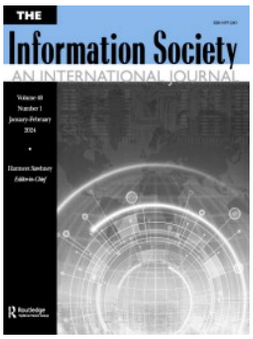

The Information Society
An International Journal

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/utis20

The Chinese surveillance state in Latin America? Evidence from Argentina and Ecuador

Maximiliano Facundo Vila Seoane & Carla Morena Álvarez Velasco

To cite this article: Maximiliano Facundo Vila Seoane & Carla Morena Álvarez Velasco (23 Feb 2024): The Chinese surveillance state in Latin America? Evidence from Argentina and Ecuador, The Information Society, DOI: 10.1080/01972243.2024.2317057

To link to this article: https://doi.org/10.1080/01972243.2024.2317057

THE INFORMATION SOCIETY
https://doi.org/10.1080/01972243.2024.2317057

The Chinese surveillance state in Latin America? Evidence from Argentina and Ecuador

Maximiliano Facundo Vila Seoane[a] and Carla Morena Álvarez Velasco[b]

[a]School of Politics and Government, National University of San Martín, San Martín, Argentina; [b]Institute of High National Studies, Quito, Ecuador

ABSTRACT

Western authors fear that Chinese exports of surveillance technologies to Global South countries may lead to reproduction of the problematic surveillance practices that the Chinese state practices within its borders. However, much of this literature is not based on empirically-grounded research. To examine such concerns, we investigated two surveillance projects built in Argentina and Ecuador in cooperation with Chinese enterprises—JSeI in Argentina and ECU 911 in Ecuador. Based on empirical evidence, we argue for a more situated and differentiated approach for examining such projects that considers the distributed agency among local and Chinese actors, as well as the economic, social, and political factors that led to their deployment.

KEYWORDS

Argentina; Chinese surveillance technologies; Ecuador; Global South; surveillance state

Introduction

The internationalization of Chinese companies selling surveillance technologies in the Global South is a matter of pressing academic and policy concern. Western academics, policy analysts, and pundits fear that the export of such technologies may lead to reproduction of the problematic surveillance practices that the Chinese state practices within its borders. Thereby, it is argued that China is at the forefront of spreading what Freedom House has termed "digital authoritarianism" (Shabhaz 2018); a model of governance *via* digital technologies that is believed to further embed autocracies, and degrade democracies. In specific relation to Latin America, US academics, policy makers, and media outlets have advanced similar arguments regarding the threats posed by the deployment of Chinese surveillance systems in the region (Berg 2021; Democratic Staff Report 2020; Ellis 2021, 2022; Garrison 2019; Mozur, Kessel, and Chan 2019). However, much of this literature is not based on empirically-grounded research. Therefore, there is little knowledge about the veracity of such claims, about why states in the Global South initiated such surveillance projects with Chinese companies, and how were they really implemented.

We contribute to this literature by investigating two prominent cases of surveillance systems built by Chinese state-owned enterprises in Latin America: the ECU 911 project in Ecuador (2012–2021) and Jujuy Seguro e Interconectado (JSeI) project in Argentina (2016–2022). These cases matter because they were portrayed as representing the menacing expansion of Chinese surveillance systems into the region (Garrison 2019; Mozur, Kessel, and Chan 2019). Further, if China seeks to expand its problematic surveillance practices into Latin American states, it is reasonable to assume this will be more visible in these cases, where the state influence is direct. Specifically, in this article we investigate the reasons why both states cooperated with their Chinese counterparts, detailing the features of the so-called surveillance projects. Furthermore, we analyze the implementation of the projects, including an examination of the criticisms and opposition they faced.

We argue for a situated and differentiated approach for examining the implementation of Chinese surveillance projects in the Global South. First, although foreign critics have portrayed these projects as surveillance systems, actually they involve more dimensions, e.g. increased the connectivity of government organizations, enhanced emergency response systems.

CONTACT Maximiliano Facundo Vila Seoane mvila@unsam.edu.ar School of Politics and Government, National University of San Martín, Av. 25 de Mayo 1021, 1650 San Martín, Buenos Aires, Argentina.

Second, as our case studies indicate, the agency in these projects is distributed, rather than limited to Chinese actors. In fact, different combinations of Chinese, local, and even foreign actors have participated in the initiation, definition of requirements, technological design, implementation, management and operation, and upgrade of the projects. Third, much of the criticisms against the expansion of Chinese firms selling surveillance technologies is ahistorical, since it disregards the fact that the deployment of such systems had been well under way before the procurement from Chinese companies. Fourth, the procurement of Chinese surveillance technologies does not depend on the political leaning of the Latin American political parties in power. Policy makers chose Chinese systems mainly due to economic reasons. Finally, we found a divergence between the local criticisms of the projects and the widely-distributed foreign ones. The former focused on technological dependence, alleged corruption in the procurement of the systems, and the need for more accountability in the implementation of the systems, whilst the latter reproduced the view of US government sources about the threat posed by Chinese firms.

The rest of the present article has five sections. The first one synthesizes the literature about the expansion of China's surveillance systems in the Global South. The second explains the methods used to collect and analyze data. The third section presents the results of the analysis of both case studies. The final two sections discuss and then conclude with a synthesis of the main findings.

China's surveillance systems in the Global South

During the last decade, Chinese companies selling surveillance technologies have been quite successful in their internationalization in the Global South. Video surveillance cameras, smart city, and safe city solutions provided by firms such as Dahua, Hikvision, and Huawei, among others, can be found in many cities of the developing world. This is an offshoot of the boom in smart cities in China (Hu 2019), which has led to the accumulation of technological capabilities and solutions for urban management. Since then, Chinese firms have sought to export surveillance technologies to other markets, competing with Western firms offering similar products and solutions, such as Bosch, Cisco, IBM, and Siemens.

However, this expansion of Chinese surveillance companies in the Global South has become a persistent issue in policy and media circles in the US and other Western countries (Cheney 2019; Democratic Staff Report 2020; Gravett 2020; Polyakova and Meserole 2019; Shabhaz 2018). These commentators denounce the very problematic practices of surveillance implemented within China. For example, China has deployed the largest video surveillance system in the world, the SkyNet project, which has over 200 million cameras, and can identify a citizen in less than 10 min thanks to advanced facial recognition technology. Likewise, they generally make reference to the controversial use of AI-enabled surveillance technologies against Uyghurs in Xinjiang. Similarly, they condemn China's censorship practiced through digital technologies, such as the Golden Shield Project (also known as the Great Firewall), that blocks Chinese internet users' access to banned foreign websites and services.

Furthermore, they are equally concerned about China's exports of surveillance technologies into the Global South, because it may propagate China's practices of digital authoritarianism (Cheney 2019; Democratic Staff Report 2020; Gravett 2020; Hemmings 2020; Polyakova and Meserole 2019; Shabhaz 2018). Although their criticism targets the digital expansion of Chinese firms in general, the sale of surveillance technologies, often branded as "safe city" projects, has especially attracted scrutiny. They fear that these projects may lead to the violation of human rights in recipient states as in China, because they provide video surveillance cameras and advanced facial recognition technologies that can be used to infringe citizens' rights. For some commentators, these concerns are especially problematic in states they classify as autocracies (Shabhaz 2018). Others consider the export of Chinese surveillance technologies equally dangerous in both autocracies and democracies, because they spread political illiberalism (Cheney 2019; Democratic Staff Report 2020; Feldstein 2019). In fact, they claim that, in the former, surveillance technologies may further entrench the state's power over civil society, whilst in the latter, the use of such technologies may cause democracies to backslide into autocracies.

American academics and policy analysts specializing in China-Latin America relations have expressed worries about Chinese companies selling surveillance technologies to Latin America in articles and public statements, especially at the US-China Economic and Security Review Commission (Berg 2021; Ellis 2021, 2022). For example, Ryan Berg, senior fellow at the Center for Strategic and International Studies, while acknowledging surveillance technology may be used for addressing physical security challenges in Latin

America, claimed that "Chinese surveillance technology could play a key role in assisting democratic backsliding in the region" (Berg 2021, 6). Likewise, Evan Ellis (2021), an American professor at the US Army War College, accused China of cultivating "anti-US leftist populism". In his view, leftist regimes have opened the door to Chinese surveillance systems in the region, and potentially to the expansion of digital authoritarianism. Ellis (2022, 27) considers Bolivia, Ecuador, and Venezuela among China's "authoritarian friends" that have received funding and surveillance systems to remain in power.

In this vein, the projects we studied—JSeI in Argentina and ECU 911 in Ecuador—also received critical coverage in the literature (e.g. Gravett 2022; Kassenova and Duprey 2021). In the case of Ecuador, the *New York Times* published an article titled "Made in China, exported to the world: The surveillance state" (Mozur, Kessel, and Chan 2019), which argued that the ECU 911 system is part of the expansion of the Chinese surveillance state into the country. Its authors stated that Ecuador's "feared domestic intelligence agency" may have abused its access to ECU 911's video feed for domestic espionage. They based their allegation on the testimony of a critic of former President Correa, who said that the government installed a camera in front of his house to spy on him. They concluded that "It was a move out of the police playbook in China, where cameras are positioned outside the doors of high-profile activists" (Mozur, Kessel, and Chan 2019). Likewise, the JSeI project attracted international and national attention due to an article by an American journalist, Cassandra Garrison, working for Reuters wrote an article entitled "'Safe like China': In Argentina, ZTE finds eager buyer for surveillance tech" (Garrison 2019). Garrison asserted that "Chinese telecoms giant ZTE is installing a little slice of the Asian nation's vast surveillance state—security cameras that the local government says will help to curb street crime" (Garrison 2019), prioritizing a US government sources, who said that "China gathers and exploits data on an unrivalled scale, and uses the information to promote corruption, support arbitrary surveillance, and silence dissent" (Garrison 2019). Garrison added that ZTE had been involved in the procurement of technologies for the problematic Chinese surveillance practices in Xinjiang (Garrison 2019).

In contrast, there are few research or other articles that challenge these criticisms. For instance, Gagliardone (2019) points out that the preoccupation with the supposed export of China's digital authoritarianism model underestimates the similar role that Western models have played in justifying repressive surveillance practices. Indeed, numerous African countries have drawn on the US War on Terror to justify the procurement of surveillance equipment and software from foreign providers—including Western ones—to prevent internal and foreign terrorist threats. Similarly, Woodhams (2020) questions the claim that China is entirely to blame for the global spread of surveillance technologies, since many Western firms and governments have also been selling surveillance technologies in the Global South.

A general limitation of this literature is that much of the criticism as well as the few instances of counter-criticism are based on secondary sources and limited reporting, or are speculative claims that extrapolate the surveillance practices within China to all the countries in the Global South. All in all, there is a general lack of empirically-grounded research that supports such claims or even refutes them. In this article we seek to help fill this gap *via* an empirical analysis of how two such surveillance projects were implemented in states of the Global South.

Methodology

We chose projects in Argentina and Ecuador for our case studies—JSeI in Argentina and ECU 911 in Ecuador, because they illustrate the intensifying and broadening relations with China in the region, which has been historically under the influence of the US. Indeed, since 2007 China has displaced the US as Argentina's second most important trading partner after Brazil. Politically, although the bilateral relationship between Argentina and China was not exempt from frictions (Saguier and Vila Seoane 2022), ties have strengthened with the signing of a comprehensive strategic partnership in 2014, and Argentina's joining China's Belt and Road Initiative in 2022. In the case of Ecuador, under the presidency of Rafael Correa (2007–2017), the country established closer ties with China (Herrera-Vinelli and Bonilla 2019). In terms of economic ties, since 2011, China has its second biggest trading partner after the US. With regard to political ties, in 2015, the China and Ecuador signed a comprehensive strategic partnership, and, in 2018, Ecuador joined China's Belt and Road Initiative. Since the presidency of Lenin Moreno (2017–2021) there was a realignment of Ecuador's foreign policy toward the US (Jepson 2022) but China's economic relevance remains. In both countries we find similar criticisms of the increased political and economic ties with China, namely, the emergence of a new and

asymmetrical core-periphery relationship, a growth in low added-value natural resource exports that undermines national industrialization strategies, and concerns about the environmental impacts of infrastructure projects, among others (Bernal-Meza and Xing 2020; Gonzalez-Vicente 2017; Herrera-Vinelli and Bonilla 2019; Jepson 2022; Saguier and Vila Seoane 2022). In this context, both states have been subject to US pressure and criticisms against Chinese infrastructure projects and investments.

For our case studies, in 2022, we collected documents, made on-site observations, and conducted in-depth interviews. Specifically, we conducted a web search of policy, media, and government public documents, plus a search of academic articles and books discussing the two surveillance systems. Furthermore, we made on-site visits to the cities of Quito in Ecuador and San Salvador de Jujuy in Argentina, where the main components of each system were installed. In these visits we observed the systems in operation and we visited the management centers. Moreover, we complemented these sources with primary data collected through in-person and online interviews. We contacted local actors involved in the design and implementation of the systems, and other stakeholders who had conveyed both support and criticisms of the projects; conducting 14 interviews in total (see Appendix 1 for details including the interviewee codes used in the Findings section). We prepared an interview guide that we slightly adapted according to the profile of each interviewee. The interview questions sought to explore who were the actors involved in the initiation and implementation of the projects, the partnerships established with Chinese firms, if there were local adaptations of Chinese technologies, opinions of interviewees about the coverage by media outlets of both projects, and criticisms of the projects. We triangulated these different sources to trace the actors involved in the different phases of the projects.

Table 1. Main actors involved in ECU 911 and JSeI projects.

	ECU 911	JSeI
Initiated by	Coordinating Ministry of Security	Jujuy's Ministry of Security
Requirements defined by	Coordinating Ministry of Security	Jujuy's Ministry of Security
Designed by	CEIEC (technical)	ZTE (technical)
Implemented by	Local firms and CEIEC	Local firms and ZTE
Managed and operated by	ECU 911	Jujuy's Ministry of Security
Maintained and upgraded by	Until 2018: CEIEC From 2018 onwards: still under negotiation	ZTE for 3 years

Findings

Table 1 provides a summary of the various local and foreign actors involved in the different phases of the projects. The next subsections examine each of the case studies in more detail.

ECU 911

The installation of ECU 911 in Ecuador must be contextualized in the broader political transformations that the country experienced during the presidencies of Rafael Correa (2007–2017). In 2007, the center-left political coalition Alianza PAIS led by President Correa started a process of profound political and institutional reform in various areas of the country, which led the passing of a new national constitution in 2008. The reorientation of Ecuador's foreign policy and changes in its security sector are the reforms that matter most for our present discussion.

In terms of foreign policies, the Correa administration strengthened political and trade alliances with different countries, both within and outside Latin America. One of the administration's goals was to weaken Ecuador's economic and political dependence on the US. In this context, the government sought a strategic rapprochement with China with the aim of increasing exports to it, as well as accessing its funding sources. Furthermore, in 2008, the new national constitution prohibited the installation of military bases within Ecuador. Consequently, President Correa refused to renew the 10-year agreement that Ecuador had with the US military which, in 2009, had to close its Forward Operating Location base in the coastal city of Manta (Álvarez Velasco 2014).

As for the security sector, the new constitution introduced the "integral security" concept, which would thereafter become the guiding precept to rethink the national security architecture of Ecuador (Cabrera 2019; Lucio Vásquez 2020). It called for the updating of the National Security Law, enacted in 1979 during the transition from military dictatorship to a democratic regime, during the Cold War, when it was influenced by the US counterinsurgency strategy against communism in the region (Lucio Vásquez 2020). The 1979 law was especially criticized for its focus on military actions against external threats. Instead, the integral security precept called for broadening the areas falling within the security sphere, less linked to the field of defense and closer to the notion of human security formulated by UNDP (1994) as well as extending security concerns to nature (EC1). Although the specificities of the actualization of the

integral security concept evolved during the Correa administration (Cabrera 2019), it led to a planning process whose outcomes were two national plans for Integral Security for the periods 2011–2013 and 2014–2017 respectively.

ECU 911 implementation under the Correa administrations (2011–2017)

After the 2010 police strike that caused a national political crisis and a local insecurity crisis in Quito (EC5), in 2011, the National Integral Security Plan for 2011–2013 announced the creation of an Integrated Security System (SIS), named ECU 911. This project aimed to materialize integral security by articulating all related institutions with responsibilities within this broader framework, such as the National Police, the Secretariat of Risk Management, local governments, the Red Cross, the Ministry of Public Health, the Ecuadorian Social Security Institute, the National Transit Agency, the Fire Department, and the Ministry of National Defense. In particular it established a comprehensive response system for citizens' emergencies *via* a national 911 number (Ministerio de Coordinación de Seguridad 2011, 34), which the country lacked (Corral-De-Witt et al. 2018). Moreover, the main specificity of this project is that it sought to build a network of centers of national, regional, and local scope. Each of them would have video surveillance capabilities to reduce violence in public spaces and to respond to emergencies. Furthermore, these centers would generate other data of public interest. Most importantly, these ECU 911 centers would all be interconnected, creating a network. Thereby, this system, ECU 911, would have national reach.

Although announced in 2011, the government had been planning ECU 911 since 2008. In that year, the Correa administration organized a technical commission comprising public officials of the Coordinating Ministry of Security and Ecuador's navy (EC8), which studied smart city projects in other countries, such as Argentina, Brazil, China, Spain, the UK and the US, (EC2, EC3). It sought to learn from the strengths and weaknesses of other preexisting projects to design a system for Ecuador that went beyond the surveillance function (EC1). During the 2008 Beijing Olympics, Ecuadorean public officials saw the smart city solution employed in China's capital (EC3). This led to a contact with the Chinese government *via* its embassy in Ecuador, which offered funding for a project tailored to Ecuador's needs on the condition that it was implemented by a Chinese state-owned enterprise: the China National Electronics Import & Export Corporation (CEIEC). Based in Beijing and founded in 1980, CEIEC had an overseas division with experience in integration engineering in numerous sectors in African and Asian countries, and it also had a division of defense electronics system integration (CEIEC 2011). On February 2011, the Coordinating Ministry of Security signed an agreement with CEIEC to develop the project in Ecuador (Secretaría Nacional de Riesgos 2011). China funded the project *via* an estimated USD 240 million loan (Aid Data n.d.).

Although CEIEC was the firm integrating and deploying the project, interviewees noted that the design of the system was based on the knowledge Ecuador's public officials had acquired during their visits to smart city projects of other countries. According to a former ECU manager, "the ECU-911 has the best of each of these places we visited" (EC3). For example, the video surveillance system copied the practices in the UK, whilst the 911 system was copied from the US system (EC3). Other norms and procedures for operation of the system were developed in a participatory manner by different stakeholders involved in the actualization of the integral security concept (EC1). According to ECU 911's management, this is the reason the project has received prestigious certifications from different Western organizations related to public security (EC3). For instance, the ECU 911 established measures to safeguard the information captured by the ECU 911 nodes, such as video surveillance, audio, and other data types, for the purpose of analysis and evaluation by the judicial institutions in accordance with national legislation (ECU 911 2015, 21). These local guidelines could reduce the concerns about how data from a Chinese-installed system is used, though there have still been criticisms by some human rights organizations that, at the time, Ecuador still lacked a data protection law that could effectively underpin such guidelines (Access Now 2021, 53).

In terms of technology, ECU 911 used components from suppliers from countries other than just China; for example, the data storage devices were supplied by HP, a US company (EC3, EC5). Therefore, it is inaccurate to present the ECU 911 as solely Chinese in origin or design (EC3). The main part developed entirely by CEIEC was the software platform that integrates components and coordinates the ECU 911 system. The source code was given to ECU 911's public officials, who could, in principle, keep on developing it afterwards (EC3). However, Ecuadorian technicians never modified the source code by themselves (EC5). Instead, the changes were implemented by Chinese technicians upon the request and

supervision of Ecuadorian technicians (EC3). Overall, then, the cooperation with CEIEC did not involve any process of technology or knowledge transfer that would allow Ecuadorians locally to maintain or update the software or hardware. In case of malfunctions or upgrades, CEIEC offered technical support until December 2018 (EC5).

Local Ecuadorian actors have always been in charge of the overall management and operation of ECU 911. To facilitate this and to learn about the operation of the system, a small group of Ecuadorian technicians were trained in China, who then replicated the training in Ecuador. Our sources stressed that the training was technical, not ideological, with the purpose of developing local capabilities to operate ECU 911's technologies, as indeed happened (EC2, EC3). ECU 911 operators received training from other states as well. For instance, ECU 911 signed a cooperation agreement with the UK Government, which sent specialists from the College of Policing to train local operators in video surveillance (British Embassy Quito 2014). There has also been some degree of transparency about the operation of the system with resolutions and other administrative documents made available on ECU 911's web page. This somewhat rebuts the presumption that Chinese-installed systems are implemented in an opaque way, though it is notable that, despite this transparency by ECU 911 and its public officials, CEIEC representatives did not reply to our interview requests.

On February 6, 2012, President Correa inaugurated the first national center of ECU 911 in the city of Samborondón, neighboring Guayaquil. From then onwards, numerous other centers were installed across the country until the network of centers was completed. Each of these centers articulates the services provided by different institutions in charge of operationalizing the concept of integral security. By 2016, ECU 911 had two national centers, five zonal centers, and nine local centers, managing a total of approximately 4,600 cameras that would increase in the following years. From 2012 to 2016, ECU 911 received around 62 million calls, out of which 10 million were emergencies that required response from the involved institutions (Corral-De-Witt et al. 2018).

Due to its scale and achievements, ECU 911 became an emblematic project in the cooperation between China and Ecuador. In November 2016, President Xi visited ECU 911's center at Quito, where he heard workers' testimonies about the key role the system had played in coordinating the response to the earthquake that Ecuador suffered in April of that year (Xinhua Español 2016). This leading case helped CEIEC to project its technological prowess, which led it to offer similar projects to other countries in the region, such as Argentina, Bolivia, Peru, and Venezuela.

ECU 911 under the Moreno administration (2017–2021) and beyond

In 2017, the results of the presidential elections that took place in Ecuador would affect the development trajectory of ECU 911. Although former President Correa supported Lenin Moreno, who won the election and governed during the period 2017–2021, soon after his inauguration, Moreno broke with his mentor. This cleavage significantly modified numerous policies in Ecuador. President Moreno denounced his predecessor as authoritarian, corrupt, and initiated a process of persecution of his former allies. These tensions aggravated the political polarization in the country. Economically, President Moreno distanced his administration from the "Socialism of the twenty first Century" of Correa, and brought back again policies characterized by critics as neoliberal. This involved a steep adjustment of the public budget, which reduced funds for the security sector. On top of that, the COVID-19 pandemic forced the government to prioritize health care above other sectors, which led to further cuts for security. In terms of foreign policies, President Moreno realigned Ecuador with the US (Jepson 2022). For example, Ecuador returned as a debtor to the IMF. In 2018, the country accepted once again US military operations in its territory. The concept of integral security was downgraded to prioritize more militarized security strategies.

These dramatic twists in Ecuador's politics led to a decline of ECU 911. This was caused partly due to the neoliberal policies of budget constraints, which meant that ECU 911 could not replace outdated technologies on time (ECU 911 2019). For instance, in 2022, ECU public officials estimated 50% of their cameras required replacement by 2023, while they stated 1,081 cameras were no longer working (Sanchez 2022). The deterioration was further accentuated by both domestic and international criticisms voiced against ECU 911. Domestically, the most important one was the presumed overpricing involved in Ecuador's dealings with CEIEC during the construction of ECU 911 (El Comercio 2018). Internationally, the *New York Times* published the article referenced above claiming that ECU 911 was part of the Chinese surveillance state's expansion into Ecuador (Mozur, Kessel, and Chan 2019). This article has been highly influential: cited 93 times at the time of writing according to Google Scholar and referenced by

numerous Western policy documents as evidence that the Chinese surveillance state is dangerously expanding into Latin America (Access Now 2021; Berg 2021; Ellis 2022). The Moreno administration echoed this reporting to further accuse his previous mentor, former President Correa, of authoritarianism. Finally, US politicians have used this reporting to criticize ECU 911, and more broadly, to oppose the cooperation between Ecuador and China (Democratic Staff Report 2020; Menendez 2022).

The allegations in the *New York Times* are problematic for three main reasons. First, the reporting was done and published during Moreno's administration, without consulting sources linked to the previous Correa administration, although the latter was the target of the criticisms. Hence, the article reproduced the Moreno administration's view about his predecessor, which was unsurprisingly negative, and rather overblown, amidst the public political struggle between them. Second, the alleged danger posed by the expansion of Chinese surveillance technologies into Ecuador disregarded the broader local factors driving the procurement of the system, such as the concept of integral security. Similarly, these sources overlooked that the system was managed and operated mainly by local actors. Finally, it overlooked the view of officials from Ecuador's intelligence agency, who rejected claims that the ECU 911 system was used for surveillance of citizens (EC7). Although they recognize they had access to video feeds, they stressed these were rarely used, and definitely not useful for the generation of strategic intelligence, which is the main mission of the agency (EC7). In fact, for their daily analysis of strategic data they use IBM Watson artificial intelligence technology (EC7).

In this context, the technical support that CEIEC offered was not renewed from January 2019 onwards (EC5). Although Ecuador and CEIEC initiated a discussion for a new contract, they did not reach a new agreement for two reasons. First, Ecuador's public officials found that the price CEIEC demanded was unreasonable (EC5). This indicates that the tailored platform that CEIEC developed for ECU 911 brought with it the danger of technological dependence on the Chinese provider, which could arbitrarily increase its price over time. Second, in November 2020 the US sanctioned CEIEC over alleged cooperation with the Venezuelan government to undermine democracy. Consequently, since then, CEIEC cannot trade with Ecuador (EC5), a challenge that is compounded by the fact that Ecuador's economy is dollarized.

The situation has not changed much since the presidency of Guillermo Lasso, who took office in mid-2021. Since then, ECU 911 public officials have been planning and budgeting a major upgrade of the system to replace the hardware and software that passed its life expectancy (EC5). Although this has not been accomplished yet, the sources we consulted said they will be open to all providers, irrespective of nationality. However, the pressures from US government officials against the project have continued. For example, in March 2022, the US Senate introduced the United States-Ecuador Partnership Act, which pledges to combat the negative Chinese influence in the country, and portrays ECU 911 as a threat to Ecuador's democratic governance (Menendez 2022). Despite these allegations, neither the Moreno nor the Lasso administration closed ECU 911 because of any alleged misuse for authoritarian surveillance practices. By contrast, it has continued operating basically for the public service it offers to citizens, though with economic and technological difficulties to fulfill its work. However, the trend suggests Western actors are increasingly becoming involved either as financers or technology suppliers, in replacement of previous Chinese counterparts. For instance, the US-led Inter-American Development Bank (IADB) has been granting credits to upgrade parts of the system. Likewise, during the pandemic, ECU 911 incorporated machine learning software developed by the IADB to detect patterns in the video surveillance images of people that were not respecting a 1-meter social distancing. To conclude, how the system may unfold in the future remains open, and shaped by local and international politics.

Argentina: Jujuy Seguro e Interconectado (JSeI)

During the last two decades, Chinese surveillance firms have been expanding significantly in Argentina. A market study by the Argentine Chamber of Electronic Security shows that in 2018 national firms commercializing surveillance technologies imported them mostly from China (62%), followed far behind by Canada (5.7%), Brazil (5.2%), México (5%), and the US (4.7%) (CASEL 2019, 35). Indeed, any pedestrian of Argentine cities can easily find video cameras supplied by Chinese private firms in shops and as part of public safety systems. Among Chinese state-owned enterprises, ZTE is the most prominent one selling surveillance equipment to the Argentine state. This company, which has been at the forefront of the internationalization of Chinese telecommunication firms across the globe, has been operating in Argentina since 2005, mainly providing equipment and services to telecommunication carriers, governments, and selling smartphones to consumers.

Our particular focus here is a public safety system sold by ZTE to the northwestern province of Jujuy. To understand the origins of this project, we need to contextualize the security and political situation of the province. Jujuy's crime statistics are not as dramatic as in other parts of the country. In fact, whilst during 2017–2020 the average national homicide rate was 5.35 victims per 100,000 inhabitants, Jujuy had 3.4 victims per 100,000 inhabitants (Ministerio de Seguridad de Argentina 2022). If we consider citizens' perception of insecurity, the last available statistics from 2017 show that 40.2% of Jujuy' citizens thought that security was a very serious problem, slightly below the national average which was 41.7% (INDEC 2018). In this context, security policies are usually at the top of politicians' agendas. This was the case of candidate Gerardo Morales who, in 2015, was running for Governor of Jujuy as part of Cambiemos (Let's Change), a national center-right political coalition. On the campaign trail, Morales made several promises to fight crime, such as creating a Ministry of Security, which the province lacked, and upgrading video surveillance capabilities. The preexisting system was deployed in 2013 by the left-wing ruling party. It consisted of a 911 emergency response number and a video surveillance system supplied by a German company (TodoJujuy 2015). They were under the management and operation of the provincial police. However, during the campaign, deputies of Morales' party denounced these systems as dysfunctional, because the number of working cameras (44) was insufficient and the police force was under-resourced to respond to emergencies (Jujuy al Día 2015).

Once elected, Governor Morales' team at the brand-new Ministry of Security began working on the update of the 911 response and video surveillance system. The first option they considered was following a similar model to that of the municipality of Tigre. This touristic city near Buenos Aires, inspired by the models in New York and Washington, DC, was one of the first in the country to implement a cutting-edge surveillance system in cooperation with NEC, a Japanese company. However, this model involved the procurement of cameras under a commodatum agreement, which meant the devices would not be owned by the province. Therefore, Jujuy's policy makers did not favor this model (AR1). The other safe city model that Jujuy's policy makers visited was deployed in the neighboring province of Salta by Claro, a Mexican telecommunications firm, in partnership with Chinese companies, initially Huawei and later updated by ZTE (AR1). Jujuy's policy makers were not convinced by this model either, because the fiber optic network needed for the surveillance system remained owned by the Mexican firm (AR1). Despite this, the visit to Salta led to a contact with ZTE, which proposed a tailored solution to Jujuy's needs, in which the provincial government would own both the cameras and the fiber optic network (AR1). Therefore, the policy makers were persuaded by this provider's offer due to the advantages of ownership over the equipment and network.

In July 2016, the Government of Jujuy and ZTE signed a Memorandum of Understanding to advance the project. ZTE sought to use direct contracting procurement without the need for public tender, which was possible through a state-to-state agreement that Argentina had signed with China. However, Jujuy public officials preferred an international public procurement process to ensure transparency (AR1). In November 2016, the public tender for the project was launched, and it was titled Jujuy Seguro e Interconectado (JSeI) (Ministerio de Seguridad de Jujuy 2016), describing the technical requirements of the project defined by the Government of Jujuy. It involved deploying a video surveillance system composed of 600 cameras, a monitoring center for 24 operators, and a TV wall. In addition, the tender required the installation of a telecommunications network connecting 310 points of government, such as government offices, hospitals, police stations, schools. The tender included the list of government-defined geolocations of video cameras and points of government. The budget was estimated at US$24 million plus taxes. The government called this first tender phase 1 of the project, because it was focused on the city of San Salvador of Jujuy, though the authorities envisioned its extension to the rest of the province in subsequent phases of the project. In comparison to Ecuador's case, this was therefore a relatively small turnkey project.

ZTE was the only company that presented a proposal and it won the tender. It proposed that 85% of the project's cost be paid *via* an 8-year term loan granted by the Chinese Exim Bank to the province of Jujuy. The result of the tender was questioned by opposition politicians, who disputed the decision to borrow in dollars, since it endangered the fragile finances of the province (AR2). Furthermore, they alleged that the video cameras were overpriced, suggesting that there was corruption in the procurement process (AR2). Although these accusations were not proven, and debt-related worries were dismissed by Jujuy's government, it is important to note that the surveillance capabilities of the system were not questioned, but rather how it was procured.

In May 2017, in the presence of President Xi, Jujuy's Minister of Security signed the contract with ZTE in Beijing. The project was then delayed for two years due to contractual issues that were finally solved on March 2019, though the Chinese funding was finally channeled *via* a different bank (BBVA Hong Kong) but under the same initial funding conditions agreed with the Exim Bank (AR1, AR3). In May 2019, the government of Jujuy and ZTE officially launched the project. The ZTE executive in charge of the presentation pledged to finish it in 18 months. He also presented the company's special task force for implementing the project, composed of Chinese, local, and other foreign workers (Morales 2019). The Chinese executive closed the presentation promising to turn Jujuy into a "safe, interconnected and intelligent city" (Morales 2019, 1:05).

Six weeks after this official launch, Reuters published an article asserting that the project represented the expansion of the Chinese surveillance state into Argentina (Garrison 2019). Although the reporting prioritized US government sources, in contrast to the *New York Times's* article about Ecuador, this one did include views of Argentine and Chinese actors dismissing such criticisms. However, rather than analyzing in depth what the project actually consisted of and what were the reasons for its implementation, the article framed the project as part of the so-called "US-China tech war" (Garrison 2019). As in Ecuador's case, the importance of the Reuters article resides in the broader ramifications it had in Argentina. For example, Argentine national newspapers reproduced the US critical views about ZTE's project that the Reuters article conveyed, without any further local reporting. Similarly, the Reuters article has been cited in reports by Access Now that criticize the spread of surveillance technologies into the region (e.g. Access Now 2021).

However, the fears of US government sources about expansion of the so-called Chinese surveillance state conveyed *via* the Reuters article seem overstated when we take into account several features of the project. First, the supposed "Chinese surveillance system" is in fact the work of many actors, including local firms. For instance, the installation of the cameras was done by local firms in cooperation with the provincial state-owned electric company (EJESA) (AR1). Likewise, the fiber optic network connecting the points of government, once finished, will be managed by a provincial state-owned enterprise, Jujuy Digital SAPEM (AR1). Second, the capital city of Jujuy already had a 911 and a video surveillance system, which was deployed during the previous administration of the current left-wing opposition party, mainly using surveillance technologies from a German supplier. In effect, the cooperation project with ZTE upgraded this earlier system rather than introduce entirely new surveillance capabilities into Jujuy. Third, ZTE won the tender because it could offer the tailored solution that Jujuy needed in a cost-effective way, in particular the ownership of both the cameras and the fiber optic network (AR1, AR4). Chinese state funding was important in tipping the balance in favor of ZTE, but there was no a priori reason why non-Chinese foreign suppliers could not have bid and provided similar technological capabilities. Finally, the project is under the management and operation of Jujuy's Ministry of Security. Although ZTE did offer training, this was solely technical and related to the operation of the telecom infrastructure and the cameras; it did not involve wider political or ideological content (AR4). For all these reasons, it seems that ZTE's motivations were commercial, rather than political—exporting Chinese surveillance practices.

Nevertheless, opposition politicians do fear that the video surveillance system may strengthen what they characterize as a punitive state in the province (AR2). Indeed, since Governor Morales came to power, there have been numerous cases of persecution of his critics, though not *via* the use of video surveillance. The most salient case was the incarceration of the indigenous leader Milagro Sala who, in 2016, was imprisoned by the Jujuy courts due to alleged incitement to commit crimes, organize riots, and sedition. The Inter-American Court of Human Rights and the UN Human Rights Council have denounced this decision as arbitrary and demanded that the province release her, with no results so far. A researcher from an Argentine human rights organization shared these worries about the potential misuse of the system by Morales' administration, but also extended the concerns to the opposition center-left party, which similarly had problematic cases of police abuse while in power (AR5). These concerns are based on the lack of independent accountability mechanisms for the use of such systems by security forces (AR5). Furthermore, the researcher criticized the lack of public documents assessing the human rights impact of the JSeI (AR5). In this context, these critics fear that the video surveillance part of JSeI might be misused for political purposes (AR2, AR5).

During fieldwork in 2022, these were speculative concerns, however, at the moment of writing this article (July 2023), the situation looks far more problematic. The reason for this assessment is that in June 2023, the police of Jujuy used excessive force against

indigenous protestors who resisted a reform of the provincial constitution. Several human rights organizations condemned the provincial state violence (Buenos Aires Herald 2023). Although the manner in which JSeI was employed in these incidents is not public, this context of violence supports the apprehensions posited by the aforementioned sources.

Discussion

The empirical data we gathered from Argentina and Ecuador challenges several claims of the authors criticizing the expansion of Chinese surveillance systems into the Global South (Berg 2021; Cheney 2019; Democratic Staff Report 2020; Ellis 2021, 2022; Garrison 2019; Gravett 2020; Hemmings 2020; Mozur, Kessel, and Chan 2019; Polyakova and Meserole 2019; Shabhaz 2018), at least in relation to democratic countries. Thereby, our research supports and extends the counterarguments advanced by Gagliardone (2019) and Woodhams (2020) regarding the export of Chinese surveillance technologies.

Although video surveillance is a central component of the projects we studied, naming them just as surveillance systems is inaccurate, because it is not the locally-used term nor does it cover all the other dimensions involved in the projects. Indeed, their main aim has been to tackle citizens' concerns about security; hence, they are locally presented as public safety or citizens security systems. Likewise, they are not limited to video surveillance capabilities. Take the case of Ecuador, where the name of the system, ECU 911, plainly conveys the number that allows citizens to contact the public authorities in case of emergencies. In the case of Jujuy, the project also includes connectivity in its name, since it deployed a fiber optic network to connect different arms of the provincial government.

Likewise, our cases indicate that the projects are not entirely Chinese. They comprised different combinations of Chinese, local, and even foreign actors at different phases of the project. For instance, in both cases, local actors led the initiation of the projects and defined the requirements for their technical design, which was then undertaken by the Chinese firms. In the case of Ecuador, the requirements were based on smart city models from Western countries, and part of the equipment was sourced from Western firms (e.g. HP), whilst in JSeI the technical design was implemented by ZTE in response to requirements of the provincial government. Regarding the deployment of the systems, apart from the Chinese companies, in both cases local firms were involved. The management and operation of the systems is undertaken by local actors, with no Chinese actors involved. For contractual reasons, the maintenance and update of the systems depends on the Chinese companies, but they can be replaced by other providers (EC5, AR1).

Furthermore, much of the criticism against the spread of surveillance technologies in the Global South is ahistorical, assuming they began with the export of Chinese technologies. In fact, in both cases the spread of surveillance technologies had been well underway, and provided by other foreign providers, including Western ones. Prior to the timeframe of our study, the city of Quito initiated its surveillance system in 2002 in partnership with a Colombian firm (Löfberg 2008), whilst as noted in our case, the video surveillance system in Jujuy had been initiated with German technologies. For the same reasons, both systems could potentially have been sourced from non-Chinese foreign providers, offering technologies with similar capabilities. In fact, Ecuador's public officials consulted several others before choosing the Chinese company. Likewise, Jujuy's public officials were first interested in the offer of a Japanese company.

US-based critics accuse leftist parties of introducing Chinese surveillance technology in Latin America (Berg 2021; Ellis 2021, 2022). However, in the Jujuy case, it was the governing center-right political coalition that closed the deal with Chinese firms. Indeed, even though the source we consulted in Jujuy's government expressed apprehension about China's political system, in their view, that is unrelated to the attractive financing and technology offer made by ZTE (AR1). Our empirical data therefore contradicts the idea that only anti-US leftist political parties procure surveillance technologies from Chinese firms.

Be that as it may, the cases indicate that the Chinese state is supporting the internationalization of companies involved in the provision of citizen security equipment, who compete with other foreign firms selling similar technologies in Latin America. Actually, the access to Chinese state funding alongside low price was the key factor according to decision makers in Argentina and Ecuador that inclined them to choose Chinese providers over others, rather than technological superiority or an ideological affinity with the problematic surveillance practices within China.

In both cases, the documents by Western academics, policy makers, and media were more concerned to show the malign influence that China had in the projects (Berg 2021; Democratic Staff Report 2020; Ellis 2021, 2022; Garrison 2019; Mozur, Kessel, and

Chan 2019), rather than to explore why they were started, how they were implemented, and any achievements they may have had. Notwithstanding these limitations, these examples do demonstrate the power of Western media portrayals of Chinese projects, and the associated narrative they follow, which have had an impact both in the West and in Latin America. Local policy makers accused such sources of defaming their projects with Chinese actors; something seen as originating due to the geopolitical threat that China represents to US influence in Latin America (EC2, EC3, AR1).

Nonetheless, there have been local criticisms of these projects, but not focused on the presumed authoritarian practices that the partnership with Chinese companies may trigger, as denounced by foreign critics. First, local media reports focused on the shadowy practices in the procurement processes that favored Chinese companies. Second, policy makers were concerned with the issue of technological dependence. In our particular cases, this related to Chinese suppliers because, even though the management and operation of the systems is done by local actors, in neither case did we find a transfer of technological capabilities for repurposing the software platform at the core of both systems. However, this reflects a wider issue not solely linked to China, as seen in the concerns expressed about technological ownership by the Japanese and Mexican companies in existing Argentine surveillance systems. Third, human rights organizations have been questioning the deployment of surveillance technologies in general: not just the specific projects with Chinese companies but thus also including those in both countries where the suppliers are firms from Western countries, such as Germany, Japan and Israel. Finally, although opposition politicians and civil society sources that we spoke to expressed concerns about the potential abuse of video surveillance technologies (EC6, AR5), during fieldwork, such worries remained in the speculative plane, and did not attract much national media coverage. However, the potential misuse of these systems should not be underestimated.

We think there are at least two reasons that explain this divergence between the foreign criticisms and the local ones. First, Western critics reproduced a dominant narrative within Western, particularly US, sources that portrays whatever is linked to China as a threat. In doing this, these authors assume a simplistic model, in which legitimate concerns about the use of Chinese surveillance technologies in some contexts have been over-extrapolated, and supposed to apply in the same way in all countries of the Global South. But, as this article suggests, a differentiated approach is needed that takes into account of each individual context the particular history, actors, motivations, processes, technologies, etc. Second, surveillance technologies are perceived differently across the world. In contrast to many other Chinese infrastructure projects in extractive industries of Latin America, which are seriously questioned by the citizens due to their environmental impacts, these citizen security projects were demand-driven. Indeed, among the many reasons for the acceptance of such technologies in Latin American countries (Arteaga Botello 2012; Lio 2015), it is worth noting the widely shared belief—even if not evidence-based—that surveillance technologies contribute to address the pressing security challenges faced by citizens on a daily basis. Accordingly, citizen security projects are demanded both by politicians and citizens, regardless of the country of origin of the suppliers.

Conclusions

The empirical data collected in Argentina and Ecuador suggests the need for a differentiated and situated approach to the study of citizen security projects built in cooperation with Chinese firms. Indeed, we showed that it is inaccurate to present such projects just as surveillance systems, when in fact they cover other dimensions, such as emergency response, or increasing the connectivity of public institutions. Furthermore, our data also challenges the claim that these systems are Chinese. Not only are the technologies within them sometimes of multiple origins but we found that the agency in these projects is distributed among Chinese, local and other foreign actors, varying with the phase of the project: initiation, requirements, technical design, implementation, management and operation, and maintenance and update. Similarly, the criticisms against Chinese providers are ahistorical, since they overlook the fact that surveillance processes were already well underway in both states due to the sale of surveillance technologies by non-Chinese foreign firms, including Western ones. In fact, they could have provided a similar solution as the chosen Chinese firms. Additionally, our results showed that the procurement of Chinese surveillance technologies did not depend on the political leaning of the Latin American political parties in power. Policy makers from both right- and left-leaning political parties chose Chinese providers mainly due to their lower costs and state financing, rather than an ideological affinity to emulate Chinese surveillance practices. Finally, the local criticisms of the projects did not overlap with those

made by Western sources, which have too often fitted a US-generated narrative about the presumed threat posed by Chinese companies.

For all these reasons, we conclude that the incorporation of surveillance technologies from Chinese providers did not transfer the problematic authoritarian surveillance practices criticized in China to Argentina and Ecuador. However, our contextualized and differentiated approach does not exclude such an outcome in other conditions of deployment, where local actors may actively seek to emulate such practices, or where preexisting authoritarian practices may be enhanced by the procurement of such technologies. If Chinese companies are only trying to compete against Western companies for market share, then to avoid getting entangled in such cases, it is important that they conduct thorough due diligence of who their clients are.

Acknowledgements

We thank Richard Heeks, Nick Jepson and Seth Schindler of the Global Development Institute, University of Manchester, for the constructive feedback that we received in previous versions of this manuscript. We also thank the comments and suggestions from two anonymous reviewers. All remaining errors are the authors' own responsibility.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This article was supported by the project, "China's Digital Expansion in the Global South," funded by the Faculty of Humanities, University of Manchester, UK. Vila Seoane also thanks the support received from the National Scientific and Research Council (CONICET) of Argentina *via* a postdoctoral scholarship grant.

ORCID

Maximiliano Facundo Vila Seoane http://orcid.org/0000-0002-0134-7714
Carla Morena Álvarez Velasco http://orcid.org/0000-0002-3372-5273

References

Access Now. 2021. Surveillance tech in Latin America: Made abroad, deployed at home. https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf (accessed June 12, 2023).

Aid Data. n.d. China commits a loan of $240 million to Ecuador to set up security service ECU 911. https://china.aiddata.org/projects/39281/ (accessed August 10, 2022).

Álvarez Velasco, C. 2014. *Reforms and contradictions in Ecuador's drug policy*. Washington, DC: Washington Office on Latin America (WOLA). https://www.wola.org/sites/default/files/Drug%20Policy/Ecuador%20memo%20English_FINAL.pdf (accessed June 12, 2023).

Arteaga Botello, N. 2012. Surveillance studies: An agenda for Latin America. *Surveillance & Society* 10 (1):5–17. doi: 10.24908/ss.v10i1.4282.

Berg, R. C. 2021. *China in Latin America and the Caribbean*. Washington, DC: Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep37529 (accessed June 12, 2023).

Bernal-Meza, R., and L. Xing, eds. 2020. *China-Latin America relations in the 21st century: The dual complexities of opportunities and challenges*. Cham: Springer. doi: 10.1007/978-3-030-35614-9.

British Embassy Quito. 2014. Especialistas ingleses del College of Policing entrenan personal del ECU 911 – Ecuador [English specialists from the College of Policing train ECU 911 personnel – Ecuador]. https://www.gov.uk/government/news/254304.es-419 (accessed June 12, 2023).

Buenos Aires Herald. 2023. Jujuy: International human rights organizations express concern. *Buenos Aires Herald,* June 21. https://buenosairesherald.com/human-rights/jujuy-international-human-rights- organizations-express-concern (accessed July 17, 2023).

Cabrera, L. 2019. La seguridad integral en Ecuador: Una visión crítica del concepto a una década de su concepción [Integral security in Ecuador: A critical view of the concept a decade after its conception]. *UNISCI Journal* 17 (51):397–416. doi: 10.31439/UNISCI-69.

CASEL. 2019. Estudio de mercado de la seguridad electrónica de la República Argentina [Market study of electronic security in the Argentine Republic]. *Innovación: Seguridad Electrónica* 17 (115):6–69. https://www.revistainnovacion.com/uploads/revista/pdf/INNOVACION_115_Estudio_de_Mercado.pdf (accessed June 12, 2023).

CEIEC. 2011. Corporate profile (September 1). https://web.archive.org/web/20110901021720/http://www.ceiec.com.cn/english/type/Info.aspx?code=01002 (accessed June 12, 2023).

Cheney, C. 2019. China's digital silk road: Strategic technological competition and exporting political illiberalism. [Issues & Insights Working Paper 19 (WP8)]. Honolulu, HI: Pacific Forum. https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf (accessed November 5, 2023).

Corral-De-Witt, D., E. V. Carrera, J. A. Matamoros-Vargas, S. Munoz-Romero, J. L. Rojo-Alvarez, and K. Tepe. 2018. From E-911 to NG-911: Overview and challenges in Ecuador. *IEEE Access*. 6:42578–91. doi: 10.1109/ACCESS.2018.2858751.

Democratic Staff Report. 2020. The new big brother: China and digital authoritarianism (A Democratic staff report prepared for the use of the Committee on Foreign Relations

United States Senate). https://www.foreign.senate.gov/imo/media/doc/The%20New%20Big%20Brother%20-%20China%20and%20Digital%20Authoritarianism%20-%20SFRC%20Dem%20Staff%20Report.pdf (accessed June 12, 2023).

ECU 911. 2015. Informe: Gestión anual del servicio integrado de seguridad ECU 911 (Report: Annual management of the integral security service ECU 911). https://issuu.com/ecu911/docs/informe_de_gestion2015 (accessed June 12, 2023).

ECU 911. 2019. Plan estratégico institucional 2020-2023 (Strategic institutional plan 2020-2023). https://www.ecu911.gob.ec/wp-content/uploads/2022/02/Plan-Estrat%C3%A9gico-SIS-ECU-911-2019-2023.pdf (accessed June 12, 2023).

El Comercio. 2018. Ministro Navas negó que haya un informe de la contraloría en su contra [Minister Navas denied that there is a report from the comptroller against him]. El Comercio, January 9. https://www.elcomercio.com/actualidad/seguridad/ministro-cesarnavas-niega-informe-contraloria.html (accessed June 12, 2023).

Ellis, R. E. 2021. China's diplomatic and political approach in Latin America and the Caribbean (Testimony before the US-China Economic and Security Review Commission). https://www.uscc.gov/sites/default/files/2021-05/Evan_Ellis_Testimony.pdf (accessed June 12, 2023).

Ellis, R. E. 2022. El avance digital de China en América Latina [The digital advance of China in Latin America]. *Revista Seguridad y Poder Terrestre* 1 (1):15–39. doi: 10.56221/spt.v1i1.5.

Feldstein, S. 2019. The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy* 30 (1):40–52. doi: 10.1353/jod.2019.0003.

Gagliardone, I. 2019. *China, Africa, and the future of the Internet*. London: Zed.

Garrison, C. 2019. "Safe like China": In Argentina, ZTE finds eager buyer for surveillance tech. *Reuters*, May 7. https://www.reuters.com/article/us-argentina-china-zte-insight-idUSKCN1U00ZG (accessed June 12, 2023).

Gonzalez-Vicente, R. 2017. South-South relations under world market capitalism: The state and the elusive promise of national development in the China-Ecuador resource-development nexus. *Review of International Political Economy* 24 (5):881–903. doi: 10.1080/09692290.2017.1357646.

Gravett, W. H. 2020. Digital coloniser? China and artificial intelligence in Africa. *Survival* 62 (6):153–78. doi: 10.1080/00396338.2020.1851098.

Gravett, W. H. 2022. Digital neocolonialism: The Chinese surveillance state in Africa. *African Journal of International and Comparative Law* 30 (1):39–58. doi: 10.3366/ajicl.2022.0393.

Hemmings, J. 2020. Reconstructing order: The geopolitical risks in China's digital silk road. *Asia Policy* 15 (1):5–21. doi: 10.1353/asp.2020.0002.

Herrera-Vinelli, L., and M. Bonilla. 2019. Ecuador-China relations: The growing effect of Chinese investment on Ecuadorian domestic politics, 2007–2016. *Journal of Chinese Political Science* 24 (4):623–41. doi: 10.1007/s11366-018-09588-6.

Hu, R. 2019. The state of smart cities in China: The case of Shenzhen. *Energies* 12 (22):4375. doi: 10.3390/en12224375.

INDEC. 2018. Encuesta nacional de victimización 2017 [National victimization survey 2017]. https://www.indec.gob.ar/uploads/informesdeprensa/env_2017_02_18.pdf (accessed June 12, 2023).

Jepson, N. 2022. Infrastructure-led development with post-neoliberal characteristics: Buen Vivir, China, and extractivism in Ecuador. In *The Rise of the infrastructure state: How US-China rivalry shapes politics and place worldwide*, eds. by S. Schindler and J. DiCarlo, 106–21. Bristol, UK: Bristol University Press. doi: 10.51952/9781529220803.ch008.

Jujuy al Día. 2015. *El gobierno no tiene política de seguridad* [El gobierno no tiene política de seguridad]. *Jujuy al Día*, May 19. https://www.jujuyaldia.com.ar/2015/05/19/el-gobierno-no-tiene-politica-de-seguridad/ (accessed June 12, 2023).

Kassenova, N., and B. Duprey, eds. 2021. *Digital silk road in Central Asia: Present and future*. Cambridge, MA: Davis Center for Russian and Eurasian Studies, Harvard University.

Lio, V. 2015. Ciudades, cámaras de seguridad y video-vigilancia: Estado del arte y perspectivas de investigación [Cities, security cameras and video surveillance: State of the art and research perspectives]. *Astrolabio* 15:273–302. doi: 10.55441/1668.7515.n15.9903.

Löfberg, S. 2008. *Ojos de Águila: Una primera aproximación al sistema de video vigilancia en Quito* [Eagle Eyes: A first approximation to the video surveillance system in Quito]. *Ciudad Segura. Programa Estudios de La Ciudad*. https://www.flacso.org.ec/biblio/catalog/resGet.php?resId=20859 (accessed June 12, 2023).

Lucio Vásquez, A. G. 2020. Evolución del concepto de seguridad en la República del Ecuador: Desde una perspectiva de seguridad nacional hacia la seguridad integral [Evolution of the concept of security in the Republic of Ecuador: From a national security perspective towards integral security]. *Relaciones Internacionales* 43 (43):171–88. doi: 10.15366/relacionesinternacionales2020.43.009.

Menendez, R. 2022. S.3591 - United States-Ecuador Partnership Act of 2022. https://www.congress.gov/bill/117th-congress/senate-bill/3591 (accessed November 5, 2023).

Ministerio de Coordinación de Seguridad. 2011. Plan nacional de seguridad integral (National integral security plan). https://issuu.com/micsecuador/docs/plan_nacional_seguridad_integral (accessed June 12, 2023).

Ministerio de Seguridad de Jujuy. 2016. Proyecto integral Jujuy Seguro e Interconectado [Integral project Jujuy Seguro e Interconectado]. http://seguridad.jujuy.gob.ar/wp-content/uploads/sites/27/2016/11/LICITACION-JUJUY-SEGURO-E-INTERCONECTADO-FINAL.pdf (accessed June 12, 2023.

Ministerio de Seguridad de Argentina. 2022. Homicidios dolosos 2017-2020 [Intentional homicides 2017-2020]. https://estadisticascriminales.minseg.gob.ar/reports/Informe_Homicidios_Dolosos.pdf (accessed June 12, 2023).

Morales, G. 2019. Presentación del plan de trabajo de Jujuy Seguro e Interconectado [Presentation of the work plan for Jujuy Seguro e Interconectado]. https://www.youtube.com/watch?v=Jb9ORPUxva4 (accessed June 12, 2023).

Mozur, P., J. M. Kessel, and M. Chan. 2019. Made in China, exported to the world: The surveillance state. New York

Times, April 24. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html (accessed June 12, 2023).

Polyakova, A., and C. Meserole. 2019. *Exporting digital authoritarianism: The Russian and Chinese models*. Washington, DC: Brookings Institution. https://www.brookings.edu/research/exporting-digital-authoritarianism/ (accessed June 12, 2023).

Saguier, M., and M. F. Vila Seoane. 2022. Argentina and the spatial politics of extractive infrastructures under US-China tensions. In *The rise of the infrastructure state: How US-China rivalry shapes politics and place worldwide*, eds. S. Schindler and J. DiCarlo, 153–66. Bristol, UK: Bristol University Press. doi: 10.51952/9781529220803.ch011.

Sanchez, E. 2022. El 60% de los equipos del ECU 911 necesita renovación [60% of the ECU 911 equipment needs renewal]. *Expreso,* June 3. https://www.expreso.ec/actualidad/60-equipos-ecu-911-necesita-renovacion-128805.html (accessed June 12, 2023).

Secretaría Nacional de Riesgos. 2011. Sistema nacional de comando y control para la seguridad ciudadana SIS911 [National command and control system for citizen security SIS911]. http://app.sni.gob.ec/sni-link/sni/PDOT/SNRG/GALAPAGOS/GALAPAGOS/VARIOS/AUTOCAD/Isla%20San%20Cristobal/PresSIS%20Galapagos.pdf (accessed June 12, 2023).

Shabhaz, A. 2018. The rise of digital authoritarianism (Report: Freedom on the net 2018). Washington, DC: Freedom House. https://freedomhouse.org/sites/default/files/2020-02/10192018_FOTN_2018_Final_Booklet.pdf (accessed June 12, 2023).

TodoJujuy. 2015. Capacitan a operadores del 911. *Todo Jujuy,* March 26. https://www.todojujuy.com/jujuy/capacitan-operadores-del-911-n32613 (accessed June 12, 2023).

UNDP. 1994. Human development report 1994: New dimensions of human security. New York: Oxford University Press. https://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf.

Woodhams, S. 2020. China, Africa, and the private surveillance industry. *Georgetown Journal of International Affairs* 21 (1):158–65. doi: 10.1353/gia.2020.0002.

Xinhua Español. 2016. Presidente Chino promete a Ecuador más apoyo para reconstrucción tras sismo [Chinese President promises Ecuador more support for reconstruction after earthquake]. *Xinhua Español*, November 19. http://spanish.xinhuanet.com/2016-11/19/c_135841469.htm (accessed June 12, 2023).

Appendix 1. Interviews

Code	Interviewee
EC1	Former ECU 911 director
EC2	Former vice-minister of the Defense Ministry
EC3	Former ECU 911 director and former Minister of Coordination of Internal and External Security
EC4	Ecuadorian academic who investigated ECU 911
EC5	Current technical manager of ECU 911
EC6	Senior communications and advocacy specialist at Access Now Ecuador
EC7	Former official of Ecuador's intelligence agency during Correa's administration
EC8	Former vice-minister of the Coordinating Ministry of Security
AR1	Public official at Ministry of Security of Jujuy in charge of JSel
AR2	Representative of opposition political party of Jujuy
AR3	Public official within national government in charge of international funding
AR4	ZTE manager
AR5	ADC researcher (Argentine human rights organization)
AR6	Argentine academic who investigates surveillance