova, V. *et al.* (2021) *Digital Society Survey Codebook*. Digital Society Project (DSP). Available at: http://digitalsocietyproject.org/data/.

Meester, J. (2021) *'Designed in Ethiopia' and 'Made in China': Sino-Ethiopian technology collaboration in South-South relations*. CRU Policy Brief. Clingendael Institute. Available at: https://www.jstor.org/stable/resrep28771 (Accessed: 7 July 2021).

Meissner, M. *et al.* (2016) *Is Big Data Increasing Beijing's Capacity for Control?*, *ChinaFile*. Available at: https://www.chinafile.com/conversation/Is-Big-Data-Increasing-Beijing-Capacity-Control%3F

(Accessed: 7 July 2021).

Milner, H.V. (2006) 'The Digital Divide: The Role of Political Institutions in Technology Diffusion', *Comparative Political Studies*, 39(2), pp. 176–199. doi:10.1177/0010414005282983.

Morgenbesser, L. (2017) 'The autocratic mandate: elections, legitimacy and regime stability in Singapore', *The Pacific Review*, 30(2), pp. 205–231. doi:10.1080/09512748.2016.1201134.

Mozur, P. (2019) 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority', *The New York Times*, 14 April. Available at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (Accessed: 7 August 2021).

Mozur, P., Kessel, J.M. and Chan, M. (2019) 'Made in China, Exported to the World: The Surveillance State', *The New York Times*, 24 April. Available at: https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html (Accessed: 26 June 2021).

Oreglia, E., Ren, H. and Liao, C.-C. (2021) 'The Puzzle of the Digital Silk Road', in *Digital Silk Road in Central Asia: Present and Future*. Davis Center for Russian and Eurasian Studies, Harvard University; Sustainable Kazakhstan Research Institute, Narxoz University, pp. 1–8.

Pan, J. (2017) 'How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship', *Problems of Post-Communism*, 64(3–4), pp. 167–188. doi:10.1080/10758216.2016.1181525.

Passini, S. (2012) 'The facebook and Twitter revolutions: Active participation in the 21st century', *Human Affairs*, 22(3), pp. 301–312. doi:10.2478/s13374-012-0025-0.

Peterson, D. (2020) *Designing Alternatives to China's Repressive Surveillance State*. Center for Security and Emerging Technology. Available at: https://cset.georgetown.edu/publication/designing-alternatives-to-chinas-repressive-surveillance-state/ (Accessed: 3 July 2021).

Pierskalla, J.H. and Hollenbach, F.M. (2013) 'Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa', *The American Political Science Review*, 107(2), pp. 207–224.

Qiang, X. (2019) 'The Road to Digital Unfreedom: President Xi's Surveillance State', *Journal of Democracy*, 30(1), pp. 53–67. doi:10.1353/jod.2019.0004.

Reardon, S. (2012) ‘Was it really a Facebook revolution?’, *New Scientist*, 214(2859), p. 24. doi:10.1016/S0262-4079(12)60889-6.

Remarks on Internet Freedom (2010) *U.S. Department of State*. Available at: //2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (Accessed: 8 September 2021).

Reuter, O.J. and Szakonyi, D. (2015) ‘Online Social Media and Political Awareness in Authoritarian Regimes’, *British Journal of Political Science*, 45(1), pp. 29–51. doi:10.1017/S0007123413000203.

Robbins, S. and Henschke, A. (2017) ‘The Value of Transparency: Bulk Data and Authoritarianism’, *Surveillance & Society*, 15(3/4), pp. 582–589. doi:10.24908/ss.v15i3/4.6606.

Rød, E.G. and Weidmann, N.B. (2015) ‘Empowering activists or autocrats? The Internet in authoritarian regimes’, *Journal of Peace Research*, 52(3), pp. 338–351. doi:10.1177/0022343314555782.

Romaniuk, S.N. and Burgers, T. (2018) ‘How China’s AI Technology Exports Are Seeding Surveillance Societies Globally’, *The Diplomat*, 18 October. Available at: https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/ (Accessed: 26 June 2021).

Ruijgrok, K. (2017) ‘From the web to the streets: internet and protests under authoritarian regimes’, *Democratization*, 24(3), pp. 498–520. doi:10.1080/13510347.2016.1223630.

Sahin, K. (2020) ‘The West, China, and AI surveillance’, *Atlantic Council*, 18 December. Available at: https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/ (Accessed: 25 June 2021).

Shahbaz, A. (2018) *The Rise of Digital Authoritarianism*, *Freedom House*. Available at: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism (Accessed: 2 July 2021).

Shapiro, J.N. and Siegel, D.A. (2010) ‘Is this Paper Dangerous? Balancing Secrecy and Openness in Counterterrorism’, *Security Studies*, 19(1), pp. 66–98. doi:10.1080/09636410903546483.

Shapiro, J.N. and Weidmann, N.B. (2015) ‘Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq’, *International Organization*, 69(2), pp. 247–274. doi:10.1017/S0020818314000423.

Shirky, C. (2009) *Here Comes Everybody: How Change Happens when People Come Together*. Penguin UK.

Shorey, S. and Howard, P.N. (2016) ‘Automation, Big Data and Politics: A Research Review’, *International Journal of Communication*, 10(0), p. 24.

Singer, P.W. and Brooking, E.T. (2018) *Likewar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.

SIPRI (2015) *SIPRI Military Expenditure Database 2015*. Electronic dataset. Stockholm International Peace Research Institute (SIPRI). Available at: http://milexdata.sipri.org.

Stoycheff, E. *et al.* (2019) ‘Privacy and the Panopticon: Online mass surveillance’s deterrence and chilling effects’, *New Media & Society*, 21(3), pp. 602–619. doi:10.1177/1461444818801317.

Stoycheff, E. and Nisbet, E.C. (2014) ‘What’s the Bandwidth for Democracy? Deconstructing Internet Penetration and Citizen Attitudes About Governance’, *Political Communication*, 31(4), pp. 628–646. doi:10.1080/10584609.2013.852641.

Stoycheff, E., Nisbet, E.C. and Epstein, D. (2016) ‘Differential Effects of Capital-Enhancing and Recreational Internet Use on Citizens’ Demand for Democracy’, *Communication Research*, 47(7), pp. 1034–1055. doi:10.1177/0093650216644645.

Tang, M. and Huhe, N. (2014) ‘Alternative framing: The effect of the Internet on political support in authoritarian China’, *International Political Science Review*, 35(5), pp. 559–576. doi:10.1177/0192512113501971.

Tsang, S. (2009) ‘Consultative Leninism: China’s new political framework’, *Journal of Contemporary China*, 18(62), pp. 865–880. doi:10.1080/10670560903174705.

Tufekci, Z. (2014) ‘Engineering the public: Big data, surveillance and computational politics’, *First Monday* [Preprint]. doi:10.5210/fm.v19i7.4901.

UNCTAD (2009) *United Nations Conference on Trade and Development: Manual for the Production of Statistics on the Information Economy*. UNCTAD/SDTE/ECB/2007/2/REV.1.

United Nations. Available at:
https://unctad.org/system/files/official-document/sdteecb20072rev1_en.pdf.

UNCTAD (2021a) *Gross domestic product: Total and per capita, current and constant (2015) prices, annual*. Electronic dataset. United Nations Conference on Trade and Development (UNCTAD). Available at: https://unctad.org/statistics.

UNCTAD (2021b) *Total and urban population, annual*. Electronic dataset. United Nations Conference on Trade and Development (UNCTAD). Available at: https://unctad.org/statistics.
Weidmann, N.B. *et al.* (2016) 'Digital discrimination: Political bias in Internet service provision across ethnic groups', *Science*, 353(6304), pp. 1151–1155. doi:10.1126/science.aaf5062.

Weidmann, N.B. and Rød, E.G. (2019) *The Internet and Political Protest in Autocracies*, *The Internet and Political Protest in Autocracies*. Oxford University Press. Available at: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190918309.001.0001/oso-9780190918309 (Accessed: 26 June 2021).

Xu, X. (2021) 'To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance', *American Journal of Political Science*, 65(2), pp. 309–325. doi:10.1111/ajps.12514.

Yan, au T. (2019) *Smart Cities or Surveillance? Huawei in Central Asia*, *The Diplomat*. Available at:
https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/ (Accessed: 26 June 2021).

Zeng, J. (2015) *The Chinese Communist Party's Capacity to Rule: Ideology, Legitimacy and Party Cohesion*. Springer.

Zeng, J. (2016) 'China's date with big data: will it strengthen or threaten authoritarian rule?', *International Affairs*, 92(6), pp. 1443–1462. doi:10.1111/1468-2346.12750.

Zeng, J. (2020) 'Artificial intelligence and China's authoritarian governance', *International Affairs*, 96(6), pp. 1441–1459. doi:10.1093/ia/iiaa172.

Appendix

Appendix A: Full variable list with data sources

The full dataset can be accessed at:
https://www.dropbox.com/s/zzmclfg2dk723md/dataset_v1.4.final.csv?dl=0

Variable	Description	Source
Country Name (*country_name*)	Name of coded country. Variable type: String	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Country Name Abbreviation (*country_text_id*)	Abbreviated country names. Variable type: String	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
V-Dem Country ID (*country_id*)	Unique country ID corresponding to IDs used in the V-Dem dataset. Variable type: Numeric	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
COW Code (*COWcode*)	Correlates of War (COW) project country codes. Variable type: Numeric	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Year (*year*)	Observation year coded annually from 2000–2020. Variable type: Interval	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Adoption of Chinese AI surveillance technology (*ctech*)	Adoption of Chinese AI surveillance technology coded as 0 (not adopted) before 2017 and as 1 (adopted) from 2017-2020.	Feldstein, S. 2019. *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace.

	Variable type: Binary	https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847
Government domestic dissemination of false information (*smgovdom*)	How often the government and its agents use social media to disseminate misleading viewpoints or false information to influence its own population. Values range from -5 (extremely often) to 5 (never, or almost never). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Government Internet shut down in practice (*smgovshut*)	How often the government shuts down domestic access to the Internet. Values range from -5 (extremely often) to 5 (never, or almost never). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Government social media shut down in practice (*smgovsm*)	How often the government shuts down access to social media platforms. Values range from -5 (extremely often) to 5 (never, or almost never). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Government social media censorship in practice (*smgovsmcenprc*)	The degree to which the government censors political content on social media. Values range from -5 (extremely often) to 5 (never, or almost never). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Arrests for political content (*smarrest*)	The likelihood of the arrest of a citizen that posts political content online that runs counter to the government and its policies. Values range from -5 (extremely likely) to 5 (extremely unlikely). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Government social media alternatives (*smgovsmalt*)	The prevalence of usage of social media platforms that are wholly controlled by either the government or its agents. Values range from -5 (all social media usage occurs on platforms controlled by the state) to 5 (practically no social media usage occurs on platforms controlled by the state).	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/

	Variable type: Ordinal	
Government social media monitoring (*smgovsmmon*)	How comprehensive the surveillance of political content is on social media by the government or its agents. Values range from -5 (extremely comprehensive) to 5 (not at all). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Online media existence (*smonex*)	The prevalence of domestic online media consumption. Values range from -5 (not at all) to 5 (extensively). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Online media fractionalization (*smmefra*)	How similar presentation of major (political) news is by major domestic online media outlets. Values range from -5 (extremely similar) to 5 (diverse). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Average people's use of social media to organize offline action (*smorgavgact*)	How often average people use social media to organize offline political action of any kind. Values range from -5 (never or almost never) to 5 (regularly). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Polarisation of society (*smpolsoc*)	The differences of opinions on major political issues in the society. Values range from -5 (serious polarisation) to 5 (no polarisation). Variable type: Ordinal	Mechkova, V., Pemstein, D., Seim, B., Wilson, S. 2020. Electronic dataset. *Digital Society Project Dataset v3*. Digital Society Project (DSP). http://digitalsocietyproject.org/data/
Military expenditure (*militaryexp*)	Country military expenditure as a percentage share of government expenditure. Variable type: Numerical	*SIPRI Military Expenditure Database 2015*. 2015. Electronic dataset. Stockholm International Peace Research Institute (SIPRI). http://milexdata.sipri.org
Polity2 score (*polity2*)	Democratic and autocratic regime changes. Values range from -10 (hereditary monarchy) to 10 (consolidated democracy).	*Polity V: Political Regime Characteristics and Transitions, 1800-2018*. 2018. Electronic

	Variable type: Interval	dataset. Center for Systemic Peace (CSP). https://www.systemicpeace.org/inscrdata.html
Civil liberties (*civlib*)	The extent to which civil liberties are respected. Values range from 0 (low respect) to 1 (high respect). Variable type: Interval	Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Bernhard, M., Cornell, A., Fish, M. S., Gastaldi, L., Gjerløw, H., Glynn, A., Hicken, A., Lührmann, A., Maerz, S. F., Marquardt, K. L., McMann, K., Mechkova, V., Paxton, P., Pemstein, D., von Römer, J., Seim, B., Sigman, R., Skaaning, S. E., Staton, J., Sundtröm, A., Tzelgov, E., Uberti, L., Wang, Y. T., Wig, T., Ziblatt, D. 2021. *V-Dem [Country–Year/Country–Date] Dataset v11.1*. Electronic dataset. Varieties of Democracy (V-Dem) Project. https://www.v-dem.net/en/data/data/v-dem-dataset-v111/
Political liberties (*pollib*)	The extent to which political liberties are respected. Values range from 0 (low respect) to 1 (high respect). Variable type: Interval	Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Bernhard, M., Cornell, A., Fish, M. S., Gastaldi, L., Gjerløw, H., Glynn, A., Hicken, A., Lührmann, A., Maerz, S. F., Marquardt, K. L., McMann, K., Mechkova, V., Paxton, P., Pemstein, D., von Römer, J., Seim, B., Sigman, R., Skaaning, S. E., Staton, J., Sundtröm, A., Tzelgov, E., Uberti, L., Wang, Y. T., Wig, T., Ziblatt, D. 2021. Electronic dataset. *V-Dem [Country–Year/Country–Date] Dataset v11.1*. Varieties of Democracy (V-Dem) Project. https://www.v-dem.net/en/data/data/v-dem-dataset-v111/
Internet penetration (*internet*)	The percentage of total households in the population with internet access at home.	*Digital Development Dashboard.* n.d. Electronic

	Variable type: Numerical	dataset. International Telecommunication Union (ITU). https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx
GDP per capita (*gdppp*)	Gross domestic product per capita in US dollars at constant prices (2015). Variable type: Numerical	UNCTAD. 2021. Electronic dataset. *Gross domestic product: Total and per capita, current and constant (2015) prices, annual.* United Nations Conference on Trade and Development (UNCTAD). https://unctad.org/statistics
Total population (*pop*)	The absolute value of the total population in thousands. Variable type: Numerical	UNCTAD. 2021. Electronic dataset. *Total and urban population, annual.* United Nations Conference on Trade and Development (UNCTAD). https://unctad.org/statistics
Urban population (*urbanpop*)	The percentage of the total population that live in urban areas. Variable type: Numerical	UNCTAD. 2021. Electronic dataset. *Total and urban population, annual.* United Nations Conference on Trade and Development (UNCTAD). https://unctad.org/statistics
Conflict (*newconf*)	The occurrence of a new conflict in the country (not a new episode of an ongoing conflict). Coded as 1 if the country-year contains a new conflict/conflict-dyad and 0 otherwise. Variable type: Binary.	Gleditsch, N. P., Wallensteen, P., Eriksson, M., Sollenberg, M., Strand, H. 2002. Armed Conflict 1946–2001: A New Dataset. Journal of Peace Research 39(5). https://ucdp.uu.se/downloads/index.html#onset

Appendix B: Full list of African countries included in the analysis indicating Chinese AI surveillance technology (AIST) adoption

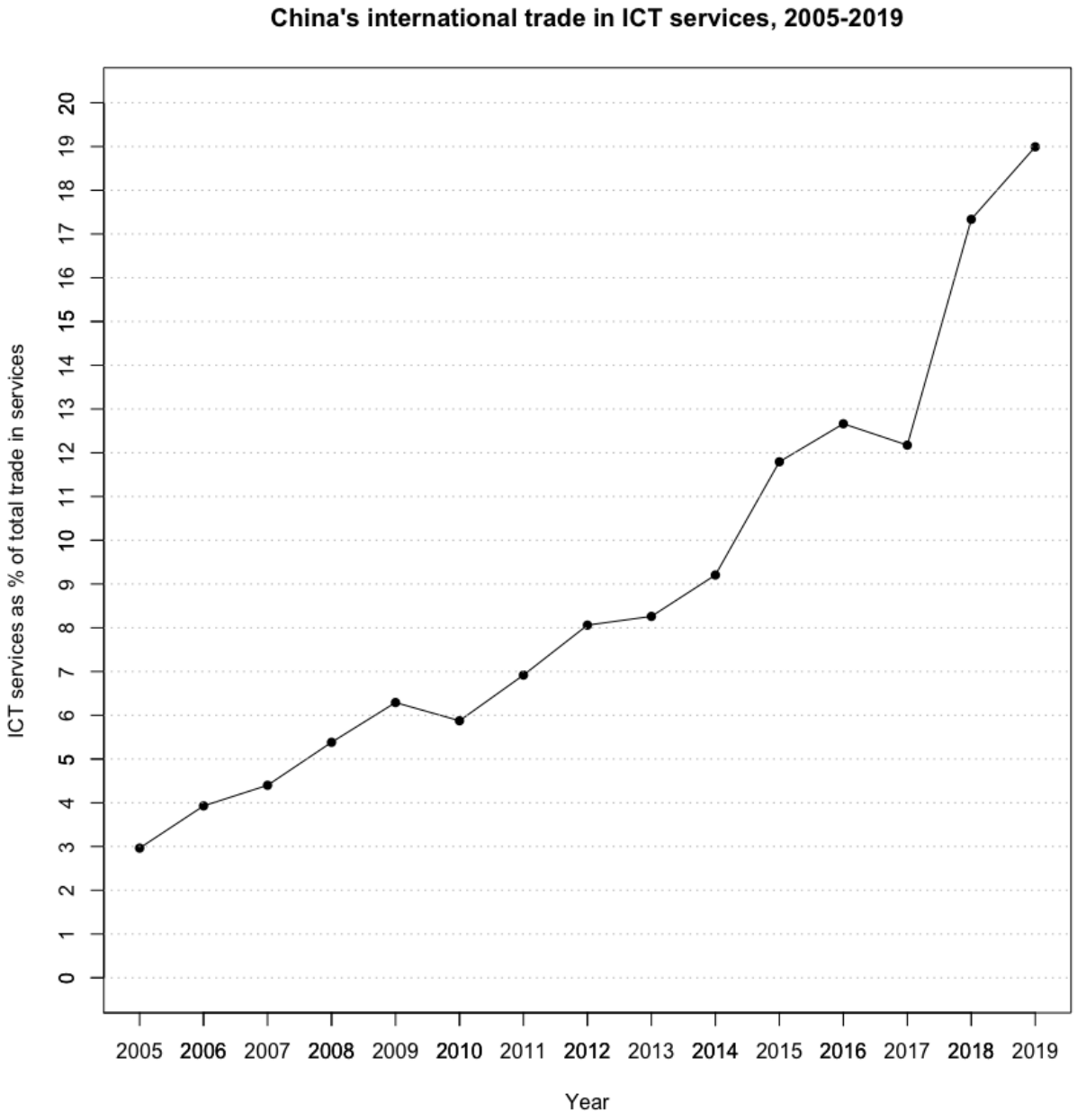
Country name	Adopted Chinese AIST?
Algeria	yes
Angola	no
Benin	no
Botswana	yes
Burkina Faso	no
Burundi	no
Cameroon	no
Cape Verde	no
Central African Republic	no
Chad	no
Democratic Republic of the Congo	no
Djibouti	no
Equatorial Guinea	es
Eritrea	no
Eswatini	no
Ethiopia	yes
Gabon	no
Ghana	yes
Guinea	no
Guinea-Bissau	no
Ivory Coast	yes
Kenya	yes
Lesotho	no
Liberia	no
Libya	no

Madagascar	no
Malawi	no
Mali	no
Mauritania	no
Mauritius	yes
Morocco	yes
Mozambique	no
Namibia	yes
Niger	no
Nigeria	yes
Republic of the Congo	no
Rwanda	yes
Senegal	no
Seychelles	no
Sierra Leone	no
Somalia	no
Somaliland	yes
South Africa	no
South Sudan	no
Sudan	no
Tanzania	no
The Gambia	no
Togo	no
Tunisia	no
Uganda	yes
Zambia	yes
Zimbabwe	yes
Total	**Yes**

52	16

Data source: Feldstein, S. 2019. The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace.
https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Appendix C: China's international trade in ICT services, 2005-2019



Data source: UNCTAD. 2020. Electronic dataset. *International trade in ICT services, value, shares and growth, annual*. United Nations Conference on Trade and Development (UNCTAD). https://unctad.org/statistics

Appendix D: Regression outputs

Table 1: Regression outputs for dependent variable government domestic dissemination of false information *(smgovdom)*

	OLS		2FE
	Bivariate	Multivariate	
	(1)	(2)	(3)
ctech	0.014	0.21	-0.216***
	(0.141)	(0.219)	(0.057)
militaryexp		-6.065*	
		(3.316)	
polity2		-0.059**	
		(0.026)	
civlib		3.964*	
		(1.989)	
pollib		-0.822	
		(1.857)	
internet		-0.001	
		(0.005)	
gdppp		-0.0001	
		(0.0001)	
pop		0.00000	
		(0.00000)	
urbanpop		0.002	
		(0.007)	
newconf		0.180	
		(0.386)	
smgovsmalt		0.343**	

		(0.132)	
smgovsmmon		0.193	
		(0.134)	
smonex		-0.106	
		(0.113)	
smmefra		-0.177*	
		(0.097)	
smorgavgact		-0.087	
		(0.100)	
smpolsoc		0.228**	
		(0.097)	
Observations	1,081	68	1,081
R^2	0.00001	0.823	0.911
Adjusted R^2	-0.001	0.767	0.905
			*p**p***p<0.01

Table 2: Regression outputs for dependent variable government internet shutdowns (*smgovshut*)

	OLS		**2FE**
	Bivariate	**Multivariate**	
	(4)	**(5)**	**(6)**
ctech	0.124	0.413	0.016
	(0.149)	(0.198)	(0.049)
militaryexp		-0.141	
		(2.995)	
polity2		0.061**	
		(0.023)	
civlib		3.821**	

		(1.796)	
pollib		-1.714	
		(1.677)	
internet		-0.008*	
		(0.004)	
gdppp		-0.0001	
		(0.0001)	
pop		-0.00000	
		(0.00000)	
urbanpop		-0.006	
		(0.007)	
newconf		-0.413	
		(0.349)	
smgovsmalt		0.693***	
		(0.119)	
smgovsmmon		-0.015	
		(0.121)	
smonex		0.239**	
		(0.102)	
smmefra		-0.171*	
		(0.087)	
smorgavgact		0.133	
		(0.090)	
smpolsoc		0.271***	
		(0.087)	
Observations	1,081	68	1,081
R^2	0.001	0.877	0.939
Adjusted R^2	-0.0003	0.839	0.935

*p**p***p<0.01

Table 3: Regression outputs for dependent variable government social media shutdown (*smgovsm*)

	OLS		2FE
	Bivariate	Multivariate	
	(7)	(8)	(9)
ctech	0.351**	0.697**	-0.063
	(0.147)	(0.278)	(0.056)
militaryexp		1.100	
		(4.200)	
polity2		0.059*	
		(0.033)	
civlib		1.782	
		(2.519)	
pollib		-1.043	
		(2.352)	
internet		-0.009	
		(0.006)	
gdppp		-0.0001*	
		(0.0001)	
pop		-0.00001***	
		(0.00000)	
urbanpop		-0.008	
		(0.009)	
newconf		-0.490	
		(0.489)	

smgovsmalt		-0.484***	
		(0.167)	
smgovsmmon		-0.045	
		(0.169)	
smonex		0.466***	
		(0.143)	
smmefra		-0.030	
		(0.123)	
smorgavgact		0.164	
		(0.127)	
smpolsoc		0.373***	
		(0.123)	
Observations	1,081	68	1,081
R^2	0.005	0.683	0.921
Adjusted R^2	0.004	0.583	0.916
			*p**p***p<0.01

Table 4: Regression outputs for dependent variable government social media censorship (*smgovsmcenprc*)

	OLS		**2FE**
	Bivariate	**Multivariate**	
	(10)	**(11)**	**(12)**
ctech	-0.062	0.376*	-0.218***
	(0.150)	(0.216)	(0.069)
militaryexp		1.221	
		(3.262)	
polity2		-0.006	
		(0.025)	

civlib		-4.846**	
		(1.957)	
pollib		5.507***	
		(1.827)	
internet		-0.012**	
		(0.004)	
gdppp		-0.0001	
		(0.0001)	
pop		-0.00001***	
		(0.00000)	
urbanpop		0.022***	
		(0.007)	
newconf		0.078	
		(0.380)	
smgovsmalt		0.007	
		(0.130)	
smgovsmmon		0.382***	
		(0.131)	
smonex		0.287**	
		(0.111)	
smmefra		0.154	
		(0.095)	
smorgavgact		0.143	
		(0.098)	
smpolsoc		-0.041	
		(0.095)	
Observations	1,081	68	1,081
R^2	0.0002	0.785	0.881

Adjusted R^2	-0.001	0.718	0.873
			*p**p***p<0.01

Table 5: Regression values for government arrests for posting political content online (*smarrest*)

	OLS		**2FE**
	Bivariate	**Multivariate**	
	(13)	**(14)**	**(15)**
ctech	0.164	-0.397**	-0.175**
	(0.151)	(0.164)	(0.077)
militaryexp		-10.395***	
		(2.478)	
polity2		-0.006	
		(0.019)	
civlib		-2.248	
		(1.486)	
pollib		1.542*	
		(1.388)	
internet		0.006*	
		(0.003)	
gdppp		0.0001*	
		(0.00004)	
pop		-0.00000	
		(0.00000)	
urbanpop		0.012**	
		(0.006)	
newconf		0.269	
		(0.289)	

smgovsmalt		0.117	
		(0.099)	
smgovsmmon		0.362***	
		(0.100)	
smonex		0.103	
		(0.085)	
smmefra		0.222***	
		(0.071)	
smorgavgact		-0.103	
		(0.075)	
smpolsoc		-0.011	
		(0.072)	
Observations	1,081	68	1,081
R^2	0.001	0.919	0.854
Adjusted R^2	0.0002	0.894	0.843
			*p**p***p<0.01

Table 6: Heteroskedasticity-robustness checks

	smgovdom		**smgovshut**		**smgovsm**		**smgovsmcenprc**		**smarrest**	
	2FE	**coeftest**	**2FE**	**coeftest**	**2FE**	**coeftest**	**2FE**	**coeftest**	**2FE**	**coeftest**
	(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**
ctech	-0.216***	-0.216*	0.016	0.016	-0.063	-0.063	-0.218***	-0.218	-0.175**	-0.175
	(0.057)	(0.123)	(0.049)	(0.099)	(0.056)	(0.131)	(0.069)	(0.135)	(0.077)	(0.159)
Observations	1,081		1,081		1,081		1,081		1,081	
R^2	0.014		0.0001		0.001		0.010		0.005	
Adjust	-0.056		-0.071		-0.070		-0.061		-0.066	

ed R^2					
					*p**p***p<0.01

Appendix E: Results replication code in R

```
### name dataset 'surv'

surv <- read.csv("dataset_v1.4.final.csv")

#################################################################
######### SIMPLE REGRESSION
#################################################################

library(texreg)

lm_falseinfo <- lm(smgovdom ~ ctech, surv)
screenreg(lm_falseinfo)

lm_intshut <- lm(smgovsm ~ ctech, surv)
screenreg(lm_intshut)

lm_smshut <- lm(smgovshut ~ ctech, surv)
screenreg(lm_smshut)

lm_censor <- lm(smgovsmcenprc ~ ctech, surv)
screenreg(lm_censor)

lm_arrest <- lm(smarrest ~ ctech, surv)
screenreg(lm_arrest)

#################################################################
######### MULTI REGRESSION
#################################################################

mlm_falseinfo <- lm(smgovdom ~ ctech
                    + militaryexp + polity2
                    + civlib + pollib + internet + gdppp
                    + pop + urbanpop + newconf
                    + smgovsmalt + smgovsmmon + smonex + smmefra
                    + smorgavgact + smpolsoc,
                    surv)
screenreg(mlm_falseinfo)

mlm_intshut <- lm(smgovsm ~ ctech
```

```
                  + militaryexp + polity2
                  + civlib + pollib + internet + gdppp
                  + pop + urbanpop + newconf
                  + smgovsmalt + smgovsmmon + smonex + smmefra
                  + smorgavgact + smpolsoc,
                  surv)
screenreg(mlm_intshut)

mlm_smshut <- lm(smgovshut ~ ctech
                 + militaryexp + polity2
                 + civlib + pollib + internet + gdppp
                 + pop + urbanpop + newconf
                 + smgovsmalt + smgovsmmon + smonex + smmefra
                 + smorgavgact + smpolsoc,
                 surv)
screenreg(mlm_smshut)

mlm_censor <- lm(smgovsmcenprc ~ ctech
                 + militaryexp + polity2
                 + civlib + pollib + internet + gdppp
                 + pop + urbanpop + newconf
                 + smgovsmalt + smgovsmmon + smonex + smmefra
                 + smorgavgact + smpolsoc,
                 surv)
screenreg(mlm_censor)

mlm_arrest <- lm(smarrest ~ ctech
                 + militaryexp + polity2
                 + civlib + pollib + internet + gdppp
                 + pop + urbanpop + newconf
                 + smgovsmalt + smgovsmmon + smonex + smmefra
                 + smorgavgact + smpolsoc,
                 surv)
screenreg(mlm_arrest)

#################################################################
######### FIXED EFFECTS
#################################################################

library(plm)
```

```
plm_falseinfo <- plm(
  smgovdom ~ ctech,
  data = surv,
  index = c("country_name", "year"),
  model = "within",
  effect = "twoways"
)
screenreg(plm_falseinfo)

plm_intshut <- plm(
  smgovshut ~ ctech,
  data = surv,
  index = c("country_name", "year"),
  model = "within",
  effect = "twoways"
)
screenreg(plm_intshut)

plm_smshut <- plm(
  smgovsm ~ ctech,
  data = surv,
  index = c("country_name", "year"),
  model = "within",
  effect = "twoways"
)
screenreg(plm_smshut)

plm_censor <- plm(
  smgovsmcenprc ~ ctech,
  data = surv,
  index = c("country_name", "year"),
  model = "within",
  effect = "twoways"
)
screenreg(plm_censor)

plm_arrest <- plm(
  smarrest ~ ctech,
  data = surv,
  index = c("country_name", "year"),
  model = "within",
```

```
  effect = "twoways"
)
screenreg(plm_arrest)

### calculating the R^2 for 2FE models

fe_falseinfo <- lm(smgovdom ~ ctech + as.factor(country_name) +
as.factor(year), surv)
screenreg(fe_falseinfo)

fe_intshut<- lm(smgovshut ~ ctech + as.factor(country_name) +
as.factor(year), surv)
screenreg(fe_intshut)

fe_smshut <- lm(smgovsm ~ ctech + as.factor(country_name) +
as.factor(year), surv)
screenreg(fe_smshut)

fe_censor <- lm(smgovsmcenprc ~ ctech + as.factor(country_name)
+ as.factor(year), surv)
screenreg(fe_censor)

fe_arrest <- lm(smarrest ~ ctech + as.factor(country_name) +
as.factor(year), surv)
screenreg(fe_arrest)

#################################################################
######### T-TESTS
#################################################################

t.test(surv$smgovdom~surv$ctech, 0, alt = "two.sided")

t.test(surv$smgovshut~surv$ctech, 0, alt = "two.sided")

t.test(surv$smgovsm~surv$ctech, 0, alt = "two.sided")

t.test(surv$smgovsmcenprc~surv$ctech, 0, alt = "two.sided")

t.test(surv$smarrest~surv$ctech, 0, alt = "two.sided")
```

```
#################################################################
######### ROBUSTNESS CHECKS
#################################################################

library(lmtest)

coeftest_plm_falseinfo <- coeftest(plm_falseinfo, vcov =
vcovHC(plm_falseinfo, type = "HC3"))
screenreg(list(plm_falseinfo, coeftest_plm_falseinfo))

coeftest_plm_intshut <- coeftest(plm_intshut, vcov =
vcovHC(plm_intshut, type = "HC3"))
screenreg(list(plm_intshut, coeftest_plm_intshut))

coeftest_plm_smshut <- coeftest(plm_smshut, vcov =
vcovHC(plm_smshut, type = "HC3"))
screenreg(list(plm_smshut, coeftest_plm_smshut))

coeftest_plm_censor <- coeftest(plm_censor, vcov =
vcovHC(plm_censor, type = "HC3"))
screenreg(list(plm_censor, coeftest_plm_censor))

coeftest_plm_arrest <- coeftest(plm_arrest, vcov =
vcovHC(plm_arrest, type = "HC3"))
screenreg(list(plm_arrest, coeftest_plm_arrest))
```