Exporting the Tools of Dictatorship: The Politics of China's Technology Transfers

Erin Baggott Carter and Brett L. Carter

The Chinese government is revolutionizing digital surveillance at home and exporting these technologies abroad. Do these technology transfers help recipient governments expand digital surveillance, impose internet shutdowns, filter the internet, and target repression for online content? We focus on Huawei, the world's largest telecommunications provider, which is partly state-owned and increasingly regarded as an instrument of its foreign policy. Using a global sample and an identification strategy based on generalized synthetic controls, we show that the effect of Huawei transfers depends on preexisting political institutions in recipient countries. In the world's autocracies, Huawei technology facilitates digital repression. We find no effect in the world's democracies, which are more likely to have laws that regulate digital privacy, institutions that punish government violations, and vibrant civil societies that step in when institutions come under strain. Most broadly, this article advances a large literature about the geopolitical implications of China's rise.

Erin Baggott Carter is an Assistant Professor in the Department of Political Science and International Relations at the University of Southern California (baggott@usc.edu), a Hoover Fellow at the Hoover Institution at Stanford University, a faculty affiliate at the Center on Democracy, Development and the Rule of Law (CDDRL) at Stanford University, and a nonresident scholar at the 21st Century China Center at UC San Diego. She received a Ph.D. from Harvard University. Her first book, Propaganda in Autocracies: Institutions, Information, and the Politics of Belief *(Cambridge University Press, 2023), studies the politics of propaganda. Her other work has appeared in the* British Journal of Political Science, Journal of Conflict Resolution, Security Studies, International Interactions, *China Quarterly, and* Foreign Affairs, *among others.*

Corresponding author: Brett Carter is an Assistant Professor in the Department of Political Science and International Relations at the University of Southern California (blcarter@usc.edu), a Hoover Fellow at Stanford University's Hoover Institution, and a faculty affiliate at Stanford's Center on Democracy, Development, and the Rule of Law. He received a Ph.D. from Harvard University, where he was a fellow at the Harvard Academy for International and Area Studies. His first book, Propaganda in Autocracies: Institutions, Information, and the Politics of Belief *(Cambridge University Press, 2023), probes the politics of propaganda. His articles have appeared in the* Journal of Politics, British Journal of Political Science, Journal of Conflict Resolution, Security Studies, Journal of Democracy, China Quarterly, *and* Foreign Affairs, *among others.*

1 Introduction

Despite China's growing global footprint, there remains widespread disagreement about the effects of Chinese engagement on politics and economics in recipient countries. Some observers view China as a "rogue donor," which directs aid to non-democratic governments and props them up in the face of domestic opposition.[1] Chinese aid appears more easily targeted towards domestic political constituencies (Dreher et al. 2022), is associated with perceptions of local corruption (Isaksson and Kotsadam 2018), and induces the World Bank to attach fewer "good governance" conditions to development projects (Hernandez 2016; Brazys and Vadlamannati 2021). Others argue that Chinese engagement may well be a net plus (Brautigam 2009). Chinese development finance has generated substantial economic returns, in part by providing major infrastructure projects that link economically productive areas (Dreher et al. 2022). There is no evidence that Chinese engagement fuels civil conflict or state repression (Gehring, Kaplan and Wong 2019) or systematically targets autocracies over democracies (Dreher et al. 2022).

Many in the policy community claim that one form of Chinese engagement – digital technology transfers – has pernicious effects in recipient countries. At home, the Chinese Communist Party (CCP) has combined ubiquitous surveillance cameras, the world's most sophisticated facial recognition software, DNA samples, and massive amounts of private data from domestic technology companies to let it reward supporters and punish dissidents with unprecedented precision (Xu 2021; Chin and Lin 2022). *The Washington Post* (2020) editorial board argued

doi:10.1017/S1537592724002226

that the CCP is exporting these tools of "digital authoritarianism" to "build a world in its image." Many NGOs, think tanks, and media outlets, agree, as does the United States Congress (Shahbaz 2018; Cave et al. 2019; Polyakova and Meserole 2019; Mozur, Kessel and Chan 2019; Andersen 2020; Barma, Durbin and Kendall-Taylor 2020; Feldstein 2020; U.S. Senate Committee on Foreign Relations 2020; Tiffert and McPherson-Smith 2022). Notwithstanding this emerging consensus among policymakers, there is virtually no quantitative evidence that informs this debate.

Do Chinese technology transfers help recipient governments expand digital surveillance, impose internet shutdowns, filter internet content, and engage in targeted repression against dissidents for online content?[2] To answer this question, we focus on Huawei Technologies, the largest global supplier of telecommunications equipment (Maizland and Chatzky 2020). Though technically privately held, Huawei is subject to substantial pressure from the CCP, receives large state subsidies, and is increasingly regarded as an instrument of foreign policy (Maizland and Chatzky 2020). Our focus on Huawei is motivated by data availability. The AidData project has coded Chinese foreign investments in a variety of sectors; reflecting Huawei's dominance of the Chinese telecommunications sector, it has coded contracts from this firm alone (Custer et al. 2021). This focus entails relatively few drawbacks. As the world's largest telecommunications provider, Huawei's foreign transfers far outstrip ZTE's, its closest Chinese competitor. As of 2019, Huawei's Safe City systems appeared in 700 cities across more than 100 countries; ZTE's appeared in just 160 cities across 45 countries (Chin and Lin 2022). In Africa, Huawei is responsible for 70% of the 5G network. Within China, Huawei has constructed 58% of 5G base stations; ZTE just 31% (Slotta 2024). If governments around the world receive Chinese technology transfers, they are overwhelmingly likely to come from Huawei. Second, although China's smaller, more focused technology firms occasionally enter into bilateral contracts with foreign governments, their technologies are routinely used as component parts in Huawei ecosystems, and hence often impossible to record separately (Cave, Ryan and Xu 2019). This inter-operability is a key principle of China's domestic technology supply chain. Consequently, Huawei offers a unique opportunity to assess the impact of digital technology transfers from China. The dataset records 153 Huawei projects worth roughly $1.6 billion in 64 countries worldwide between 2000 and 2017.

This article presents the first plausibly causal, cross-country evidence that Huawei digital technology transfers facilitate digital repression in the world's autocracies. For two reasons, we argue, digital technology transfers are more likely to have pernicious effects in autocracies than democracies. First, the motivations for acquiring Huawei digital technology may differ according to a country's preexisting political institutions. Threatened chiefly by collective action, the world's autocracies have stronger incentives to seek Huawei digital technology to repress protest leaders, block coordination by citizens, and strengthen their control over the domestic internet. Though some democratically-elected governments may seek digital tools to undermine the institutions that brought them to power (Feldstein 2021), democracies, on average, have stronger electoral incentives to provide public goods and foster economic growth, which Huawei technology transfers can facilitate (Acemoglu and Robinson 2019, 489-492). Second, different political institutions impose different constraints on how dual-use digital technologies are employed by recipient governments. The world's democracies are more likely to have guardrails – legislatures, courts, and independent media organizations – that increase the likelihood that dual-use digital technologies are used to advance living standards rather than violate basic rights (Wise 2020). When these institutions waver, the world's democracies are also more likely to feature vibrant civil societies that mobilize in defense of these institutions.

Estimating the effect of Huawei technology transfers on digital repression is complicated for three reasons. First, although Huawei allocates commitments in a given year, implementation generally occurs over several. As a result, there is almost certainly a lag of several years before the impact of the technology transfer is realized. Put differently, a recipient country is "treated" at the moment of the technology transfer, and this transfer persists, perhaps with heterogeneous effects due to an initial installation period or some other change in the recipient country. Second, Huawei's transfers to foreign governments have been staggered over time. Although we document two spikes – one in 2008, driven by a major commitment to Indonesia, and another in 2014, driven by the expansion of the Belt and Road Initiative (BRI) to Sub-Saharan Africa – these are the exception. Since roughly 2005, the annual rate of Huawei transfers to foreign governments has been relatively steady. Finally, the governments that receive Huawei transfers are systematically different than those that do not, and in ways that may be correlated with state repression.

To accommodate these features, we employ a generalized synthetic control (GSC) estimator (Xu 2017), which estimates an average treatment effect on the treated (ATT) by constructing counterfactual outcomes for each treated unit in each post-treatment period using data from a control group. Akin to an out-of-sample prediction model, the GSC estimator is robust to violations of the parallel slopes assumption required for differences-in-differences (DiD) estimators and accommodates the possibility that the effects of Huawei transfers may take time to realize.

Our dataset encompasses all known Huawei technology transfers to the world's governments between 2000 and 2017 (Custer et al. 2021; Carter & Carter 2024). We present three core results. First, Huawei technology transfers appear to be driven by market size, demand for low-cost telecommunications, and prior Chinese aid in recipient countries, rather than natural resource endowments or regime type. Second, in the world's autocracies, Huawei transfers increase digital surveillance, internet shutdowns, internet filtering, and targeted repression for online content. We find none of these effects in the world's democracies. We also find no evidence that expansion of a country's digital infrastructure more broadly is associated with digital repression, which suggests that the effect is unique to Huawei.

In addition to advancing our understanding about the effects of China's global engagement, this article contributes to two broad literatures. First, it illuminates the relationship between digital technology and autocratic survival. When the Information Age dawned, scholars and policymakers were optimistic that digital technologies would let citizens coordinate against repressive governments (Diamond 2010). Censoring the internet, President Bill Clinton quipped, was "like trying to nail Jello to the wall" (Allen-Ebrahimian 2016). Notwithstanding some evidence that telecommunications technologies foster protest (Manacorda and Tesei 2016; Christensen and Garfias 2018) and that many countries face significant obstacles in adopting Chinese surveillance technologies (Pan 2017; Feldstein 2021), it is increasingly clear that the world's autocracies have adapted, in part by exploiting technologies that enable widespread censorship (King, Pan and Roberts 2013; Gallagher and Miller 2019), mass surveillance (Feldstein 2021; Chin and Lin 2022; Beraja et al. 2023a,b), targeted repression (Frantz, Kendall-Taylor and Wright 2020; Xu 2021), and inhibit collective action (Gohdes 2015, 2020, 2024). The effect of digital technology on domestic politics, this article shows, is shaped by a society's political institutions.

Second, with American hegemony receding into multipolarity, scholars are confronted with new questions about autocratic politics in the 21st century. This article helps answer some of those questions. During the Cold War, with the United States and Soviet Union locked in geopolitical competition, many of the wold's autocrats secured financial support in exchange for membership in the Western or Eastern bloc. When the Berlin Wall collapsed, they lost this leverage and were forced to permit democratic reforms. This unleashed both a wave of democracy and nominally democratic institutions in autocracies (Levitsky and Way 2010). Given China's rise, America's apparent decline, and the outsized role of global hegemons in shaping political institutions (Gunitsky 2017; Miller 2021), a prolonged democratic recession seems increasingly likely (Diamond 2022). This article suggests one key mechanism of diffusion: technology transfers from China that are adapted by recipient governments to facilitate digital repression. This article also suggests, however, that this mechanism may serve principally to strengthen autocracies.

2 Theory

2.1 The CCP's Surveillance State

The Information Age has revolutionized surveillance in the world's autocracies. In 1998, the CCP launched the Golden Shield Project, which Xu (2021, 316) describes as "a domestic surveillance and filtering system that integrates online government databases with an all-encompassing surveillance network."[3] In the first phase, completed in 2005, the CCP built a massive network of population databases, ID tracking systems, and internet surveillance tools, which let it record the movement of potential dissidents as revealed, in part, by their online behavior. In 2017, the CCP announced the completion of its "Sky Net" program, which entails 176 million surveillance cameras across China and plans for 626 million by 2020, nearly one camera for every two citizens (Hersey 2017; Russell 2017). The result, Qiang (2019) writes, is "the largest video-surveillance network in the world."

Simultaneously, the CCP built a facial database that encompassed every adult citizen (Chin and Lin 2017) and a DNA database that encompassed 54 million citizens and, by 2020, will reportedly reach 100 million (Qiang 2019). The CCP's facial recognition technology is employed for check-in and security at airports (Dai 2018; Yang 2018), train stations (Chen, Jing and Dai 2018), and hotels (Chan 2018). In 2017, the CCP applied facial recognition technology to detect jaywalkers, with offenders notified via text message and their pictures displayed at major intersections (Li Tao 2018). This pervasive surveillance apparatus lets the CCP repress dissidents and spend less on public goods (Xu 2021). It also complements more analog forms of repression, such as informants and hired thugs (Deng and O'Brien 2013; Mattingly 2020; Ong 2022). Digital surveillance is now a conspicuous feature of everyday life.

The CCP's digital surveillance apparatus is supported by a network of domestic technology firms, which are subsidized by the state and routinely used as instruments of foreign policy. The most general are Huawei and ZTE. Huawei is the world's largest manufacturer of telecommunications equipment (Chin and Lin 2022, 131), and especially dominant in Africa, where it has provided 70% of the 5G network. Its products span mobile phones and other consumer electronics, telecommunications networks, face and voice recognition technology, and video cameras. China has a number of more focused technology firms that are implicated in surveillance. Several of these specialize in video cameras and facial recognition software: Hikvision,

Dahua, CloudWalk, Megvii, YITU, and SenseTime, most notably. Of these, Hikvision is perhaps the most consequential. In 2019, it was responsible for nearly a quarter of the world's surveillance cameras (Hillman 2021, 98). Dahua has also supplied cameras for Safe City projects, so called for their use of digital surveillance to support the local security apparatus (Chin and Lin 2022). Other firms specialize in still different areas of surveillance. Meiya Pico reportedly built an app used by the Chinese government to extract data from citizens' smartphones during street checks (Chen and Jing 2019; Cheng 2020). iFlytek develops voice recognition software (Hvistendahl 2020). Each of these firms has been sanctioned by Washington.

As the largest and most general of China's technology firms, Huawei often collaborates with the more specialized firms, both to develop new technologies and to ensure inter-operability: that the technologies developed by the specialized firms work on Huawei's infrastructure. Huawei partnered with Megvii to enhance the CCP's facial recognition technology in Xinjiang (Harwell and Dou 2020). Huawei teamed up with iFlytek to develop the "iFlytek Voiceprint Management Platform," which "can identify individuals by comparing the sound of their voice against a large database of recorded 'voiceprints'" (Dou 2021). The voice assistant in Huawei's smartphones thus features iFlytek's voice recognition software (Cave, Ryan and Xu 2019). Huawei has partnered with other Chinese technology firms to pioneer surveillance tools for prisons, "political persons of interest," and even employees of private sector firms (Dou 2021). Huawei's Smart City systems routinely incorporate YITU's facial recognition and traffic monitoring software (Cave, Ryan and Xu 2019).

2.2 Exporting Digital Surveillance Technology

Governments across the world have sought to acquire Chinese digital technology. Huawei, given its scale, has been central to this, often incorporating the technologies developed by China's smaller, more focused firms. The anecdotal evidence suggests four broad ways that these exports can be adapted by recipient governments to facilitate digital repression.

The first is facial recognition. Huawei's Safe City programs generally feature video surveillance cameras, which feed data to police command centers and help detect dissidents. Huawei began marketing its Safe City technology abroad in 2010 (Chin and Lin 2022, 134). In 2017, Huawei identified 40 countries where its Smart City surveillance technology had been introduced. By 2018, its reach had expanded to at least 90 countries and 230 cities (Cave et al. 2019). By 2019, Huawei had installed Safe City systems in 700 cities across more than 100 countries (Chin and Lin 2022, 135). Huawei pitches its digital surveillance technologies to national security agencies, with subsidized financing provided by China's Exim Bank (Feldstein 2019). ZTE provides similar packages, but its scope is much smaller. It began marketing its Safe City solutions several years after Huawei and, by 2019, had built similar systems in 160 cities across 45 countries (Chin and Lin 2022, 135). Governments occasionally advertise these surveillance capabilities to citizens, even emphasizing their Chinese origins. In Cameroon, as the Anglophone Crisis raged in February 2017, the government announced a contract with Huawei on the front page of its flagship propaganda newspaper, the *Cameroon Tribune*, that provided for "1,500 cameras in regional capitals and certain strategic points in the country," "2,000 portable listening devices equipped with cameras," and "the construction of nine command centers" (Carter and Carter 2023).

Second, the telecommunications networks installed by Huawei generally feature surveillance middleboxes with Deep Packet Inspection capabilities. These middleboxes power China's Great Firewall, the most extensive censorship operation in human history (King, Pan and Roberts 2013). They monitor users' internet activity, can censor online content, and can block access to virtual private networks (Weber and Ververis 2021). Huawei's middleboxes have been documented in 72 countries. In at least 18 of those, the middleboxes have been used for internet censorship (Earp 2021; Weber and Ververis 2021). Middleboxes with Deep Packet Inspection capabilities have been linked to internet and social media shutdowns (Woodhams and O'Donnell 2021), an increasingly ubiquitous feature of life in autocracies (Feldstein 2021), even if such shutdowns undermine a government's ability to collect high-quality intelligence (Gohdes 2015, 2020, 2024).

Third, China's technology transfers have been used to create the sort of integrated surveillance system that the CCP's Golden Shield Project pioneered. This has been especially well documented in Venezuela, where ZTE helped the government create a national identification card – dubbed the "fatherland card" – that records voting behavior, party membership, social media use, personal finances, and medical histories. ZTE provided servers for the database and developed the ID card's mobile payment application. The Maduro government appears to be using the fatherland card to divert state resources to loyalists and monitor dissidents: "Everybody must get one," Maduro announced in 2016. Said one Venezuelan technical advisor, who was assaulted and accused of treason after he objected to it: "What we saw in China changed everything. They were looking to have citizen control" (Berwick 2018). As of 2015, ZTE was helping the government build a series of "emergency response centers" in urban areas and centralize its video surveillance capabilities (U.S. Senate Committee on Foreign Relations 2020, 30-31).

The broader objective, many citizens believe, is a "social credit system" modeled after the CCP's (Polyakova and Meserole 2019).

Of course, the ability of recipient governments to use Chinese technology transfers for digital repression may be hampered by limited state capacity or other obstacles (Pan 2017). Feldstein (2021) documents, for instance, how several governments have imported the tools of digital repression, but have had difficulty putting them to use. This may be why Huawei offers direct personnel support to recipient governments. This is nowhere more apparent than in Sub-Saharan Africa, where preexisting digital surveillance capabilities are generally less sophisticated than those provided by Chinese firms. In 2018, for instance, the Ugandan security apparatus began to track Bobi Wine, a musician turned leading opponent to President Yoweri Museveni in the 2021 election. After installing spyware on Wine's phone, the Ugandan police enlisted Huawei engineers – with whom they shared an office, emblazoned with Huawei's logo on the walls – to help them operate it. Huawei engineers helped Ugandan security officials intercept encrypted messages, eavesdrop on his phone, and track his location (Parkinson, Bariyo and Chin 2019; Woodhams 2019; Chin and Lin 2022). Huawei engineers provided similar support in Zambia, helping security forces intercept encrypted messages sent by local journalists, track their whereabouts, and ultimately help with their arrest (Woodhams 2019).

2.3 Differential Effects by Preexisting Political Institutions

To be sure, there are important differences among forms of digital repression (Gohdes 2015, 2020, 2024). Surveillance technologies – such as facial recognition, content monitoring, and location tracking – help governments engage in targeted repression against dissidents and opposition leaders. By contrast, censorship technologies – like internet shutdowns and internet filtering – may provide cover for indiscriminate repression and inhibit collective action, but at the cost of high-quality intelligence that can help governments target dissidents with precision. Technically, shutdown technologies may also be easier to implement than surveillance technologies, which some governments have had trouble using effectively even after adoption (Feldstein 2021).

Our focus is not on the strategic calculations and technical constraints that give rise to different forms of digital repression. Autocrats, after all, may employ different technologies at different times and against different targets, using Chinese technology transfers for digital surveillance and internet shutdowns alike. Rather, we probe whether Chinese technology transfers have been adapted to facilitate digital repression, broadly construed, and whether there are key differences across regimes. Technology transfers, indeed, are intrinsically dual-use. Recipient governments can use them for digital repression, as the examples in Section 2.2 suggest, but also to expand internet access, provide public goods, and give citizens tools to monitor governments and coordinate collective action against them. Chinese technology firms are attractive suppliers on purely market terms. Huawei's telecommunications equipment, in particular, is generally high-quality and as much as 30% cheaper than competitors, due in part to financial subsidies from the Chinese government (El Kadi 2022) and preferential loan terms from the Exim Bank (Feldstein 2019).

Our basic argument is that dual-use technology transfers are likely to have differential effects based on a country's preexisting political institutions. The world's autocracies and democracies likely pursue Huawei technology transfers for different objectives and, once acquired, confront different constraints in their application.

2.3.1 Different Objectives. Autocracies and democracies may want digital technology for different reasons. Since the end of the Cold War, as the rate of coups has declined, popular protests have emerged as a chief threat to autocratic survival (Marinov and Goemans 2014). This is especially true in Sub-Saharan Africa, home to nearly half of the world's autocracies. Between 1960 and 1989, on average, 70% of all autocratic exits each year were due to coups or assassinations, while just 25% of exits were driven by elections, term limits, revolts, and other forms of popular pressure. After the Cold War, this flipped. Between 1990 and 2021, 25% of autocratic exits were due to coups or assassinations, while 68% were driven by elections, term limits, and other forms of popular pressure (Carter 2024). Insofar as Chinese technology transfers help recipient governments block collective action – by repressing potential protest leaders or making coordination among participants as difficult as possible – the world's autocrats should have particularly strong incentives to acquire them.

Some democratically-elected presidents may attempt to use Huawei technology transfers to undermine the institutions that brought them to power. On average, however, political leaders in democracies have stronger electoral incentives to provide public goods and foster economic growth. Again, since Chinese technology transfers are intrinsically dual use, their relatively cheaper price points are attractive for these objectives as well. Indonesia, as we document in Section 3, is the largest single recipient of Huawei technology transfers. Part of this may have been driven by the public security interests of the government of President Susilo Bambang Yudhoyono, who held office between 2004 and 2014 (Guild 2021; Kurlantzick 2021). But part of it is also due to the economic policies of his successor, Joko Widodo, who has made support for Indonesia's technology sector a centerpiece of his economic

program. In addition to providing telecommunications equipment that links Indonesia's islands, in 2020 Huawei committed to training 100,000 citizens in ICT technology, part of an effort to redress the skills gap between Indonesia and other major Asian economies (Herscovitch, van der Kley and Priyandita 2022; Priyandita, van der Kley and Herscovitch 2022).

Huawei's engagement in Ghana, the 10th leading recipient of Huawei transfers in Sub-Saharan Africa and among the continent's most vibrant democracies, appears to be similar. By 2022, Huawei technology transfers had facilitated the emergence of one of Africa's leading tech hubs and an internet penetration rate of 53%, considerably greater than the African average (28% in 2019) and only slightly lower than Mississippi (59% in 2020) and Texas (68% in 2020).[4] In 2019, Accra, Ghana's capital, became home to Google's first artificial intelligence (AI) lab in Africa (Adeyemi 2021). Accra-based innovators are developing technologies to reduce identity theft (de Vergès 2020), facilitate electronic payments, improve agricultural output, strengthen cross-border supply chains, and monitor COVID's spread (Adeyemi 2021).

2.3.2 Different Constraints. Autocracies and democracies also confront different constraints on the use of dual-use technologies for digital repression. In democracies, the spread of digital technology has often been accompanied by contentious debates about personal privacy. These debates are facilitated by political institutions that let citizens, elected officials, and courts monitor how governments use digital technologies, and hence ensure that technology transfers are used to advance the public interest (Adeniran and Osakwe 2021). Elected leaders also confront the prospect of prosecution, which, in turn, shapes their behavior in office. These political institutions are buttressed by free and independent media, which help document government malfeasance. When these institutional guardrails waver in the face of executive power grabs, vibrant civil societies can mobilize to defend them (Feldstein 2021).

These constraints – from institutions, media watchdogs, and vibrant civil societies – are perhaps nowhere more evident than in Costa Rica, one of Latin America's most vibrant democracies and, as we document in Section 3, the fourth leading recipient of Huawei technology transfers. These transfers are one reason that internet penetration increased from 36.5% in 2010 to 82.7% in 2021 (Alvarado, Fernando Martínez de Lemos and Weal 2022). In 2018, shortly after his election, Costa Rican President Carlos Alvarado Quesada quietly created the Presidential Unit of Data Analysis, which compiled confidential personal data from other government entities, he said later, to craft better policy. In response, in 2020, Costa Rican prosecutors raided presidential offices, ultimately compelling a series of senior resignations and oversight hearings by the national legislature. Soon thereafter, Alvaros disbanded the unit itself (Cordoba 2020; Alvarado, Fernando Martínez de Lemos and Weal 2022). By the end of 2021, six months before his presidential term expired, Alvarado's approval rating was just 12% (Arrieta 2021). In many cases, protections against such actions are made explicit in national constitutions. Section 32 of the South African constitution "provides that everyone has the right of access to any information held by the state," a right further enshrined by the Promotion of Access to Information Act 2 of 2000 (Restore Data Rights 2022). Put simply, countries with democratic institutions are far better placed to ensure that new communications technologies are managed in a way that minimizes the probability of digital repression (Acemoglu and Robinson 2019, 489-492).

Autocratic governments are less encumbered by institutions and civil societies that might prevent the use of telecommunications infrastructure for digital repression. From Section 2.2, since roughly 2015 the Ugandan government has used Huawei technology to monitor the social media accounts of opposition leaders, intercept their encrypted communications, and track their location (Parkinson, Bariyo and Chin 2019; Woodhams 2019). The government ignored existing laws that forbade doing so and, as Museveni consolidated power, passed new laws that give it more latitude. The Ugandan constitution, enacted in 1995, ostensibly guarantees the rights to privacy that the government's use of Huawei technology violated (Unwanted Witness 2015). In 2010, the government passed legislation that let it monitor private communications (Mayiga 2010). In 2011 and again in 2022, the government passed legislation that gave it broad latitude to criminalize online speech and made offenses punishable by up to 10 years in prison. Each of these elicited condemnation from citizens and civil society groups; the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) called the 2022 law "a blow to online civil liberties in Uganda" (Muhumuza 2022). But given Museveni's hold on power, digital repression has only intensified. In 2019, the Ugandan security forces contracted a $126 million facial recognition system from Huawei (Kafeero 2020).

3 Data and Descriptive Statistics

3.1 What, Who, and When

To probe the effects of Chinese technology transfers in recipient countries, we focus on Huawei. We do so principally for reasons of data availability. Since technology transfers are generally covert, we lack systematic data on the range of transfers provided by individual Chinese companies. Huawei, the world's largest telecommunications provider, is an exception. AidData's Global Chinese Development Finance Dataset records 153 Huawei

projects worth roughly $1.6 billion in 64 countries worldwide between 2000 and 2017 (Custer et al. 2021). We view this as a relatively low-cost tradeoff. If governments around the world receive Chinese technology transfers, as we discussed in Section 1, they are overwhelmingly likely to come from Huawei. Since technologies developed by China's smaller, more focused technology firms are routinely embedded in broader Huawei systems (Cave, Ryan and Xu 2019), Huawei transfers are a good proxy for technology transfers from other Chinese firms.

When major Chinese firms strike agreements with foreign governments, they often insist on keeping their details secret. For example, contracts between the Chinese and Ecuadorian governments only became public after the 2016 Panama Papers leak. Huawei's contract with the Mauritius Safe City Project required the Mauritian police and Mauritius Telecom to invoke confidentiality when questioned by civil society groups (Walker 2023). Inferentially, this secrecy creates measurement error; its principal effect is to include in the control group some countries that were actually treated with Chinese digital technology transfers. This biases against the article's key results. Our estimates below, therefore, should be regarded as a lower bound on Huawei's effects on digital repression in recipient countries.

AidData classifies Huawei's projects into 14 sectors, which appear, by shares, in the top left panel of figure 1. The top right panel gives the leading sectors by project value. For both metrics, the most common sector for Huawei transfers is communications, which, by value, accounts for 90% of all projects worldwide. Projects in the communications sector generally focus on the provision of telecommunications and surveillance equipment to recipient governments. By frequency, the second leading sector is education, but, by value, this constitutes just 0.01% of Huawei's projects. Many of these are government training programs that support equipment transfers or various programs at educational institutions. By value, Huawei's second leading sector is energy, accounting for roughly 10% of transfers. These projects include transfers to Cameroon and Ethiopia, among the world's more repressive governments, that strengthen electricity provision, which is key to powering cameras and other digital surveillance technologies. The center left panel displays the share of Huawei transfers by world region. Together, Asian and African countries account for more than 85% of total Huawei transfers. In Africa, Huawei alone is responsible for as much as 70% of the telecommunications network (Woodhams 2019). Latin American countries account for roughly 13% of transfers. Transfers to European and Middle Eastern countries are negligible.

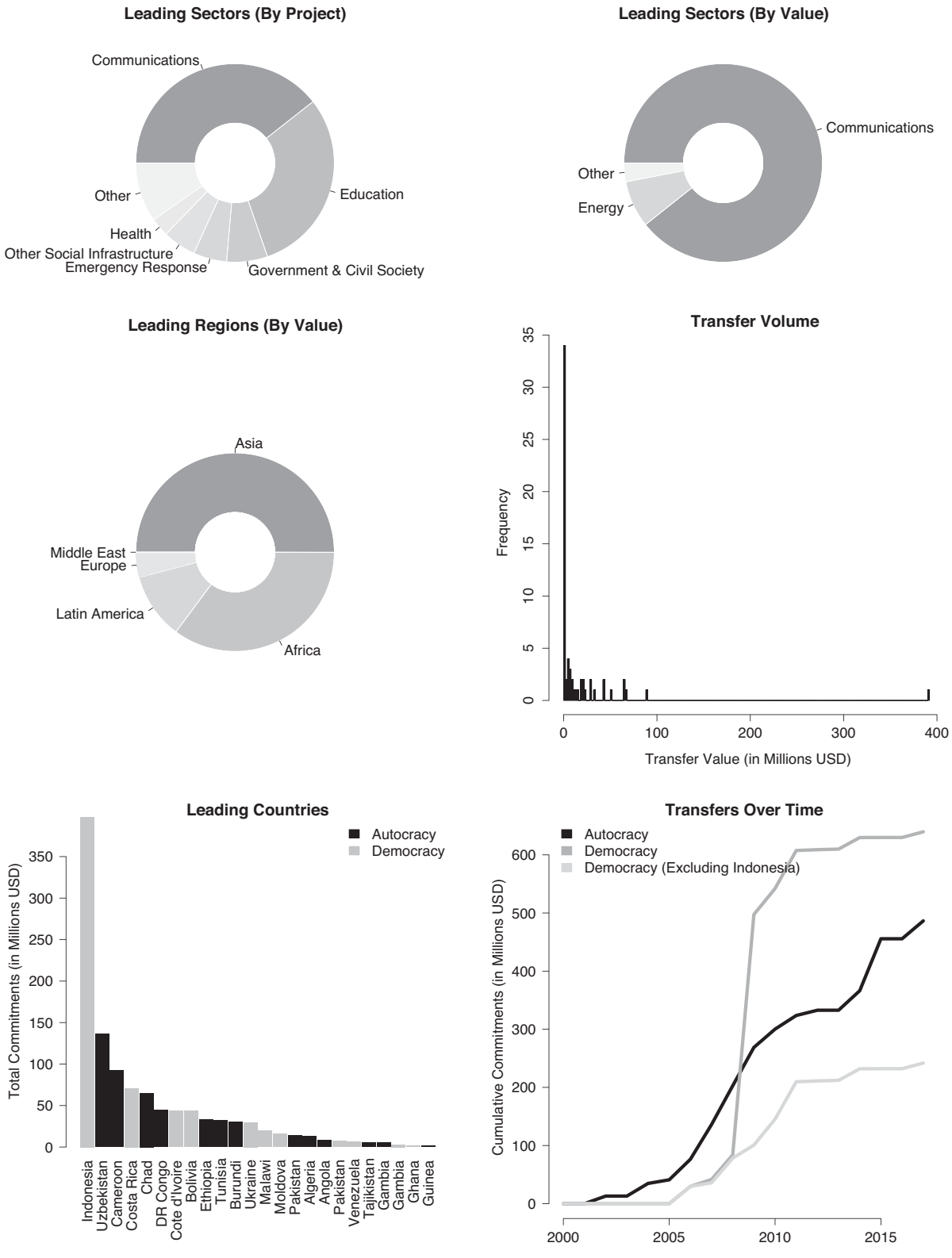
The center right panel presents a histogram for the volume of each of the Huawei transfers included in the dataset. For each total transfer value along the *x*-axis, the *y*-axis gives the number of countries that received it. The single largest recipient is Indonesia, with transfers amounting to $391 million. The largest of these occurred in 2009, when Huawei extended a $300 million supplier credit to PT Telkom, a state-owned telecommunications company. By 2022, Huawei had emerged as the largest provider of telecommunications equipment to the Indonesian market, propelled both by its low-cost hardware and its instructional programs to Indonesia's universities and government agencies (Herscovitch, van der Kley and Priyandita 2022; Priyandita, van der Kley and Herscovitch 2022).

The median transfer value is $1.2 million, just greater than the value of the surveillance equipment that Uganda's Kampala city government was promised in 2014 to "track illegal activity." In 2015, Museveni formally received from the Chinese ambassador the "Safe City Integrated Communication Platform," which, Custer et al. (2021) note, entailed "20 monitor cameras in 10 key monitoring points in Kampala," similar to what had "improved the administrative capacity of the Urumqi Municipal Administration and the efficiency of Uighur police." Huawei was nearing completion of the platform as of September 2016. By 2018, Ugandan security services were using Huawei technology to track Bobi Wine and other opposition activists (Woodhams 2019).

The bottom left panel gives recipients of Huawei technology transfers worth at least $1 million, shaded according to regime type at the time of the transfer.[5] The top recipient, again, is Indonesia. Other leading recipients include several of the world's most repressive governments: Uzbekistan under Islam Karimov, Cameroon under Paul Biya, Chad under Idriss Déby, Democratic Republic of Congo (DRC) under Joseph Kabila, Ethiopia under Meles Zenawi, Tunisia under Ben Ali, and Burundi under Pierre Nkurunziza. The fourth leading recipient, however, is Costa Rica, one of Latin America's most vibrant democracies, which has been credited for its efforts to protect digital privacy (Alvarado, Fernando Martínez de Lemos and Weal 2022).

The bottom right panel displays the cumulative value of Huawei technology transfers, by year, across autocracies and democracies. The aggregate data suggests that Huawei technology transfers have flowed slightly more to the world's democracies than the world's autocracies: roughly 55% to 45%, respectively. This is somewhat misleading, however, as the light gray line suggests. Excluding Indonesia, Huawei transfers have flowed disproportionately to the world's autocracies, accounting for nearly 70% of all transfers. Indonesia also distorts how we understand the regional allocation of Huawei transfers. Excluding Indonesia, the African continent accounts for 55% of all Huawei transfers, with Asia and Latin America accounting for just 22% and 16%, respectively.

Figure 1
Descriptive statistics



3.2 Correlates of Huawei Transfers

To better understand which countries receive Huawei transfers, we move to a simple regression framework. We estimate several models of the form:

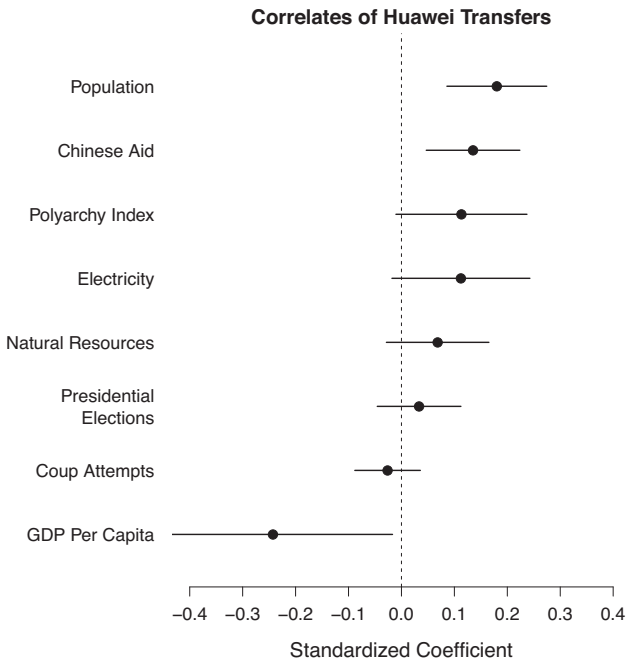
$$Y_{it} = \alpha + \beta X_{it} + \gamma_t + \epsilon \quad (1)$$

where i indexes country, t indexes year, and γ_t gives year fixed effects. The outcome Y_{it} measures the logged value of Huawei commitments in year t. The vector X_{it} includes country-level characteristics that may condition the government's interest in securing Huawei technology and Huawei's interest in providing it.

The results appear in figure 2. The x-axis reports point estimates for the standardized coefficients, surrounded by 95% confidence intervals. The results are identical across specifications.[6] Huawei transfers, we find, are driven chiefly by demand in recipient countries. More populous countries are more likely to receive Huawei transfers, as are countries with lower GDP per capita. This is intuitive. More populous countries represent more attractive markets for Huawei, while less affluent countries are more likely to be attracted by its lower price point. Huawei transfers are also more likely if the recipient government has a preexisting relationship with the CCP, as measured by its aid allocation in year t.

Equally interesting are the country-level characteristics that have no effect on Huawei transfers. Notwithstanding the cumulative transfer data in the bottom right panel of figure 2, we find no evidence that Huawei transfers are more likely in autocracies than democracies. The correlation that appears in a bivariate setting is not robust to the inclusion of other controls. We also find no evidence that Huawei technology transfers flow disproportionately to countries that are rich in natural resources or politically unstable, as measured by coup attempts in year $t-1$. In this respect, Huawei transfers are distinctive relative to transfers of facial recognition technology from Chinese firms, which flow disproportionately to nondemocracies with histories of political unrest (Beraja et al. 2023b).

Figure 2
Correlates of Huawei technology transfers



4 Generalized Synthetic Control Method

4.1 Challenges of Inference

Estimating the effect of Huawei technology transfers on digital repression is complicated for three reasons. First, although Huawei allocates commitments in a given year, the implementation generally occurs over several. Consequently, there may be a lag of several years before the impact of the transfer is realized. Put differently, a recipient country is "treated" at the moment of the transfer, and this transfer persists, though perhaps with heterogeneous effects due to an initial installation period or some other change in the recipient country.

Second, as the bottom right panel of figure 1 made clear, Huawei transfers were staggered over time. In Sub-Saharan Africa, the most significant roll-out followed the expansion of the BRI between 2014 and 2015, which accounted for 36% of the region's transfers during the sample period. The next most significant expansion followed the Global Financial Crisis of 2009, when the CCP sought to generate foreign demand for Chinese goods – and hence reduce the likelihood of a domestic recession – partly by having state-owned enterprises undertake major construction projects abroad (China News 2008; Yu 2010; Lardy 2012; Wallace 2014).

Third, from the coefficient plots in figure 2, the countries that received Huawei technology transfers are systematically different than those that did not. They are, on average, more populous, poorer, and more likely to receive Chinese aid.

4.2 Estimation Strategy

To accommodate these features, we employ the GSC estimator developed by Xu (2017). The GSC estimator is also appealing because it is robust to violations of the parallel trends assumption, which is required by conventional DiD estimators but inherently untestable.

To estimate the ATT population, the GSC estimator imputes a counterfactual outcome for treated unit i at time t. It does so in three steps. First, using only data from the control group,[7] it estimates a model using interactive

fixed effects (IFE) or the matrix completion (MC) method proposed by Athey et al. (2021).[8] Second, it uses these results from the control group to estimate factor loadings for each treated unit by minimizing the mean squared error of the predicted treated outcome in pre-treatment periods. Finally, it constructs counterfactual outcomes for each treated unit in each post-treatment period and estimates the ATT based on the differences between the observed and these counterfactual outcomes. In this sense, the GSC estimator is akin to an out-of-sample prediction method.

Implementing the GSC estimator requires specifying some minimum number of pre-treatment periods, which are used by the GSC estimator to impute counterfactual outcomes. Intuitively, specifying a higher number of minimum pre-treatment periods increases the information with which the GSC estimator imputes counterfactual outcomes, but at the expense of discarding countries that were treated early, at least relative to the beginning of the data. We specify a five-year pre-treatment minimum as a compromise. As we discuss below, our protest and repression variables begin in 1995; Huawei transfers begin around 2001. The five-year minimum lets us maximize country coverage while also providing ample information to the GSC estimator. Our country sample is global.

The basic functional form is:

$$Y_{it} = \beta_{it}(\text{Treated}_{it}) + \delta X_{it} + \lambda_i f_t + \epsilon \qquad (2)$$

where i indexes country, t indexes year, and X_{it} is a vector of time- and country-variant controls. The explanatory variable of interest, $Treated_{it}$, equals 1 if country i received Huawei transfers greater than some threshold T during year t or in some year since. We let this threshold T vary: from a commitment of just \$250,000 in year t to transfers of \$500,000, \$1 million, \$5 million, and \$10 million in year t. From Section 3, these treatment thresholds are substantively meaningful; the median transfer value is just greater than \$1 million. During the sample period, 40 countries received a transfer worth at least \$250,000, 34 received a transfer worth at least \$1 million, 28 worth at least \$5 million, and 19 worth at least \$10 million.

Our theory identifies four likely effects of Huawei technology transfers: internet shutdowns that block collective action by citizens, internet filtering that censors online content, digital surveillance, and the sort of targeted repression for online content that digital surveillance facilitates. The V-Dem project includes variables that capture each of these effects. These variables are summarized in table 1 (Coppedge et al. 2022).[9] We rescale these variables to make them more intuitive for readers, such that a higher value indicates more digital repression.[10]

The vector X_{it} includes potential country- and time-varying confounders. We control for a range of features that may reflect underlying political instability, which could be associated with both Huawei transfers and domestic repression: the number of protest and repression events as recorded by the Integrated Crisis Early Warning System (ICEWS) dataset (Boschee et al. 2015),[11] coup attempts (Powell and Thyne 2011), successful coups, and whether country i witnessed a presidential election, as recorded by Coppedge et al. (2022). We control for economic features that might be associated with Huawei transfers and domestic repression: country i's GDP per capita and GDP in year t. We also control for country i's electrification rate, which might condition the capacity of recipient governments to use Huawei technology transfers for digital repression or citizens' ability to engage in collective action. The term $\lambda_i f_t$ represents the factor component of the model: f_t is a vector of unobserved common factors and λ_i is a vector of unknown factor loadings.[12]

We estimate separate models for autocracies and democracies, which let the effect of Huawei technology transfers be a function of country i's preexisting political institutions.

Table 1
Measuring digital repression

Variable	Description
Internet Filtering	How frequently does the government censor political information (text, audio, images, or video) on the Internet by filtering (blocking access to certain websites)?
Social Media Monitoring	How comprehensive is the surveillance of political content in social media by the government or its agents?
Internet Shutdowns	How often does the government shut down domestic access to the Internet?
Arrests for Online Content	If a citizen posts political content online that would run counter to the government and its policies, what is the likelihood that citizen is arrested?

4.3 Results

Table 2 reports the ATT estimates averaged across countries and periods. The results for autocracies appear in the top panel, which reports estimates from 20 regression models: one for each of the five treatment thresholds along the left and the four outcome measures along the top. The results are consistent with the theory. Huawei technology transfers increase the likelihood of internet filtering, internet shutdowns, digital surveillance, and arrests for online content.

Table 2
Empirical results

	Autocracies *Dependent variable:*			
	Internet Filtering	**Internet Shutdowns**	**Social Media Monitoring**	**Arrests for Political Content**
Treatment Threshold 1				
Transfer ≥ $250,000	0.279***	0.317***	0.275**	0.194***
	(0.088)	(0.083)	(0.122)	(0.062)
Treatment Threshold 2				
Transfer ≥ $500,000	0.299***	0.344***	0.278*	0.177**
	(0.089)	(0.088)	(0.143)	(0.070)
Treatment Threshold 3				
Transfer ≥ $1,000,000	0.399***	0.433***	0.395**	0.207***
	(0.093)	(0.102)	(0.165)	(0.077)
Treatment Threshold 4				
Transfer ≥ $5,000,000	0.424***	0.451***	0.414**	0.209**
	(0.097)	(0.110)	(0.189)	(0.084)
Treatment Threshold 5				
Transfer ≥ $10,000,000	0.481***	0.473***	0.419*	0.131
	(0.134)	(0.147)	(0.231)	(0.109)
Country Fixed Effects	✓	✓	✓	✓
Year Fixed Effects	✓	✓	✓	✓
Control Variables	✓	✓	✓	✓
Observations	1,322	1,322	1,322	1,322
	Democracies *Dependent variable:*			
	Internet Filtering	**Internet Shutdowns**	**Social Media Monitoring**	**Arrests for Political Content**
Treatment Threshold 1				
Transfer ≥ $250,000	0.140**	–0.117	0.205*	–0.093
	(0.059)	(0.108)	(0.110)	(0.152)
Treatment Threshold 2				
Transfer ≥ $500,000	0.124*	–0.118	0.186	–0.149
	(0.064)	(0.122)	(0.115)	(0.165)
Treatment Threshold 3				
Transfer ≥ $1,000,000	0.077	–0.125	0.203	–0.180
	(0.052)	(0.135)	(0.135)	(0.176)
Treatment Threshold 4				
Transfer ≥ $5,000,000	0.100*	–0.100	0.228	–0.207
	(0.052)	(0.155)	(0.151)	(0.203)
Treatment Threshold 5				
Transfer ≥ $10,000,000	0.092*	–0.131	0.241	–0.248
	(0.056)	(0.168)	(0.156)	(0.217)
Country Fixed Effects	✓	✓	✓	✓
Year Fixed Effects	✓	✓	✓	✓
Control Variables	✓	✓	✓	✓
Observations	2,163	2,163	2,163	2,163

Note: *p<0.1; **p<0.05; ***p<0.01

To interpret the substantive magnitude of the results, we can compare the magnitude of the effect to the average difference, for each variable, between autocracies and democracies. The mean value of V-Dem's internet filtering variable for autocracies is 0.94, which is almost precisely the value for Uganda in 2021. Recall that Ugandan President Yoweri Museveni's digital surveillance apparatus – buttressed by Huawei transfers – figured prominently in Sections 2 and 3. The mean internet filtering value for democracies is –1.28, which corresponds almost precisely to prominent Western democracies: Canada, France, Germany, Italy, Spain, and the United States. The results in Models 1 through 3 suggest that Huawei transfers generate an increase in internet filtering, internet shutdowns, and social media monitoring that amounts to between 20% and 25% of the difference in means between autocracies and democracies. Huawei transfers increase arrests for online content by about 10% of the difference.

These treatment effects are averaged across post-treatment periods, and so obscure variation over time. Figures 3, 4, 5, and 6 visualize the estimated ATT by period for the four outcome variables. For each, the estimated ATT for autocracies appears at left; the estimated ATT for democracies appears at right. The shaded areas represent 95% confidence intervals. The *x*-axes give years pre- and post-treatment; the *y*-axes report the averaged coefficient across countries for a given period. As expected, after implementing the GSC estimator, the average actual outcomes and the average predicted outcomes match well in the pre-treatment periods and diverge after Huawei technology transfers. Notwithstanding some oscillations, the treatment effects for autocracies are generally stable or slightly increase over time, after an initial period of one to two years. This reflects the possibility of a phase-in, as we observed in Section 4.1. As a result of this phase-in, the effects of Huawei transfers 10 years after the start date are generally larger than the averaged estimates in table 2. From figure 3, internet filtering increases by nearly 25% of the difference in means between autocracies and democracies. Internet shutdowns increase by about 35%. Social media monitoring increases by nearly 20%. Arrests for online content increase by about 11%.

The results for democracies appear in the bottom panel of table 2. Again, this bottom panel reports the estimates of 20 regression models, each with a different treatment threshold and outcome measure. We find no clear or consistent evidence of adverse effects of Huawei transfers in democracies. Columns 2 and 4 suggest that Huawei transfers to democracies are associated with modest reductions in internet shutdowns and arrests for online content, while Columns 1 and 3 suggest that internet filtering and social media monitoring may increase slightly. For all models, the substantive effects are minimal, equivalent to just 3% of the difference in means between autocracies and democracies.

4.4 Robustness Checks

The Online Appendix includes a series of robustness checks. First, we employ two alternative approaches to regime classification. In Sections 3 and 4, we classified regime types using the V-Dem Polyarchy index. Following Kasuya and Mori (2019), we defined the cutpoint between autocracy and democracy as 0.42. In the Online Appendix, we show that the results are substantively unchanged with cutpoints of 0.33, 0.5, and 0.6, as well as a Polity score of 0. We also employ Boix, Miller and Rosato (2007)'s regime classification, a dichotomous coding of democracy based on contestation (free and fair elections) and participation (a suffrage threshold). Again, the results are substantively unchanged.

Second, we employ two alternative estimation strategies. Although we view OLS and staggered differences-in-differences as less suited than the GSC method to the characteristics of Huawei transfers, we confirm that the results are broadly similar. Following Baker, Larcker and Wang (2022), we implement the staggered DiD estimator with heterogeneous treatment effects in three steps.

Figure 3
Internet filtering

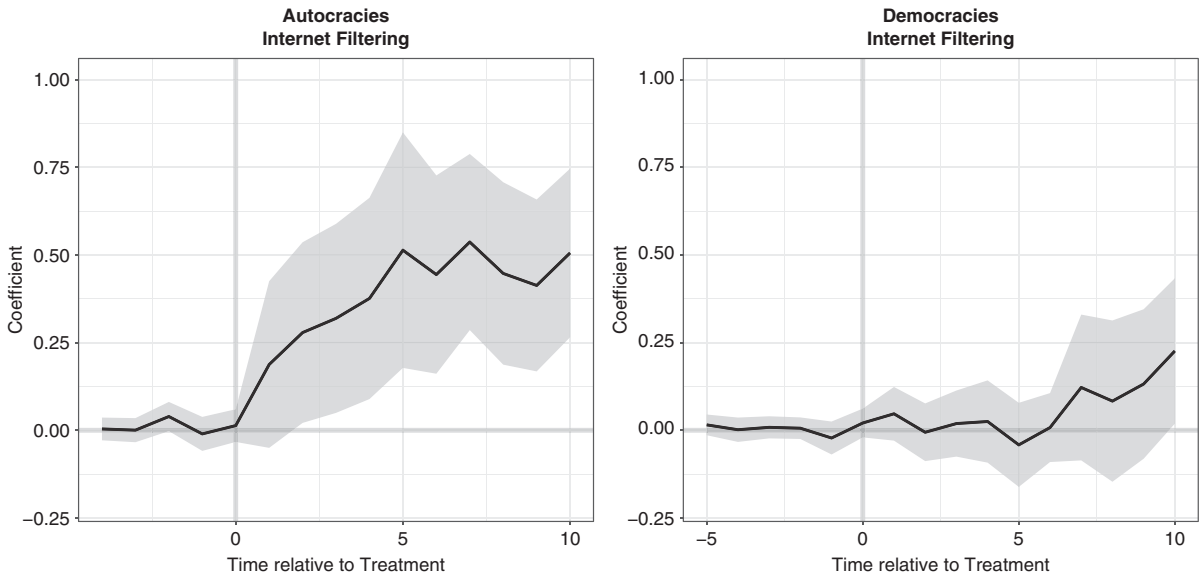


Figure 4
Social media monitoring

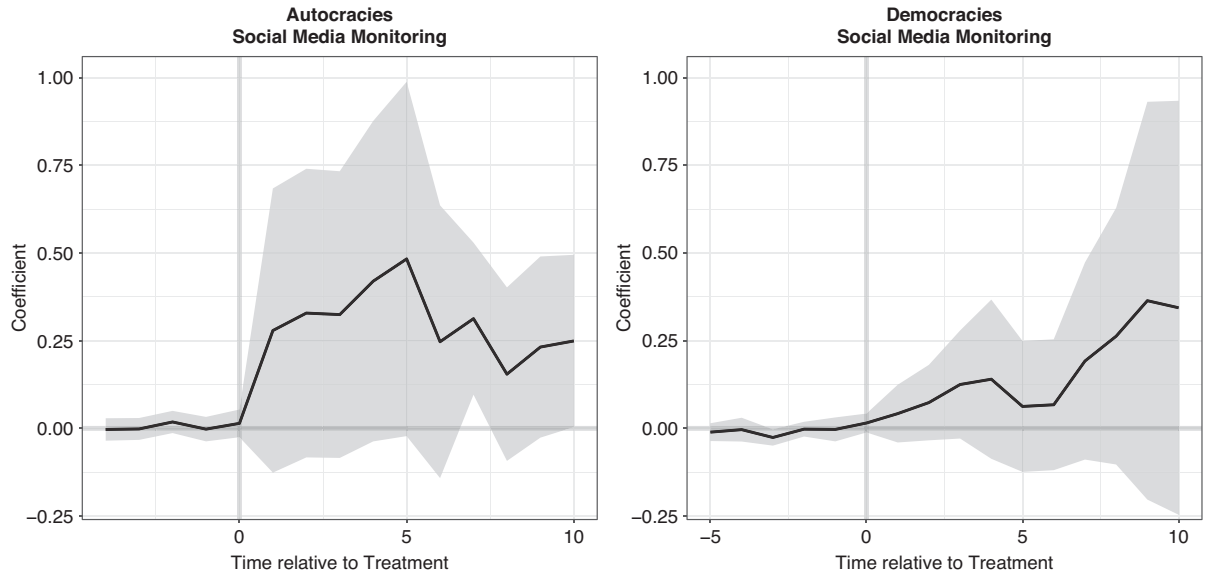
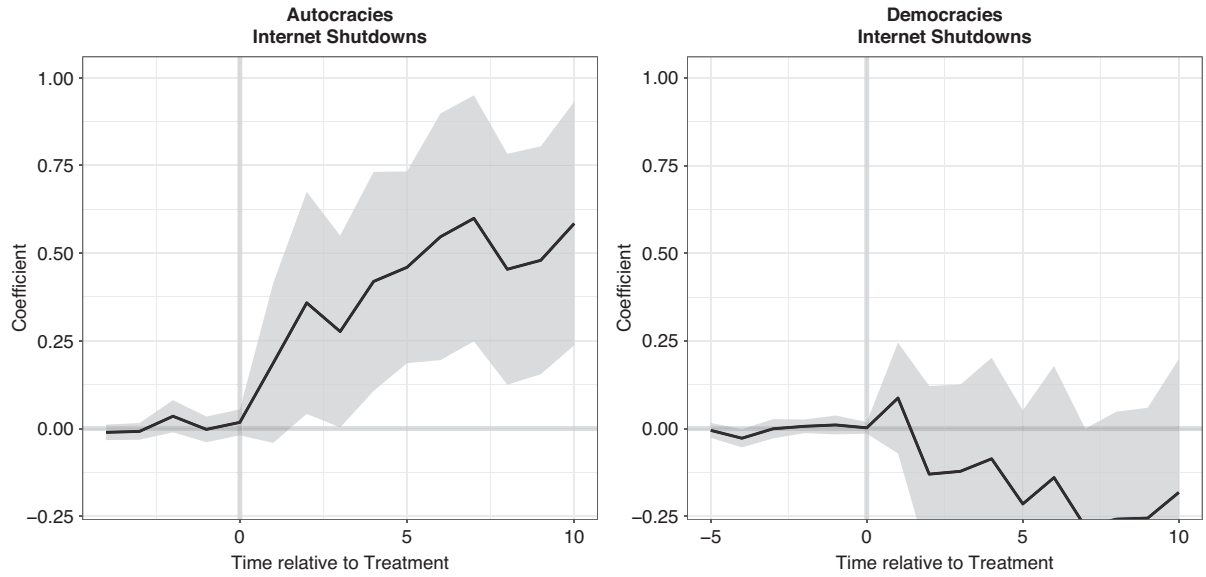


Figure 5
Internet shutdowns

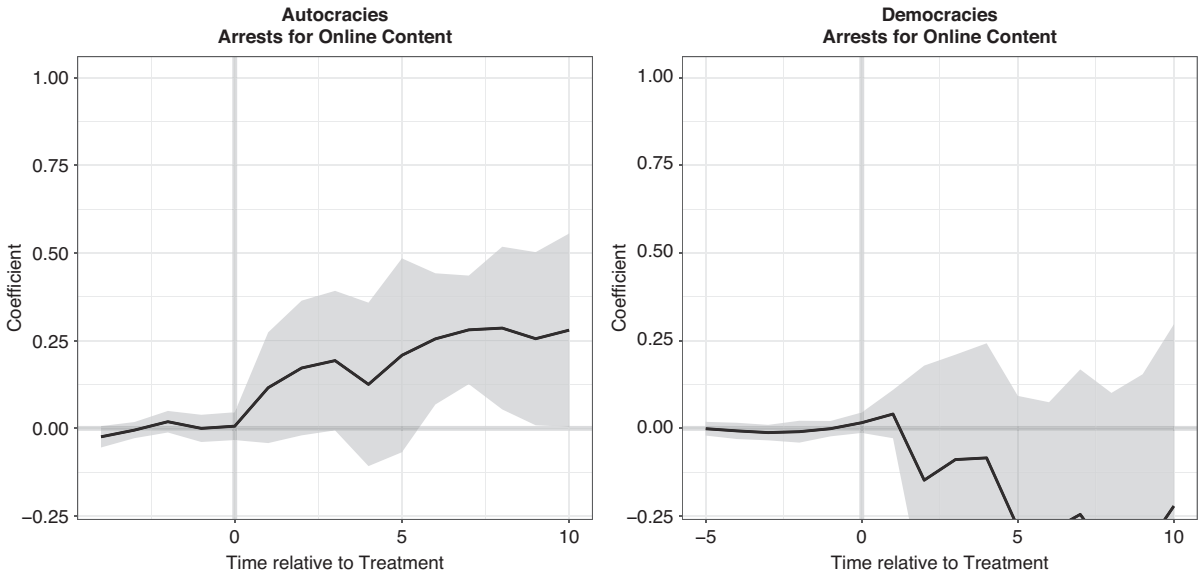


We begin by estimating a variant of the standard staggered DiD estimator with treatment effects for each country:

$$Y_{it} = \alpha + \beta_i(\text{Treated}_{it}) + \delta X_{it} + \gamma_i + \gamma_t + \epsilon \qquad (3)$$

where i indexes country, t indexes year, X_{it} is a vector of time- and country-variant controls, γ_i gives country fixed effects, and γ_t gives year fixed effects. The explanatory variable of interest, $Treated_{it}$, equals 1 if country i received Huawei transfers greater than some threshold T during year t or in some year since. Again, we let this threshold T vary: from a commitment of just $250,000 in year t to transfers of $500,000, $1 million, $5 million, and $10 million in year t. The subscript i on β_i makes clear that

Figure 6
Arrests for online content



equation (3) estimates a treatment effect for each treated country. Next, we construct a contrast matrix that counts the number of periods during which each country in the treatment group is treated. This lets us estimate the cumulative treatment effect of Huawei transfers. Last, we use this estimated cumulative effect to calculate the average treatment effect per country, per period. We then use these per country, per period average treatment effects to compute aggregate average treatment effects.

Third, notwithstanding the journalistic accounts in Section 2, readers may be concerned that there is nothing distinctive about Huawei technology transfers: that the general expansion of digital infrastructure induces digital repression. To be clear, we regard this as unlikely. Pan (2017), for instance, finds that Beijing's censorship capabilities are heavily driven by its ability to pressure domestic firms to remove content. The social media landscape in most autocracies is dominated by Western firms, which typically refuse government censorship and surveillance requests. Still, to ensure this general infrastructure effect is not driving the results in table 2, we identified three measures of digital infrastructure provision from the World Bank's World Development Indicators with the same temporal scope as our sample: internet penetration, broadband subscriptions, and fixed telephone subscriptions. We find no evidence that these general measures of digital infrastructure have an effect on digital repression, which suggests that Huawei transfers are indeed distinctive.

Fourth, readers may be concerned that V-Dem's measures of digital repression are based on expert codings, rather than direct behavior. If expert coders observe a substantial Chinese presence in country i and year t, then perhaps they assume digital repression has increased as well. To check for this, we probe whether other forms of Chinese transfers – including development aid, weapons, and overseas official finance – have similar effects on digital repression. All are drawn from AidData's global dataset over the same time span (Custer et al. 2021). We find no evidence of this, which suggests that expert coders do not observe a substantial Chinese presence in country i in year t and assume an increase in digital repression. We also confirm that our results are robust to using a different set of outcome variables: the Freedom House Freedom on the Net data, which measures obstacles to access, limits on content, violations of user rights, as well as an overall digital freedom score by country. Freedom House codes a smaller sample of countries over a shorter time span, which reduces the size of our autocracy and democracy samples. Although this forces us to shorten the pre-treatment matching period, the results with the Freedom House measures are substantively unchanged. In democracies, Huawei transfers improve digital access and content availability, leading to gains in overall digital freedom country scores. In autocracies, Huawei transfers make obstacles to access and violations of user rights more severe and overall digital freedom country scores worsen.

Fifth, we explore alternative interpretations for our results. One alternative is that democracies, which tend to be wealthier than autocracies, enjoyed better access to surveillance technologies prior to Huawei transfers, and that Huawei's observed effect in autocracies reflects this initial difference in surveillance capacities. We show that

this is unlikely to be the case. Autocracies engaged in far more digital surveillance than democracies before Huawei transfers began in the early 2000s. Another alternative interpretation is that Huawei, by providing coordination technologies, stimulates anti-regime protests, which, in turn, beget repression. We find no evidence that Huawei transfers stimulate protests in democracies or autocracies.

Finally, we employ several robustness checks tailored to the GSC estimator. Our baseline results require treated units to have at least five years of pre-treatment observations, which are used by the GSC estimator to impute counterfactual outcomes. In the Online Appendix, we specify alternative minimum pre-treatment periods: of three years, four years, six years, seven years, and eight years. The results are substantively unchanged for each. We also conduct placebo tests developed by Liu, Wang and Xu (2022) that are appropriate for the matrix completion method. These tests hide some observation periods before the treatment for treated units, and predict the untreated outcomes of the hidden periods with a model trained on the untreated units. There should be no differences between observed and predicted outcomes if the identifying assumptions are valid.[13] This is precisely what we find.

4.5 Extension: Guardrails Against Democratic Backsliding

Although we find no clear or consistent evidence that, on average, Huawei transfers have amplified digital repression in democracies, several democratically-elected governments have used Huawei transfers to erode the institutions that brought them to power (Feldstein 2021). This has been especially well-documented in Zambia, where the security forces under former president Edward Lungu used Huawei technology to intercept encrypted messages sent by local journalists, track their whereabouts, and ultimately secure their arrest (Parkinson, Bariyo and Chin 2019; Woodhams 2019). In Section 2.3.2, we identified several constraints that may prevent democratically-elected governments from using Huawei transfers for digital repression: countervailing political institutions, free and fair elections, independent media, and vibrant civil societies. Ascertaining which of these is most important is beyond the scope of this article, but our data and estimation strategy let us suggest possibilities for future research. We exploit the fact that V-Dem includes measures of the subcomponents of democracy. We then estimate a series of staggered differences-in-differences estimators,[14] each of which includes an interaction term that lets the Huawei effect vary according to a V-Dem subcomponent.

The results, which appear in the Online Appendix, are noteworthy for two reasons. First, three potential guardrails – a vibrant civil society, the rule of law, and a free and independent media – appear to offer protection from digital repression in the world's democracies. When citizens are organized, enjoy access to well-functioning courts, and are kept informed by a free media, democratically-elected governments are less likely to use Huawei transfers for digital repression. Second, across potential guardrails, weakly constrained democracies are more likely to impose internet shutdowns and monitor social media than arrest citizens for online content or filter the internet. Put differently, internet shutdowns and social media monitoring are the most common forms of digital repression where the guardrails against democratic backsliding are relatively weak. This, we believe, makes sense. Social media monitoring is less invasive, less conspicuous than arrests and internet filtering, and so easier for democratically-elected governments to employ. Likewise, the taboo against internet shutdowns seems to be weakening, which may free democratically-elected governments to employ them as well. In 2023, for instance, Access Now documented 283 internet shutdowns across 39 countries, up from 78 shutdowns across 27 countries in 2016.[15] In many years, India, the world's most populous democracy, has been the most frequent offender.

5 Conclusion

The Chinese government has revolutionized digital repression at home and is exporting its technologies abroad. These transfers have sparked widespread concern among observers. These tools of digital dictatorship, many argue, will let recipient governments expand surveillance and reinforce the wave of autocratic retrenchment and democratic erosion currently underway. This article presents the first cross-country, plausibly causal evidence that these concerns are justified, but adds nuance.

Huawei transfers are driven chiefly by demand in recipient countries. More populous countries represent more attractive markets for Huawei, while less affluent countries are more likely to be attracted by its lower price point. Huawei transfers are also more likely if the recipient government has a preexisting relationship with Beijing. The effects of these transfers, we find, depend on political institutions in recipient countries. In autocracies, where the chief political threat to incumbents is collective action by citizens and institutional oversight is weak, Huawei transfers lead to an expansion of digital surveillance, internet shutdowns, internet filtering, and targeted arrests for online content. In democracies, where governments have stronger incentivizes to provide public goods, institutional oversight is stronger, and civil societies are more vibrant, Huawei transfers have no clear or consistent effect on digital repression.

Our empirical analysis has three limitations, which constitute important directions for future research. First, since digital repression is concealed and hence intrinsically difficult to measure, we use the V-Dem project's expert-

coded indices. Although the indices permit broad comparisons across regime types – our results suggest that Huawei transfers generate an increase in digital repression of between 10% and 25% of the difference in means between autocracies and democracies – we are unable to be more specific. Given the rise of digital repression across the world, we view better cross-national data as key. Second, since Huawei is secretive about its contracts, our statistical estimates may be subject to measurement error. Huawei contracts, like other Chinese infrastructure contracts, routinely include confidentiality clauses (Gelpern et al. 2022; Walker 2023), which prohibit recipient governments from divulging information about them. Consequently, our record of Huawei transfers may be incomplete, which would effectively include some treated countries in the control group. Since this would bias against our key results, our statistical estimates should be regarded as lower bounds, with the actual effect potentially larger. Third, Huawei's secrecy means that we also lack fine-grained data about what its transfers entail. Consequently, we cannot ascertain whether certain provisions within contracts are more likely to facilitate digital repression than others. This is almost certainly the case. Transfers that entail "Safe City" infrastructure, for instance, are almost certainly more likely to facilitate digital repression than contracts that focus on IT training for university students. Likewise, Huawei may be inclined to provide some recipient governments more direct personnel support than others, helping them overcome state capacity limitations that might otherwise prevent them from using technology transfers for digital repression. In this article, we use the value of the transfer as a proxy for its substance. This, we believe, makes sense. More expensive contracts are more likely to entail sophisticated telecommunications infrastructure and direct personnel support than less valuable contracts. With more fine-grained contract data, however, policymakers could construct early-warning systems that would identify the transfers most at-risk for human rights violations in recipient countries.

We conclude with three other directions for future research. First, if Huawei transfers facilitate digital repression in autocracies, then they may have other effects. Do they reduce anti-regime protests, coups, or the probability of regime collapse? Insofar as digital repression renders countries less attractive for foreign direct investment, Huawei transfers, over time, may undermine economic growth. Second, although we find no clear and consistent evidence that Huawei transfers have amplified digital repression in democracies, these results should be regarded as preliminary, in part because when the guardrails of democracy are weak, Huawei transfers are associated with several forms of digital repression. Finally, it is also possible that Huawei transfers have had different effects over time, especially in the wake of the BRI's 2013 roll-out, a key part of Xi Jinping's global outreach strategy.

Supplementary material

The supplementary material for this article can be found at http://doi.org/10.1017/S1537592724002226.

Data replication

Data replication sets are available in Harvard Dataverse at: https://doi.org/10.7910/DVN/4URCQT.

Acknowledgments

We thank Ariella Grobman and an anonymous research assistant for invaluable work. For valuable feedback, we also thank seminar participants at Stanford University, the University of Southern California, and the 2023 Annual Meeting of the American Political Science Association.

Notes

1 For more, see Dreher et al. (2022, 122-129).
2 Henceforth, following Feldstein (2021, 67), we refer to this bundle of outcomes as "digital repression."
3 See also Walton (2001).
4 See https://www.statista.com/statistics/1171435/internet-penetration-rate-ghana/ and https://www.internetworldstats.com/unitedstates.htm.
5 We draw data on regime type from Coppedge et al. (2022). Following Kasuya and Mori (2019), we define the cutpoint for autocracy and democracy as 0.42. As we discuss in Section 4.4, the substantive implications are unchanged if we specify a cutpoint of 0.5 or use the Polity scale.
6 In the Online Appendix, we show that the results are virtually indistinguishable after excluding Indonesia, which is the largest single recipient of Huawei transfers in the dataset.
7 For democracies, the control group includes all other democracies that did not receive Huawei transfers during the sample period. For autocracies, the control group includes all other autocracies that did not receive Huawei transfers during the sample period.
8 We employ the MC method because it uses information from the treatment group in the pre-treatment period.
9 V-Dem's variables are appealing for their temporal scope, but, as Huawei establishes a longer record of global engagement, future research should also exploit more direct measures of internet shutdowns, which have sharply expanded since 2016 (Access Now, 2024).
10 In practice, this entails flipping the sign on the V-Dem variables.
11 We use ICEWS rather than other datasets because of its global coverage dating from the late 1990s.

12 For more, see Xu (2017, 58).
13 For more, see Liu, Wang and Xu (2022, 3-4, 18-20).
14 We use a staggered differences-in-differences estimator since the GSC estimator does not accommodate interaction effects.
15 For more, see https://www.accessnow.org/campaign/keepiton/.

References

Access Now. 2024. "Shutdown Tracker Optimization Project (STOP)." https://www.accessnow.org/guide/shutdown-tracker-optimization-project/.

Acemoglu, Daron and James A. Robinson. 2019. *The Narrow Corridor: States, Societies, and the Fate of Liberty*. New York: Penguin.

Adeniran, Adedeji and Sone Osakwe. 2021. "Why Digitalization and Digital Governance Are Key to Regional Integration in Africa." Washington, D.C.: Center for Global Development.

Adeyemi, Daniel. 2021. "The dawn of Ghana's tech ecosystem: Here's what you should know." *TechCabal* July 30.

Allen-Ebrahimian, Bethany. 2016. "The Man Who Nailed Jello to the Wall." *Foreign Policy* June 29.

Alvarado, Oscar Mario Jiménez, Johanna Rodríguez López Fernando Martínez de Lemos and Tessa Weal. 2022. "Amid rising digital repression, Costa Rica serves as a model for Central America—and the world at large." Washington, D.C.: Freedom House.

Andersen, Ross. 2020. "The Panopticon is Already Here." *The Atlantic* September.

Arrieta, Esteban. 2021. "Imagen de Carlos Alvarado llega a su punto más bajo en cuatro años y ahora un 72% tiene una opinión negativa de su gestión." *La Republica* November 24.

Athey, Susan, Mohsen Bayati, Nikolay Doudchenko, Guido Imbens and Khashayar Khosravi. 2021. "Matrix Completion Methods for Causal Panel Data Models." *Journal of the American Statistical Association* 116(536): 1716–1730.

Baker, Andrew C., David F. Larcker and Charles C.Y. Wang. 2022. "How much should we trust staggered difference-in-differences estimates?" *Journal of Financial Economics* 144(2):370–395.

Barma, Naazneen, Brent Durbin and Andrea Kendall-Taylor. 2020. "Digital Authoritarianism: Finding Our Way Out of the Darkness." *War on the Rocks* February 10.

Beraja, Martin, Andrew Kao, David Y. Yang and Noam Yuchtman. 2023a. "AI-tocracy." *Quarterly Journal of Economics* Forthcoming.

——. 2023b. "Exporting the Surveillance State via Trade in AI."

Berwick, Angus. 2018. "How ZTE helps Venezuela create China-style social control." *Reuters* November 14.

Boix, Carles, Michael Miller and Sebastian Rosato. 2007. "A Complete Data Set of Political Regimes, 1800-2007." *Comparative Political Studies* 46(12): 1523–1554.

Boschee, Elizabeth, Jennifer Lautenschlager, Sean O'Brien, Steve Shellman, James Starz and Michael Ward. 2015. "ICEWS Coded Event Data." Harvard Dataverse, V29, https://doi.org/10.7910/DVN/28075.

Brautigam, Deborah. 2009. *The Dragon's Gift: The Real Story of China in Africa*. New York: Oxford University Press.

Brazys, Samuel and Krishna Chaitanya Vadlamannati. 2021. "Aid Curse with Chinese Characteristics? Chinese Development Flows and Economic Reforms." *Public Choice* 188:407–430.

Carter, Brett L. 2024. *Inside Dictatorship: Social Cleavages and Institutional Constraints in the Republic of Congo.* Unpublished Manuscript.

Carter, Erin Baggott and Brett L. Carter. 2023. *Propaganda in Autocracies: Institutions, Information, and the Politics of Belief*. New York: Cambridge University Press.

——. 2024. "Replication Data for: Exporting the Tools of Dictatorship: The Politics of China's Technology Transfers." *Harvard Dataverse*, https://doi.org/10.7910/DVN/4URCQT.

Cave, Danielle, Fergus Ryan and Vicky Xiuzhong Xu. 2019. "Mapping more of China's tech giants: AI and surveillance." Sydney: Australian Strategic Policy Institute.

Cave, Danielle, Samantha Hoffman, Alex Joske, Fergus Ryan and Elise Thomas. 2019. "Mapping China's Technology Giants." Sydney: Australian Strategic Policy Institute.

Chan, Keith. 2018. "China's hotel facial recognition check-ins and AI smart rooms are here to stay." *South China Morning Post* August 6.

Chen, Celia and Meng Jing. 2019. "What you need to know about Meiya Pico, China's low-profile forensics champion named in data privacy scandal." *South China Morning Post* July 9.

Chen, Celia, Meng Jing and Sarah Dai. 2018. "Facial recognition to ticketing apps: how tech is helping ease the Lunar New Year travel crush." *South China Morning Post* January 27.

Cheng, Rita. 2020. "Chinese Police Target Muslim Minorities Using Digital Forensics: Researcher." *Radio Free Asia* October 16.

Chin, Josh and Liza Lin. 2017. "China's All-Seeing Surveillance State Is Reading Its Citizens' Faces." *The Wall Street Journal* June 26.

——. 2022. *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. New York: St. Martin's Press.

China News. 2008. "[image]." http://www.chinanews.com/hb/news/2008/12-04/1473209.shtml.
Christensen, Darin and Francisco Garfias. 2018. "Can You Hear Me Now? How Communication Technology Affects Protest and Repression." *Quarterly Journal of Political Science* 13(1):89–117.
Coppedge, Michael, John Gerring, Staffan I. Lindberg, Svend-Erik Skaaning, Jan Teorell, David Altman, Frida Andersson, Michael Bernhard, M. Steven Fish, Adam Glynn, Allen Hicken, Carl Henrik Knutsen, Kyle L. Marquardt, Kelly McMann, Valeriya Mechkova, Pamela Paxton, Daniel Pemstein, Laura Saxer, Brigitte Seim, Rachel Sigman and Jeffrey Staton. 2022. "Varieties of Democracy (V-Dem) Project." Available at https://www.v-dem.net/en/.
Cordoba, Javier. 2020. "Costa Rica presidency rocked by data collection scandal." *Associated Press* March 4.
Custer, Samantha, Dreher, Thai-Binh Elston, Andreas Fuchs, Siddharta Ghose, Joyce Jiahui Lin, Ammar A. Malik, Bradley C. Parks, Brooke Russell, Kyra Solomon, Austin Strange, Michael J. Tierney, Katherine Walsh, Lincoln Zaleski and Sheng Zhang. 2021. "*Tracking Chinese Development Finance: An Application of AidData's TUFF 2.0 Methodology*." Williamsburg: AidData at William & Mary.
Dai, Sarah. 2018. "Beijing's new Zaha Hadid-designed airport to showcase latest facial recognition technology." *South China Morning Post* July 18.
de Vergès, Marie. 2020. "Charlette N'Guessan, une pionnière de la reconnaissance faciale en Afrique." *Le Monde* December 18.
Deng, Yanhua and Kevin J. O'Brien. 2013. "Relational Repression in China: Using Social Ties to Demobilize Protesters." *The China Quarterly* 215: 533–552.
Diamond, Larry. 2010. "Liberation Technology." *Journal of Democracy* 21(3):69–83.
——. 2022. "Democracy's Arc: From Resurgent to Imperiled." *Journal of Democracy* 33(1):163–179.
Dou, Eva. 2021. "Documents link Huawei to China's surveillance programs." *The Washington Post* December 14.
Dreher, Axel, Andreas Fuchs, Bradley Parks, Austin Strange and Michael J. Tierney. 2022. *Banking on Beijing: The Aims and Impacts of China's Overseas Development Program*. New York: Cambridge University Press.
Earp, Madeline. 2021. "How China's Huawei technology is being used to censor news halfway across the world." Washington, D.C.: Committee to Protect Journalists.
El Kadi, Tine Hinane. 2022. "How Huawei's Localization in North Africa Delivered Mixed Returns." Washington, D.C.: Carnegie Endowment for International Peace.
Feldstein, Steven. 2019. "The Global Expansion of AI Surveillance." Washington, D.C.: Carnegie Endowment for International Peace.
——. 2020. "When It Comes to Digital Authoritarianism, China is a Challenge – But Not the Only Challenge." *War on the Rocks* February 12.
——. 2021. *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. New York: Oxford University Press.
Frantz, Erica, Andrea Kendall-Taylor and Joseph Wright. 2020. "Digital Repression in Autocracies." *V-Dem Institute Working Paper* March.
Gallagher, Mary E. and Blake Miller. 2019. "Who Not What: The Logic of China's Information Control Strategy." *The China Quarterly* 248(1):1011–1036.
Gehring, Kai, Lennart Kaplan and Melvin H.L. Wong. 2019. "China and the World Bank: How Contrasting Development Approaches Affect the Stability of African States." *Journal of Development Economics* 158:102902.
Gelpern, Anna, Sebastian Horn, Scott Morris, Bradley C. Parks and Christoph Trebesch. 2022. "How China Lends: A Rare Look Into 100 Debt Contracts with Foreign Governments." *Economic Policy* November.
Gohdes, Anita R. 2015. "Pulling the Plug: Network Disruptions and Violence in Civil Conflict." *Journal of Peace Research* 52(3):352–367.
—— 2020. "Repression Technology: Internet Accessibility and State Violence." *American Journal of Political Science* 64(3):488–503.
—— 2024. *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*. New York: Oxford University Press.
Guild, James. 2021. "Reappraising the Economic Legacy of Susilo Bambang Yudhoyono." *The Diplomat* September 28.
Gunitsky, Seva. 2017. *Aftershocks: Great Powers and Domestic Reforms in the Twentieth Century*. Princeton: Princeton University Press.
Harwell, Drew and Eva Dou. 2020. "Huawei tested AI software that could recognize Uighur minorities and alert police, report says." *The Washington Post* December 8.
Hernandez, Diego. 2016. "Are "New" Donors Challenging World Bank Conditionality?" *World Development* 96:529–549.
Herscovitch, Benjamin, Dirk van der Kley and Gatra Priyandita. 2022. "Why Indonesia Has Embraced Huawei." *Foreign Policy* July 28.
Hersey, Frank. 2017. "China to have 626 million surveillance cameras within 3 years." *TechNode* November 22.
Hillman, Jonathan E. 2021. *The Digital Silk Road: China's Quest to Wire the World and Win the Future*. New York: Harper Business.

Hvistendahl, Mara. 2020. "How a Chinese AI Giant Made Chatting—and Surveillance—Easy." *Wired* May 18.
Isaksson, Ann-Sofie and Andreas Kotsadam. 2018. "Chinese Aid and Local Corruption." *Journal of Public Economics* 159:146–159.
Kafeero, Stephen. 2020. "Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests." *Quartz* November 27.
Kasuya, Yuko and Kota Mori. 2019. "Better Regime Cutoffs for Continuous Democracy Measures." *V-Dem Institute Working Paper #25* October:1–31.
King, Gary, Jennifer Pan and Margaret E. Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107(2):326–343.
Kurlantzick, Joshua. 2021. "Yudhoyono and Wikileaks." Washington, D.C.: Council on Foreign Relations.
Lardy, Nicholas R. 2012. *Sustaining China's Economic Growth After the Global Financial Crisis*. Washington, D.C.: Peterson Institute for International Economics.
Levitsky, Steven and Lucan A. Way. 2010. *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. New York: Cambridge University Press.
Li Tao. 2018. "Jaywalkers under surveillance in Shenzhen soon to be punished via text messages." *South China Morning Post* March 27.
Liu, Licheng, Ye Wang and Yiqing Xu. 2022. "A Practical Guide to Counterfactual Estimators for Causal Inference with Time-Series Cross-Sectional Data." https://ssrn.com/abstract=3555463.
Maizland, Lindsay and Andrew Chatzky. 2020. "Huawei: China's Controversial Tech Giant." New York: Council on Foreign Relations.
Manacorda, Marco and Andrea Tesei. 2016. "Liberation Technology: Mobile Phones and Political Mobilization in Africa." *Econometrica* 88(2):533–567.
Marinov, Nikolay and Hein Goemans. 2014. "Coups and Democracy." *British Journal of Political Science* 44(4): 799–825.
Mattingly, Daniel C. 2020. *The Art of Political Control in China*. New York: Cambridge University Press.
Mayiga, John Bosco. 2010. "*Parliament Passes Law to Intercept Communications Following Uganda Attacks*." Kampala: African Centre for Media Excellence.
Miller, Michael K. 2021. *Shock to the System: Coups, Elections, and War on the Road to Democratization*. Princeton: Princeton University Press.
Mozur, Paul, Jonah M. Kessel and Melissa Chan. 2019. "Made in China, Exported to the World: The Surveillance State." *The New York Times* April 24.
Muhumuza, Rodney. 2022. "New law in Uganda imposes restrictions on use of internet." *ABC News* October 13.
Ong, Lynette H. 2022. *Outsourcing Repression: Everyday State Power in Contemporary China*. Oxford: Oxford University Press.
Pan, Jennifer. 2017. "How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship." *Problems of Post-Communism* 64 (3-4):167–188.
Parkinson, Joe, Nicholas Bariyo and Josh Chin. 2019. "Huawei Technicians Helped African Governments Spy on Political Opponents." *The Wall Street Journal* August 15.
Polyakova, Alina and Chris Meserole. 2019. "Exporting Digital Authoritarianism: The Russian and Chinese Models." Washington, D.C.: Brookings Institution.
Powell, Jonathan M. and Clayton L. Thyne. 2011. "Global Instances of Coups from 1950 to 2010: A New Dataset." *Journal of Peace Research* 48(2): 249–259.
Priyandita, Gatra, Dirk van der Kley and Benjamin Herscovitch. 2022. "Localization and China's Tech Success in Indonesia." Washington, D.C.: Carnegie Endowment for International Peace.
Qiang, Xiao. 2019. "The Road to Digital Unfreedom: President Xi's Surveillance State." *Journal of Democracy* 30(1):53–67.
Restore Data Rights. 2022. "Transparency in South Africa." Cape Town: Available at https://restoredatarights.africa/resources/transparency-in-south-africa/.
Russell, Jon. 2017. "China's CCTV surveillance network took just 7 minutes to capture BBC reporter." *TechCrunch* December 13.
Shahbaz, Adrian. 2018. "The Rise of Digital Authoritarianism." Washington, D.C.: Freedom House.
Slotta, Daniel. 2024. "Market Share of 5G Equipment in China in 2023, By Provider." https://www.statista.com/statistics/1194757/china-market-share-of-5g-base-stations-by-manufacturer.
The Washington Post. 2020. "China is exporting its digital authoritarianism." August 5.
Tiffert, Glenn and Oliver McPherson-Smith. 2022. "China's Sharp Power in Africa: A Handbook for Building National Resilience." Stanford: Hoover Institution, Stanford University.
Unwanted Witness. 2015. "Digital Rights and Internet Freedoms in Uganda: A Policy Analysis." Kampala: .
U.S. Senate Committee on Foreign Relations. 2020. "The New Big Brother – China and Digital Authoritarianism." Washington, D.C.: .
Walker, Christopher. 2023. "How China Exports Secrecy: Beijing's Global Assault on Transparency and Open Government." *Foreign Affairs* July 11.
Wallace, Jeremy L. 2014. *Cities and Stability: Urbanization, Redistribution, and Regime Survival in China*. New York: Oxford University Press.
Walton, Greg. 2001. *China's Golden Shield: Corprations and the Development of Surveillance Technology in the People's Republic of China*. Montreal: Rights & Democracy.

Weber, Valentin and Vasilis Ververis. 2021. "*China's Surveillance State: A Global Project*." London: Top10VPN.

Wise, Carol. 2020. *Dragonomics How Latin America Is Maximizing (or Missing Out on) China's International Development Strategy*. New Haven: Yale University Press.

Woodhams, Samuel. 2019. "Huawei, Africa and the global reach of surveillance technology." *Deutsche Welle* September 12.

Woodhams, Samuel and Christine O'Donnell. 2021. "*The Tech Companies Behind Internet Shutdowns: Allot Ltd*." London: Top10VPN.

Xu, Xu. 2021. "To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance." *American Journal of Political Science* 65(2):309–325.

Xu, Yiqing. 2017. "Generalized Synthetic Control Method: Causal Inference with Interactive Fixed Effects Models." *Political Analysis* 25:57–76.

Yang, Yingzhi. 2018. "Shanghai airport first to launch automated clearance system using facial recognition technology." *South China Morning Post* October 15.

Yu, Yongding. 2010. "China's Policy Responses to the Global Financial Crisis." *East Asia Forum* January 24.