K4D | Knowledge, evidence and learning for development

Export Of Digital Surveillance Technologies from China To Developing Countries

Jacqueline Hicks
Institute of Development Studies
1 August 2022

Questions

What data is available on the levels and sources of financing from China to developing countries for the purchase of digital surveillance technologies?

Is there evidence that digital surveillance technologies bought from Chinese companies contribute to authoritarian control in developing countries?

Contents

1. Summary
2. Wider Chinese investment context
3. Chinese ICT infrastructure projects
4. Chinese smart city projects
5. Financing of smart city and ICT projects
6. Push-pull factors of technology purchases
7. Contribution to authoritarian control

1. Summary

In short, there is evidence to show that Chinese companies, with some state credit backing, are selling digital surveillance technologies to developing countries, which are then sometimes used in authoritarian practices. However, there is little direct evidence to show that surveillance technologies sold by Chinese companies have more authoritarian potential than the technologies sold by non-Chinese companies.

Q1 - data available on the spread and financing of surveillance technologies in developing countries.

Some researchers define "surveillance technologies" as including any form of **digital infrastructure**. There is data to show that developing country governments are contracting Chinese companies to build digital infrastructures, such as mobile phone networks, fibre optic cables, satellites, or data centres. Two studies on Africa show that the Chinese entities most involved in such projects are EXIM bank, Huawei and ZTE, with an estimated total loan value in Africa of around US$7-9 billion.

Other researchers define "surveillance technologies" as **smart city projects**. It is estimated that in 2019, Chinese smart city technologies have been purchased in over 100 countries worldwide. Other researchers look at more **specific elements of smart cities**: There are estimates that the "AI surveillance" components of smart cities have been purchased in 47-65 countries worldwide, and the "data integration" security platforms in at least 80 countries. Financing data on smart cities was not found, although there are some estimates of credit extended to purchasers by one Chinese firm Huawei. These estimates range from US$3 - 30 billion.

None of these figures imply anything about how these technologies are used. The **"dual use"** nature of these technologies means that they can have both legitimate civilian and public safety uses as well as authoritarian control uses.

Q2 - evidence of these technologies contributing to authoritarian control in developing countries.

There is evidence of some governments in Africa using Chinese surveillance technologies to **spy on political opponents and arrest protesters**. There is also evidence of **training provided by Chinese companies** related to smart city surveillance technologies, but little detail about what it covers. Some authors say that some Chinese smart city projects are actually not very effective, but still provide governments with a **"security aesthetic" - the appearance of control**. Research also shows that Chinese **smart city technologies have been sold mostly to illiberal regimes**.

However, **in the wider context**, there is also ample evidence of non-Chinese surveillance technologies contributing to authoritarian control in developing countries, including being used to spy on political opponents and protesters. There is also evidence that UK companies sell surveillance technologies to mostly illiberal regimes.

Some reports consulted for this rapid review **imply** that Chinese surveillance technologies are more likely to be used for authoritarian control than those sold by non-Chinese companies. This analysis is largely based on **circumstantial rather than direct evidence.** They rely on prior

judgements about the following issues, which are themselves subject to ongoing enquiry in the literature:

- **The nature of the Chinese tech companies:** particularly related to the expertise gained by involvement in the well-documented human rights violations of the Uyghur population, in addition to the levels of political influence within the companies.
- **The nature of overseas Chinese investment which emphasises the sovereignty of the nations they invest in**. This means that the current nascent European efforts to regulate the export of surveillance technologies may be unlikely to be replicated by China.
- **The relatively generous nature of Chinese financing** which may enable more developing countries (some with authoritarian tendencies) to buy surveillance technologies than would otherwise be the case.

Almost all of the reports consulted for this rapid review say that **the most important factor determining whether governments in developing countries will deploy a particular technology for repressive purposes is the quality of governance in the country**. No reports were found in the literature reviewed of Chinese state pressure on developing countries to adopt surveillance technologies, and there were some anecdotal reports of officials in developing countries saying they did not come under any pressure to buy from Chinese companies. Analyses to explain adoption range from the availability of cheap credit, to the allure of vanity projects. Most say it is a **complex mix of factors** depending on local context.

State of the evidence: There are several reasons why it is difficult to draw firm conclusions on this topic:

1. **The definition of surveillance technologies:** The studies found during the course of this rapid review define “surveillance technologies” differently. Definitions range from large scale digital infrastructures such as mobile phone networks, to automatic analyses of data using artificial intelligence (AI), to the use of smart city platforms which integrate the data collected with other government databases. Some of these describe hardware, and some of them data management processes, and they all overlap to some degree.
2. **The data:** It became apparent during the course of this rapid review that re-citations of figures with no clear origin is common in media and even academic writing. Particular care was therefore made to clarify the provenance of the data found. In general, the data on both smart cities and digital infrastructures are approximate for the reasons set out in more detail in the following sections.
3. **The definition of evidence:** Different authors have different conceptions of what constitutes evidence. For example, authors and readers may or may not consider the existence of Chinese state documents on “information sovereignty” to be evidence that the Chinese state is pursuing a grand international strategy of digital authoritarianism. Similarly, some may decide that examples of Chinese tech companies working with Chinese government departments means that they are implementing a grand strategy overseas. While the authors with the most experience of this topic say that the reality is much more complicated, judgements about the nature of evidence can be politicised.

A different strand of research looks at the influence of the Chinese government on privacy regulations and internet standards around the world, which is beyond the scope of this review.

2. Wider investment and financing context of Chinese companies in developing countries.

The 'Digital Silk Road.'

The "Digital Silk Road" (DSR) was introduced in 2015 by an official Chinese government white paper as a component of Beijing's Belt and Road Initiative (BRI). Greene and Triolo (2020) describe it as more of a brand for virtually any telecommunications or data-related product sales by China-based tech firms than a coherent, top-down policy.

Greene and Triolo (2020) note that Chinese tech firms were building telecommunications infrastructure all over the world well before the DSR policy was announced. They say that more recently, as global tech investment is increasingly framed in geopolitical terms, there are signs that the Chinese central government is exercising more influence over Chinese tech firms, and a more joined up policy on internet standards as well as foreign tech investment.

The DSR is part of the "Belt and Road Initiative" (BRI). Considered the centrepiece of the Chinese leader's Xi Jinping's foreign policy, the BRI is essentially a policy of infrastructure investments in around 70 countries (including many developing countries) along the historical land and sea trading routes Westward. According to a 2015 Chinese government white paper, the BRI has three components: transport infrastructure, energy infrastructure, and ICT infrastructure. A further policy document articulates a need for "bilateral cross-border optical cable networks at a quicker pace, plan transcontinental submarine optical cable projects, and improve spatial (satellite) information passageways to expand information exchanges and cooperation" (State Council, 2015 in Tugendhat and Voo, 2021).

The mixture of state and private financing and policy objectives.

BRI policy characterises the Chinese government as a "partner" rather than a "donor" in its economic engagement with developing countries, emphasising a "win-win" cooperation of "mutual benefit" (State Council, 2011 in Wang, 2013). In practice, this "mutual benefit" means that **Chinese infrastructure financing in developing countries encompasses a mixture of grants, concessional loans and market-rate loans** – sometimes all within one project. It also means that the majority of its projects require the use of Chinese companies and experts (Bräutigam, 2011).

This can be distinguished from **overseas foreign direct investment** (OFDI) by Chinese companies. In general, many of the Chinese companies investing overseas are state-owned enterprises (Kamal et al., 2019), although it has been noted by some scholars that state control over investment decisions through the National Development and Reform Commission (NDRC) has relaxed in recent years (Chalmers and Mocker, 2017). Other ostensibly private Chinese companies have access to relatively large amounts of credit from the domestic state banks, such as the China Development Bank, for their domestic and foreign operations.

In China, **most private companies have a Chinese Communist Party (CCP) Committee embedded within them**. Official Chinese Chamber of Commerce figures show that 92.4% of the country's top 500 private enterprises have CCP committees in them, and 48.3% of all private firms (Thomas, 2020).

The degree of control by the CCP in private firms generally is a matter of debate, and unlikely to be uniform (Thomas, 2020). As tech firm activities have become implicated in geopolitics and gained significance in the domestic market, there are **indications that the CCP is seeking more influence over these private companies.** This goes beyond embedding CCP committees to include anti-monopoly legislation and the public castigation of the country's most visible tech billionaire, Jack Ma (Carr and Liu, 2021).

3. Data on Chinese ICT infrastructure projects.

Some authors characterise any kind of Chinese ICT infrastructure to be a form of surveillance technology. Chinese companies have been involved in developing basic telecommunications and internet infrastructure by laying undersea cables and rolling out broadband in countries where such infrastructure is either underdeveloped or non-existent.

One of most well-publicised issues of recent years has been with Chinese company **sales of 5G** - the fifth generation of cellular network technology and the basis for other technological advances, including Smart Cities and the Internet of Things. It was concerns about the security implications of Chinese-made 5G networks that instigated a backlash against Huawei particularly in some European countries and the US. In this case, the concerns were related to state espionage and potential coercion if leaked data is used to blackmail political elites in those states (Bartholomew, 2020; Taylor, 2019; Kurlantzick and West, 2020).

Other types of digital infrastructure hardware, like China's BeiDou navigation **satellite network**, are also sometimes implicated as a surveillance technology (Hillman, 2021, Chapter Six).

Datasets on Chinese ICT projects.

There are some large datasets that include the funding and spread of Chinese-made ICT technologies, but the data is not definitive.

The Chinese government or banks do not systematically release data on the loans they offer to individual overseas borrowers (Acker and Brautigam, 2021, p.2). In that absence, such **data is collected by research teams at various university institutes** and think tanks, mostly based in the US. It is a mammoth, ongoing task, and **some data sources are better than others.**

The better resourced AidData and CARI (China Africa Research Initiative) flag when data is "vague" and distinguish between MOUs, loan commitments and actual implementation. Both datasets are based on media reports, publicly available Chinese government documents, contractor websites, fieldwork, and interviews.

The China section of **AidData** contains records across all sectors for 13,427 projects worth US$843 billion covering 165 countries from 2000 to 2017. It allows for searches of different phases of project implementation including official loan commitments, projects in implementation, completion and those cancelled.

The **China Africa Research Initiative (CARI)** contains 1,141 signed loan commitments worth US$153 billion with African governments between 2000 and 2019. "Loan commitments" are the formal signing of a loan contract after an MOU, but do not represent actual disbursements.

Researchers from the initiative say that it is rare that loan commitments do not go ahead once signed (Acker and Brautigam, 2021).

The **Australian Strategic Policy Institute (ASPI)** database on Chinese tech giants' overseas operations is more accurately described as a collection of summaries of media reports and other documents ranging from reports of MOUs to actual deals. It contains thousands of entries on 24 Chinese tech companies, an associated interactive map and analysis in reports.

The **Center for American Progress** dataset provides information "of all 'iron triangle' deals involving Huawei, Chinese state banks, and buyers outside China" (Hart and Link, 2020, p.10). It states that it builds on the above databases, China-Africa Research Initiative, AidData (Hart and Link, 2020, p.32), but strips the entries of any of the metadata provided by these institutes, so that it is difficult to judge what they represent.

A few random cross-checks were made on these data sources during the course of this rapid review with some discrepancies. For example, in the report associated with the ASPI database (Cave et al., 2019, p.11) a cited newspaper report about a US$500 million loan ***facility*** from the Chinese government to a Zimbabwean telco becomes in the text an actual ***loan*** of US$500 million. The same deal is recorded in AidData as US$300 million loan that is still in the pipeline.

There will always be inevitable discrepancies in such a large, ongoing task, but they are important to recognise when **tables of figures, or interactive maps offer the reader the illusion of definitive data.**

Chinese ICT projects in Africa.

This rapid review found two research papers which **aggregate data on Chinese ICT projects in Africa**, including some estimates about financing. They both show that Huawei and ZTE have the most involvement in these types of projects. One of the studies puts Chinese **"loan commitments" to African countries at US$8,947 million** (2000-2014) (Tugendhadt and Voo, 2021), the other study puts "ICT aid projects" at US$7.13 billion for Africa over the same period (Wang, 2020). Both say that most loans and credit comes via EXIM bank.

Using the CARI database, Tugendhat and Voo (2021) extracted a subset of loans related to the construction of digital infrastructure, including satellites, fibre networks, data centres, video surveillance, and e-government projects.

Some headline findings are:

- Authors identified **90 Chinese "tech infrastructure" loans between 2000 and 2019**. Of these loans, 74 were taken out by African government ministries and 16 by private companies or state-owned enterprises (SOEs) in Africa.

Figure One: Chinese Technology Infrastructure Loans by Country (US$ Millions, 2000-14)

This Graph has been removed for copyright reasons. It can be viewed at https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/610844c1b59c8123f42a0c3e/1627931842061/PB+60+-+Tugendhat+and+Voo+-+China+Digital+Silk+Road+Africa.pdf

Source: Tugendhat and Voo, 2021, p.16.

The main sources of finance for these loans were: China's EXIM Bank, Huawei, and ZTE, with roughly **55 percent of lending coming from China's EXIM Bank**.

Figure Two: Chinese Loans by Financier (2000-18)

This Graph has been removed for copyright reasons. It can be viewed at https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/610844c1b59c8123f42a0c3e/1627931842061/PB+60+-+Tugendhat+and+Voo+-+China+Digital+Silk+Road+Africa.pdf

Source: Tugendhat and Voo, 2021, p.14.

Huawei was the largest contractor involved in Chinese financed technology projects in Africa both by number of loans and by value of loans.

Wang (2020) extracted "ICT aid projects" from 2000-2014 in Africa from the AidData database, resulting in a dataset of 173 projects.

Some of the findings on spread and financing of these projects include:

- **African countries with the highest number of projects**: Zimbabwe (n = 18), Nigeria (n= 12), Zambia (n = 9), Tanzania (n = 9), and Ghana (n = 9).
- The **five countries that received the highest aid amount** (in U.S. dollars) were Nigeria (US$1.65 billion), Zimbabwe (US$822.2 million), Ethiopia (US$822 million, with one project), Tanzania (US$688 million), and Côte d'Ivoire (US$402 million, with two projects) (Wang, 2020, p.1504).

Note the difference between these figures and those cited above in Figure One by Tugendhat and Voo, 2021 which lists the top five countries as: Ethiopia, Nigeria, Angola,Tanzania, and Cote d'Ivoire for the same period.

Wang (2020) further notes:

- Huawei (n = 34) and ZTE (n = 23) were the **top two implementing agencies**.
- The **top three funding agencies** were EXIM (40 projects), Huawei (37 projects), and ZTE (26 projects).
- A total of **125 agencies from 44 countries** participated in ICT aid projects. Of those, 57% were SOEs (n = 71), 22% were private companies (n = 28), and 21% were government agencies (n = 26).

4. Data on Chinese smart city projects.

Other scholars focus more specifically on "smart cities" to determine the use of surveillance technologies.

"Smart cities" is the loosely defined category given to projects which employ a number of different technologies to collect and share previously unavailable or unconnected datasets about

various municipal operations, such as traffic patterns or for public safety (Atha et al., 2020). It can refer to an entire urban ecosystem employing smart cities principles or to the constituent technologies and applications that make up that ecosystem. There is no standard list of "smart city" technologies and applications, and **no comprehensive database quantifying Chinese smart city projects abroad** (Atha et al., 2020).

Smart Cities as a general category.

In a well-referenced report prepared for the U.S.-China Economic and Security Review Commission (an independent agency of the United States government), Atha et al. (2020) quantify Chinese exports of smart city technologies overseas. They define "smart cities projects" as "any **instances** of exported technologies, **agreements** to install systems or equipment, or **collaborations on implementation** of smart city-enabling technologies abroad" (p.56).

Researchers first compiled a list of the 65 most prominent Chinese firms selling smart cities technologies and systems, then searched the official websites of each of the 65 companies on for reports of smart cities projects in other countries.

They found **398 reported cases of 34 different Chinese firms exporting smart cities technologies in 106 countries**. The geographic distribution of these projects is presented in Figure Three below:

Figure Three: Globally Identified Chinese Smart Cities Projects

This figure has been removed for copyright reasons. It can be viewed at
https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf

Source: Atha et al., 2020, p.59.

The technologies represented by these findings include surveillance cameras, 5G infrastructure, data centers, mobile payment applications, smart energy meters, parking and traffic management, and integrated control platforms such as emergency response systems and call centers (Atha et al., 2020, p.61).

Different types of smart city collaboration for developing and developed nations:
Examining five case studies, the authors note that in the three developing nations (Malaysia, Ecuador, and Kenya), collaboration with China is more likely to be around "unified security management" projects, while in one developed nation case (United Kingdom) partnerships with Chinese companies were more aimed at ICT infrastructure, security cameras, and municipal services such as smart traffic, streetlamps and waste management. However, in Germany, Chinese companies have been involved in projects to implement integrated smart city platforms.

The authors say that dozens of Chinese companies are involved with smart cities projects globally, but that **Hikvision (cameras) and Huawei appear as the largest exporters** of relevant products and services. Although they do add that Huawei may be relatively over-represented in their dataset as they provide the most publicly available information on their smart city projects compared to other Chinese companies.

This report does not attempt to quantify the financing for these smart city projects,

“AI surveillance” component of smart cities.

One study details the global use of “AI surveillance,” including smart city, facial recognition, and smart policing.

Feldstein (2019) developed a global index of “AI surveillance” which includes technologies related to smart city, facial recognition, and smart policing, but excludes “enabling technologies” such as 5G or data centers. Only smart city platforms with a clear public safety focus are included, as opposed to, for example smart street lighting. AI facial recognition refers to cameras which match stored or live footage of individuals with databases, or assess aggregate demographic trends. Smart policing involves data-driven analysis that can be used to make predictions about crime.

The index is built on the content analysis of news articles, websites, corporate documents, academic articles, NGO reports, expert submissions, and other public sources between 2017 and 2019. **It does not distinguish between legitimate and unlawful uses of AI surveillance**, nor differentiate between countries in terms of intensity of use.

Headline findings:

- In 2019, at least seventy-five out of 176 countries globally are actively using AI technologies for surveillance purposes. This includes: smart city/safe city platforms (fifty-six countries), facial recognition systems (sixty-four countries), and smart policing (fifty-two countries). It found that **forty-seven countries out of 65 countries studied are deploying AI surveillance technology from China.**
- **Technology linked to Chinese companies**—particularly Huawei, Hikvision, Dahua, and ZTE—supply AI surveillance technology **in sixty-three countries**.
- **Huawei** alone is responsible for providing AI surveillance technology to at least fifty countries worldwide. The author says that “**No other company comes close”**, but notes that Huawei may have an incentive to highlight its surveillance capabilities compared to other companies.

As a global study, the report also includes data on **AI surveillance technology supplied by U.S. and European firms overseas.** It finds that such technology is present in thirty-two countries. The most significant U.S. companies are IBM (eleven countries), Palantir (nine countries), and Cisco (six countries).

Figure Four: AI Surveillance Technology Origin

This figure has been removed for copyright reasons. It can be viewed at
https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Source: Feldstein, 2019, p.3.

The report **does not attempt to quantify the financing available for AI surveillance technologies**. It nevertheless notes that “Chinese product pitches are often accompanied by soft loans to encourage governments to purchase their equipment. These tactics are particularly relevant in countries like Kenya, Laos, Mongolia, Uganda, and Uzbekistan—which otherwise might not access this technology. This raises troubling questions about the extent to which the Chinese government is subsidizing the purchase of advanced repressive technology” (p.2).

Platform components of smart cities.

Another study also collates data on the overseas adoption of “Chinese surveillance and public security technology platforms.”

Greitens (2020) compiled a new dataset on the adoption of “Chinese surveillance and public security technology platforms.” By focusing on “platforms”, she distinguishes her data from other studies that may include technologies like Chinese-made closed-circuit television (CCTV) cameras. By contrast, she collects information on the presence of “a data integration and analytics platform that supports one or more high-tech command-and-control centers. The platform collects, integrates, and analyzes data from a wide range of sources, such as criminal records, other government databases, networked surveillance cameras, facial and license plate recognition applications, and other sources” (p.3).

She notes that these projects are often multi-layered, with one company providing the core platform, with additional (Chinese and Western) companies involved in other aspects, extensions, or subcomponents of the project. In addition, project contracts sometimes include technical consulting in addition to sales of platforms themselves.

She derives her data from a search of “corporate, government, and media reporting” in various languages, without elaborating further on her methods.

The report’s **headline finding** on the spread of Chinese **surveillance and public security technology platforms** is that they have been **adopted in at least 80 countries since 2008**.

Reviewing the figures from other reports, Greitens (2020) cites Huawei’s 2018 annual report as claiming its smart city (branded “Safe City”) technologies are in more than 100 countries worldwide - much more than is cited in reports from the Australian Strategic Policy Institute (43 countries) and the Center for Strategic and International Studies (52 countries). She concludes that “because **Huawei and other Chinese tech companies have incentives to emphasize or exaggerate the popularity of their technology for marketing purposes**, the true number of global adoptions likely falls somewhere between these two sets of estimates” (Greitens, 2020, p.2)

The report does not attempt to quantify any financing arrangements.

5. Data on financing of Chinese ICT projects and smart cities.

In the absence of financing data on Chinese exports of smart city technologies, one report documents loans linked to Huawei’s general ICT projects overseas.

The Centre for American Progress collated a dataset of international "loan-backed projects" involving Huawei (Hart and Link, 2020). As already detailed above, this dataset relies on a number of other databases including CARI and Aiddata. It is not clear which of the data below represents MOUs, signed deals or loan commitments.

It found 99 loan-backed projects across 46 nations, from 1997 to 2019 with a total value of just under US$14.8 billion.

The study breaks down the figures geographically as:

- **Africa**: 57 loans totalling US$4.661 billion, all loans went to government borrowers and state-owned enterprises.
- **Europe**: 14 loans totalling US$4.379 billion. Only one loan involved a government borrower (Serbia); the other 13 loans went to private companies.
- **Asia**: 15 loans, total lending volume of US$2.209 billion, six loans went to government borrowers and nine went to private companies.
- **South America**: Three loans totalling US$1.4 billion to private companies in Brazil.
- **North America**: US$1.375 billion to privately owned telecom operators in Mexico.
- **Middle East**: Three loans to governments and private companies totalling US$375.4 million.
- **Oceania**: US$378.49 million in loans to governments.

The report further states that the **China Development Bank** has provided Huawei with US$30 billion in global lines of credit: US$10 billion in 2004 and an additional US$20 billion in 2009 (Zhao, 2009, cited in Hart and Link, 2020).

The authors note that a senior Huawei manager contests this figure, and say it only extended US$2.99 billion of the available US$30 billion to its customers (Palmer, 2011, cited in Hart and Link, 2020). The authors further note that this was contradicted by Huawei's vice chairman of Huawei USA, who claimed that approximately US$10 billion of the credit lines had been used (Hu, 2011, cited in Hart and Link, 2020).

Comparison of Chinese and non-Chinese ICT financing.

Most of the reports seen during the course of this rapid review highlight the role of Chinese state-supported financing in accounting for the spread of Chinese surveillance technologies, particularly in the case of Huawei (see Gallagher, 2022, p. 9-10 for discussion).

On the broader question of Chinese state-supported financing for ICT infrastructure deals overseas, some analysts make the point that companies like Huawei share some financing practices with other international ICT companies.

For example, **on the practice of "vendor-financed loans"**, where telecom companies provide financing to their customers to buy their products, one industry insider notes:

> "For decades now, winning wireless infrastructure business has been all about financing the customers. In the early days of the cellular industry in the U.S., when newly licensed operators were just getting started, a common deal offered by a system supplier would

> have included all the equipment for the network, at zero upfront cost to the buyer, plus a generous dollop of additional "working capital" to help the operator get up and running. (I remember deals that came with "150% financing" – that is, the operator got the whole network installed "for free" plus 50% of the value in cash to set up the business. To be paid back over time, as the operator's own cash flow developed.)…Huawei is following the industry game plan (Calhoun, 2020).

On **export credit and other assistance** for telco companies, including Nokia and Ericsson:

> "Official data show Swedish export authorities provided some US$10 billion in credit assistance for Sweden's tech-and-telecom sector as of 2018; Finland authorized US$30 billion in annual export credit guarantees economy wide from 2017. Huawei's largest American competitor, Cisco Systems Inc., received US$44.5 million in state and federal subsidies, loans, guarantees, grants and other U.S. assistance since 2000 (Yap, 2019)."

It is common practice for all countries to support the export capacities of their domestic industries, however, these are regulated through international trade norms and practices.

For example, most countries use export credit agencies (trade financing to domestic companies to facilitate international exports). However, there is "gentlemen's agreement" at the OECD to help ensure that "buyers make purchasing decisions based solely on the quality or price of goods or services, rather than the export credit support on offer" (Thompson, 2020).

Tied aid (concessional loans to developing countries in exchange for agreement to use a particular company) is being phased out by OECD countries but it is not yet complete (OECD, 2020).

There are anti-subsidy and anti-dumping rules at the WTO (Stojanovic, 2020).

Some potential repercussions of Chinese financing providing cheap credit for digital and surveillance technologies found in the literature include:

- It may trigger a "race to the bottom" in terms of other countries seeking to do the same, further indebting developing countries (Klein, 2021).
- It may prove "fiscally unsustainable for China's government in the long run" (Atha et. al, 2020, p.79).
- Huawei equipment may have more "vulnerabilities" because the company relies on competitive financing to make sales rather than technological superiority (Calhoun, 2020).

6. Why do developing countries buy surveillance technologies from China?

The research found for this rapid review tends to describe surveillance technology adoption in developing countries in terms of push and pull factors.

Push factors

Some reports note the "push" factors, including **Chinese strategic interests, cheap finance, and "aggressive marketing".**

Reviewing some of the literature, Greitens (2020) identifies some parts of reports that emphasise the "push" factors behind the adoption of Chinese surveillance technologies:

> "Critics in the United States and elsewhere tend to see Chinese geopolitical strategy and authoritarian instincts at work: a supply-side or 'push factor' explanation. As one recent report phrased it, 'China is a major driver of AI surveillance worldwide' (Feldstein, 2019, p.1). The report notes that over half of the countries in which it found Chinese-sourced AI technology were signatories to President Xi Jinping's flagship geopolitical project, the Belt and Road Initiative (BRI), and suggests that Chinese government loans may be used to subsidize countries' acquisition of repressive technologies (Feldstein, 2019, p.2). Another report notes that Beijing views information technology not just in terms of economic development but 'its value to Chinese foreign policy and strategy… exporting its information technology is not only about securing important new sources of revenue and data, but also generating greater strategic leverage vis-à-vis the West.' (Polyakova and Meserole, 2019). **In this view, the global adoption of these platforms is China-driven, as Beijing pushes their use for its own geopolitical strategic objectives**" (p.5).

Based on official Chinese documents, Atha et al. (2020) is just one of many reports which recognise that **Chinese policymakers see the construction of smart cities as providing a "strategic opportunity" for Chinese firms to expand abroad**.

In some of the literature, **Chinese firms are described as engaging in "aggressive marketing**", but without referring to evidence. For example: "states like China aggressively market the transfer of advanced AI technology around the globe" (Crosston, 2020, p.149); "the aggressiveness of Chinese companies to penetrate African markets" (Feldstein, 2019, p.8); "Chinese firms aggressively market their products and are present in the African market in ways that many US and European firms are not" (Feldstein, 2020a, p.3).

If these authors are referring to public marketing and advertising campaigns in different countries, this could be a fruitful future area of research to collect evidence.

Pull factors

There is some anecdotal evidence that **state officials in developing countries are not pressured by China to adopt these technologies.**

Feldstein (2019) states: "At least in Thailand, recent research interviews did not turn up indications that Chinese companies are pushing a concerted agenda to peddle advanced AI surveillance equipment or encourage the government to build sophisticated monitoring systems.

An official from Thailand's Ministry of Interior noted that while AI technology is "out there" and something the government is thinking more about, 'China hasn't offered any AI. It doesn't give AI—Thais have to ask.'" (p.15).

Noting that it is often regional or municipal officials in recipient countries that make purchasing decisions, Greitens (2020) cites some newspaper articles where public officials in various countries explain their adoption of "Safe Cities" technology. One example from Myanmar:

> "We want to guarantee the rule of law and security for the city. So, we will launch the 'Safe City' plan. There will be stability only when there is rule of law and security. Only then will investors come to us," regional Chief Minister Dr. Zaw Myint Maung said at the Mandalay Economic Forum in March" (Pho, 2019).

A case study of Ethiopia finds that:

> "The focus in Western media on China's export of surveillance technology to Ethiopia attributes most of the agency to Chinese firms and the Chinese state. However, this study has found that **the Ethiopian government has the agency to independently choose what technology it acquires and from where**. By cooperating with China as well as Europe to develop its own space technology, the Ethiopian government safeguards its negotiation position and capacity to act independently" (Van der Lugt, 2021).

None of the research found during the course of this rapid review cited any instances of officials from developing countries reporting that they came under any pressure to buy Chinese equipment.

One author describes the "allure" of surveillance technology as a vote-winner for elected officials in developing countries.

In the judgement of Hillman (2021), elected officials may adopt Chinese smart city technologies as a kind of vanity project. He describes a hypothetical situation of an elected official:

> "The command center they show you looks like NASA's mission control, something available only to the world's richest countries. Rows of workstations are arranged in concentric arcs. All face a towering wall with giant screens. Maps appear to show the locations of vehicles, the identities of people, and a variety of alerts…The local media would beg for a tour. They would write stories about leapfrogging to the forefront of innovation and the prosperous future that a smarter city offers. The outside world would have to take notice. Foreign investors would see greater opportunity and less risk…To sweeten the deal, China's state banks will provide a subsidized loan that is repayable over twenty years. By that point, the city should be transformed. The project will pay for itself. Even if it does not, you will have moved on, so it will be someone else's problem" (Chapter Four).

Some authors judge the drivers of adoption to be a complex mixture of push and pull factors unique to each location.

Greitens (2020, p.1) says: "the drivers of this trend are complex, stemming from expansion of China's geopolitical interests, increasing market power of its technology companies, and conditions in recipient states that make Chinese technology an attractive choice despite security and privacy concerns."

She further notes that: “Countries with high crime rates are comparatively more likely to adopt these technologies — but so are countries that are strategically important to the PRC [People's Republic of China]” Greitens (2020, p.1).

Evidence of a coherent strategy: Feldstein (2020b) states **there is no evidence of a grand strategy**: “On balance, there are limited signs that China is pursuing a grand strategy to systematically proliferate digital authoritarian tools. Rather, **China’s efforts vary by country, local context, and its own interests**.”

Hillman (2021) cites the study by Atha et al. (2020) to argue that:

> “Coordination challenges are even greater overseas, where Chinese companies operate with less oversight and foreign governments have their own priorities. China’s government elevates issues but does not usually provide detailed marching orders. Through the Belt and Road, for example, Xi has called for building “smart cities,” an expansive term for enhancing urban areas with digital infrastructure. But the Chinese government does not appear to have provided even top-level guidance to companies pursuing these projects abroad, according to a study by James Mulvenon, a leading expert on Chinese technology, and his colleagues for the U.S.-China Economic and Security Review Commission” (Chapter One).

However, citing some media reports, Cave et al. (2020) imply a strategic approach by the CCP stating: “The CCP has made no secret of its desire to export its concepts of internet and information ‘sovereignty’, as well as cyber censorship, around the world” (p. 4).

7. Is there evidence that Chinese digital surveillance technologies contribute to authoritarian control in developing countries?

Different studies use different approaches to find answers to this question.

There is evidence of governments using Chinese surveillance technologies to spy on political opponents and arrest protesters.

In Myanmar, leaked government budget documents showed detailed information on surveillance technology purchases. The *New York Times* reported that “the documents catalog tens of millions of dollars earmarked for technology that can mine phones and computers, as well as track people’s live locations and listen in to their conversations” (Beech, 2021). The organisation that received the documents, Justice for Myanmar, lists some of the companies involved, including some from China in addition to other countries (Justice for Myanmar, 2021).

The Ugandan police are reported to have used Huawei cameras to help track down protesters (Kafeero, 2020).

Feldstein (2019) cites a report by the *Wall Street Journal* (Parkinson et al., 2019) that “**Huawei technicians in both Uganda and Zambia helped government officials spy on political opponents**. This included ‘intercepting their encrypted communications and social media, and

using cell data to track their whereabouts.' Not only did Huawei employees play a 'direct role in government efforts to intercept the private communications of opponents,' but they also encouraged Ugandan security officials to travel to Algeria so they could study Huawei's 'intelligent video surveillance system' operating in Algiers" (p.14).

In an appendix to his book on the subject, Feldstein (2021, p. 306) lists "**Commercial Spyware Used by Governments against Domestic Opponents**" in 64 countries. It includes two instances of Huawei spyware in Uganda and Zambia, and many more from other commercial firms not based in China.

There is particular suspicion about the training provided by Chinese companies in how to use the technologies purchased.

Weber (2019) highlights the role of a Chinese cybersecurity company called Meiya Pico, drawing data from it's website about trainings the company has provided in Egypt, Malaysia, Thailand and others. Meiya Pico was linked to a spy app used by police in China to extract data from citizens' smartphones during random street checks and received a good deal of attention in the US (Chen, 2019). Weber says that the company was "instructed by the Chinese Ministry of Public Security to train countries affiliated with the BRI in digital forensics" (p.18). This is based on a reference to the Ministry in a downloaded image of the BRI from the Meiya Pico website (Image 3, p.19).

In a widely cited 2018 report, Freedom House (2018) says "Chinese officials have held trainings and seminars on new media or information management with representatives from 36 out of the 65 countries covered in this survey. While it is not always clear what transpires during such seminars, a training for Vietnamese officials in April 2017 was followed in 2018 by the introduction of a cybersecurity law that closely mimics China's own law. Increased activity by Chinese companies and officials in Africa similarly preceded the passage of restrictive cybercrime and media laws in Uganda and Tanzania over the past year."

The report is based on a 21-question survey administered to over 70 analysts from 65 countries (www.freedomonthenet.org).

Using a carefully thought-out method, one case study of Ethiopia finds that Chinese ICT contributes to the government's control over its citizens.

The question guiding the study (Van der Lugt, 2021) is: To what extent does Chinese information and communications technology (ICT) contribute to the Ethiopian government's control over its citizens?

The study breaks down the causal pathway from Chinese ICT to authoritarian control in Ethiopia into thirteen different propositions before searching for evidence. For example, the propositions include: The Ethiopian government requests surveillance tools from China; Chinese firms provide the Ethiopian government with access to data collected via their technology; The Ethiopian government adopts a cybersecurity law that mimics the Chinese cybersecurity law.

Evidence is sought from media, academic, government, and company reports with additional data from interviews with personal contacts in in China and on the African continent.

Overall, the study finds that the combination of the fact that the Ethiopian government classifies as an authoritarian regime, has access to surveillance tools, and can legally search and seize personal data at any time, leads to the fact that the Ethiopian government strengthened its control over its citizens.

Other findings include:

- **The main Chinese actor involved in the digitization of Ethiopia does not seem to be the Chinese Communist Party (CCP) or the central state, but commercial and state-owned enterprises**. This does not preclude state influence, but points to the complexity of the reality on the ground.
- The Chinese company **ZTE appears to offer more ways for the Ethiopian government to monitor the users of its network than either Huawei or the European companies** Ericsson and Nokia. However, with the software provided by European companies such as FinTech and Hacking Team, the Ethiopian government can collect similar information to that which it collects with the ZTE software ZSmart. This means that **the outcome would not be so different if the Ethiopian government did not use Chinese ICT and instead made use of other foreign ICT**.
- Chinese firms have the means and contacts to advise the Ethiopian government on a master plan for ICT is another potential example of the increased use of Chinese ICT technology in Ethiopia.

Sales of surveillance technologies to illiberal regimes.

Some research shows a predominance of illiberal regimes placing orders for Huawei's smart city technologies.

The *Financial Times* cites research from RWR Advisory which cannot be publicly accessed so its methods are unclear. The study finds that "out of 64 countries that have signed up to install the safe and smart city technology of Chinese companies, 41 were ranked as 'not free' or 'partly free' by Freedom House, a US non-governmental organisation. The remaining 23 were in countries classified as 'free'" (Kynge et al., 2021). The article reproduces a graph from the RWR Advisory research:

Figure Five: Chinese Smart City Sales by Regime Type

This graph has been removed for copyright reasons. The full graph can be viewed at: https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

Source: Kynge, 2021.

Hillman and McCalpin (2019, p.1) use a similar methodology, stating that "**Seventy-one percent of Huawei's "Safe City" agreements are in countries with an average rating of "partly free" (44 percent) or "not free" (27 percent)** by Freedom House between 2009-2018."

However, by comparison, other research shows a similar pattern of UK exports of "internet surveillance equipment" to illiberal regimes. In a submission to the British

parliament, Privacy International undertook research on the licenses approved by the UK for the export of two types of surveillance technology: (1) internet surveillance equipment which allows an authority to intercept internet traffic on a mass scale (2) equipment which monitors mobile and satellite phones in a given area indiscriminately (Privacy International, 2019).

The submission states that:

> "Out of these 284 license applications made between 2015 and September 2018 for these two technologies, only nine have been rejected because of a risk of use for internal repression. Only 21% of the destinations for these exports are considered "Free" by Freedom House's 2018 global report on political rights and civil liberties; 44% are considered "Partly Free", while 35% of all approved licences of surveillance equipment are to destinations considered "Not Free".

The aesthetics of surveillance technologies.

Two authors say that Chinese smart city technologies have actually proven to be less effective than claimed, but may still **contribute to authoritarian control by providing governments an appearance of control.**

Hillman (2021) states:

> "**Advocates trumpet massive gains in efficiency and safety. Critics warn that these systems make the government omnipresent**. While they disagree on the ultimate objective of China's digital infrastructure projects, **both sides of this debate tend to assume the technology works.** A closer look suggests that China's "Safe City" exports have a more mixed track record. Eager to win business, companies have been willing to stretch the truth" (Chapter Four).

As evidence, the author cites a report comparing Huawei's crime-reduction claims about Safe City systems in Pakistan and Kenya, and the subsequent rises in crime in those areas. A Pakistan legislative committee reported that half of the cameras were out of order in one Pakistan Safe City project in Islamabad (Prasso, 2018).

Gagliardone (2022) makes the same point, citing a different newspaper report (Hao, 2019).

Hillman (2021) argues that safe city technologies like street cameras can be perfect for governments wanting to appear technologically advanced and in control, providing a **"security aesthetic —the appearance of control."**

> "After the sale is made, both sides are incentivized to portray the product as a success. Pointing out that the systems do not work as promised will expose the government to criticism that it squandered public money and did not do its job effectively. Many countries are also reluctant to risk jeopardizing their relationship with the Chinese government, a major lender and trading partner. Consequently, governments may spend less time rigorously evaluating whether these projects work than publicly portraying them as successful" (Chapter Four).

Local context.

Two authors emphasise that research on the consequences of Chinese tech purchases by developing countries should focus on local context.

Greitens (2020) says: “the question du jour of whether China is ‘exporting digital authoritarianism’…is less a matter of divining Beijing’s intent in providing the technology to others, and more an empirical question of the scale and direction of its impact in different political environments” (Greitens, 2020, p.6).

Another influential expert adds that “The most important factor determining whether governments will deploy this technology for repressive purposes is the quality of their governance” (Feldstein, 2019, p.2).

8.References

Acker, K. and Brautigam, D. (2021). *Twenty years of data on China’s Africa lending*, https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/605cb1891cb0ff5747b12167/1616687497984/BP+4+-+Acker%2C+Brautigam+-+20+Years+of+Data+on+African+Lending.pdf

Atha, K., Callahan, J., Chen, J., Drun, J., Green, K., Lafferty, B., ... and Walz, E. (2020). *China's smart cities development*. SOS International LLC. https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf

Bartholomew, C. (2020). China and 5G. *Issues in Science and Technology*, 36(2), 50–57. https://www.jstor.org/stable/26949108

Beech, H. (2021). Myanmar’s military deploys digital arsenal of repression in crackdown. *New York Times*, https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html

Bräutigam, D. (2011). Aid “with Chinese characteristics”: Chinese foreign aid and development finance meet the OECD-DAC aid regime. *Journal of International Development*, 23(5), 752–764. doi:10.1002/jid.1798

Calhoun, G. (2020). How does Huawei acquire customers? It buys them with cheap credit. *Forbes*, https://www.forbes.com/sites/georgecalhoun/2020/06/06/how-does-huawei-acquire-customers-mostly-it-buys-them/?sh=e87b45f46062

Carr, A. and Liu, C. (2021). The China model: What the country’s tech crackdown is really about, *Bloomberg*. https://www.bloomberg.com/news/articles/2021-07-27/china-tech-crackdown-xi-charts-new-model-after-emulating-silicon-valley

Cave, D., Hoffman, S., Joske, A., Ryan, F., and Thomas, E. (2019). *Mapping China's technology giants*. Australian Strategic Policy Institute. https://www.aspi.org.au/report/mapping-chinas-tech-giants.

Chalmers, A., and Mocker, S. (2017). The end of exceptionalism? Explaining Chinese national oil companies' overseas investments. *Review of International Political Economy.* 24 (1): 119-143. doi:10.1080/09692290.2016.1275743

Chen, C. and Jing, M. (2019). What you need to know about Meiya Pico, China's low-profile forensics champion named in data privacy scandal. *South China Morning Post*. https://www.scmp.com/tech/start-ups/article/3017688/what-you-need-know-about-meiya-pico-chinas-low-profile-forensics

Crosston, M. (2020). Cyber colonization: The dangerous fusion of artificial intelligence and authoritarian regimes. *Cyber, Intelligence, and Security Journal*, 4(1), 149-171. https://www.inss.org.il/publication/cyber-colonization-the-dangerous-fusion-of-artificial-intelligence-and-authoritarian-regimes/

Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Feldstein, S. (2020a). *Testimony before the U.S.-China Economic and Security Review Commission - Hearing on China's Strategic Aims in Africa*. https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf

Feldstein, S. (2020b). *When it comes to digital authoritarianism, China is a challenge — but not the only challenge*. https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/

Feldstein, S. (2021). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Oxford Academic. doi:10.1093/oso/9780190057497.001.0001

Freedom House. (2018). *Freedom on the net 2018: The rise of digital authoritarianism*. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Gagliardone, I. (2022). *Beyond the digital cold war: Western, eastern, and southern tales of digital success and failure.* Centre for International Governance Innovation. https://www.cigionline.org/articles/beyond-the-digital-cold-war-western-eastern-and-southern-tales-of-digital-failure-and-success/

Gallagher J. (2022). *U.S. restrictions on Huawei technologies: National security, foreign policy, and economic interests.* Report#: R47012, Congressional Research Service https://crsreports.congress.gov/product/pdf/R/R47012/2

Greene, R., and Triolo, P. (2020). *Will China control the global internet via its Digital Silk Road?* Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

Greitens, S. (2020). *Dealing with demand for China's global surveillance exports*. Brookings Institution Global China Report. https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/

Hao, N. (2019). Huawei 'Safe City' systems are ineffective, crime figures show. *The Epoch Times*. www.theepochtimes.com/huawei-safe-cities-are-ineffective-according-to-crime-figures_3187283.html.

Hart, M., and Link, J. (2020). *There is a solution to the Huawei challenge*. Center for American Progress. https://americanprogress.org/wp-content/uploads/2020/10/Solution-to-Huawei-Challenge-NEW.pdf?_ga=2.103113664.1962015504.1658354988-1987556905.1657631552

Hillman, J. (2021). *The Digital Silk Road: China's Quest to Wire the World and Win the Future*. Profile Books. https://profilebooks.com/work/the-digital-silk-road/

Hillman, J. and McCalpin, M. (2019). *Watching Huawei's Safe Cities.* Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf

Hu, K. (2011). Huawei Open Letter. *The Wall Street Journal*. http://online.wsj.com/public/resources/documents/Huawei20110205.pdf.

Justice For Myanmar. (2021). *Tools of digital repression*. https://www.justiceformyanmar.org/stories/tools-of-digital-repression

Kamal, M., Shah, S., Jing W. and Hasnat, H. (2019). Does the quality of institutions in host countries affect the location choice of Chinese OFDI: Evidence from Asia and Africa. *Emerging Markets Finance and Trade*, 56:1, 208-227. DOI: 10.1080/1540496X.2019.1610876

Kafeero, S. (2020). Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests. *Quartz Africa*. https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-tosnare-protesters/

Klein, J. (2021). Hobbled US Import-Export bank is given new life to battle an aggressive China. *South China Morning Post*. https://www.scmp.com/news/china/article/3121606/hobbled-us-import-export-bank-given-new-life-battle-aggressive-china

Kurlantzick, J., and West, J. (2020). *Assessing China's digital silk road initiative: A transformative approach to technology financing or a danger to freedoms?* Council on Foreign Relations. https://www.cfr.org/china-digital-silk-road/

Kynge, J., Hopkins, V., Warrell, H., and Hille, K. (2021). *Exporting Chinese surveillance: The security risks of 'smart cities'*. *Financial Times*. https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

Lin, L. and Purnell, N. (2019). A world with a billion cameras watching you is just around the corner. *Wall Street Journal*. www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402.

OECD. (2020). *2020 Report on the DAC Recommendation on Untying ODA*. https://one.oecd.org/document/DCD/DAC(2020)54/FINAL/en/pdf

Palmer, D. (2011). Huawei rejects Eximbank chief's China aid claim. *Reuters*. https://www.reuters.com/article/us-usa-china-huawei/huawei-rejects-eximbank-chiefs-china-aid-claim-idUSTRE75F71220110616.

Parkinson, J., Bariyo, N. and Chin, J. (2019). Huawei technicians helped African governments spy on political opponents. *Wall Street Journal*. https://www.wsj.com/articles/huaweitechnicians-helped-african-governments-spy-on-political-opponents-11565793017 .

Pho, M. (2019). Huawei to supply Mandalay's Safe City project with security cameras equipment. *The Irrawaddy*. https://www.irrawaddy.com/news/burma/huawei-supply-mandalays-safe-city-project-cameras-security-equipment.html

Polyakova, A., and Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models*. The Brookings Institution. https://www.brookings.edu/research/exporting-digital-authoritarianism/

Prasso, S. (2019). Huawei's claims that it makes cities safer mostly look like hype. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-11-12/huawei-s-surveillance-network-claims-face-scrutiny#xj4y7vzkg

Privacy International. (2019). *Written evidence submitted by Privacy International*. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/committees-on-arms-export-controls/2017-arms-export-controls-annual-report/written/95815.pdf

State Council. (2011). *White Paper on China's Foreign Aid*. Beijing, China: Xinhua/Information Office of the State Council. http://english.gov.cn/archive/white_paper/2014/09/09/content_281474986284620.htm

State Council. (2015). *Action plan on the Belt and Road Initiative*. http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm

Stojanovic, A. (2020). *WTO anti-subsidy and countervailing measures agreement*. Institute for Government. https://www.instituteforgovernment.org.uk/explainers/world-trade-organization-subsidies

Taylor, E. (2019). *Who's afraid of Huawei? Understanding the 5G security concerns*. Chatham House. https://www.chathamhouse.org/2019/09/whos-afraid-huawei-understanding-5g-security-concerns

Thomas, N. (2020). *Party Committees in the private sector: Rising presence, moderate prevalence*. https://macropolo.org/party-committees-private-sector-china/?rp=m&fbclid=IwAR1bDHDjgNqDp9J8GwNLAbRo3hMHTktQocwJXbUb7Th08Zu0ObJ9bDuctL8

Thompson, F. (2020). US vs China: the battle of the ECAs. *Global Trade Review*. https://www.gtreview.com/magazine/volume-18-issue-4/us-vs-china-battle-ecas/

Tugendhat, H., and Voo, J. (2021). *China's digital silk road in Africa and the future of internet governance*. Policy Brief, No. 60/2021, China Africa Research Initiative (CARI). https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/610844c1b59c8123f42a0c3e/1627931842061/PB+60+-+Tugendhat+and+Voo+-+China+Digital+Silk+Road+Africa.pdf

Van der Lugt, S. (2021). Exploring the Political, Economic, and Social Implications of the Digital Silk Road into East Africa The Case of Ethiopia. In F. Schneider (ed.), *Global Perspectives on China's Belt and Road Initiative: Asserting Agency through Regional Connectivity* (pp. 315-346). Amsterdam University Press. doi:10.2307/j.ctv1dc9k7j.16

Wang, P. (2013). The Chinese view: Reflection of the long-term experiences of aid receiving and giving, in Y. Shimomura and H. Ohashi (eds), *A Study of China's Foreign Aid: An Asian Perspective*, Palgrave Macmillan. doi:10.1057/9781137323774_7

Wang, R., Bar, F., & Hong, Y. (2020). ICT aid flows from China to African countries: A communication network perspective. *International Journal of Communication*, 14, 1498. https://ijoc.org/index.php/ijoc/article/view/9973/3006

Weber, V. (2019). *The worldwide web of Chinese and Russian information controls*. Center for technology and global affairs, University of Oxford. https://www.ctga.ox.ac.uk/article/worldwide-web-chinese-and-russian-information-controls

Yap, C. (2019). State support helped fuel Huawei's global rise. *Wall Street Journal*. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736?mod=searchresults&page=1&pos=20

Zhao, X., and Tao, J. (2009). Guo jia kai fa yin hang yu hua wei qian shu 300 yi mei yuan zhan lue he zuo xie yi [China Development Bank and Huawei sign a USD 30 billion strategic cooperation agreement], *Xinhua News Agency*. http://www.gov.cn/jrzg/2009-09/23/content_1423891.htm.

Suggested citation

Hicks, J. (2022). *Export of digital surveillance technologies from China to developing countries.* K4D Helpdesk Report. Institute of Development Studies. DOI: 10.19088/K4D.2022.123

About this report

This report is based on twelve days of desk-based research. The K4D research helpdesk provides rapid syntheses of a selection of recent relevant literature and international expert thinking in response to specific questions relating to international development. For any enquiries, contact helpdesk@k4d.info.

K4D services are provided by a consortium of leading organisations working in international development, led by the Institute of Development Studies (IDS), with the Education Development Trust, Itad, University of Leeds Nuffield Centre for International Health and Development, Liverpool School of Tropical Medicine (LSTM), University of Birmingham International Development Department (IDD) and the University of Manchester Humanitarian and Conflict Response Institute (HCRI).