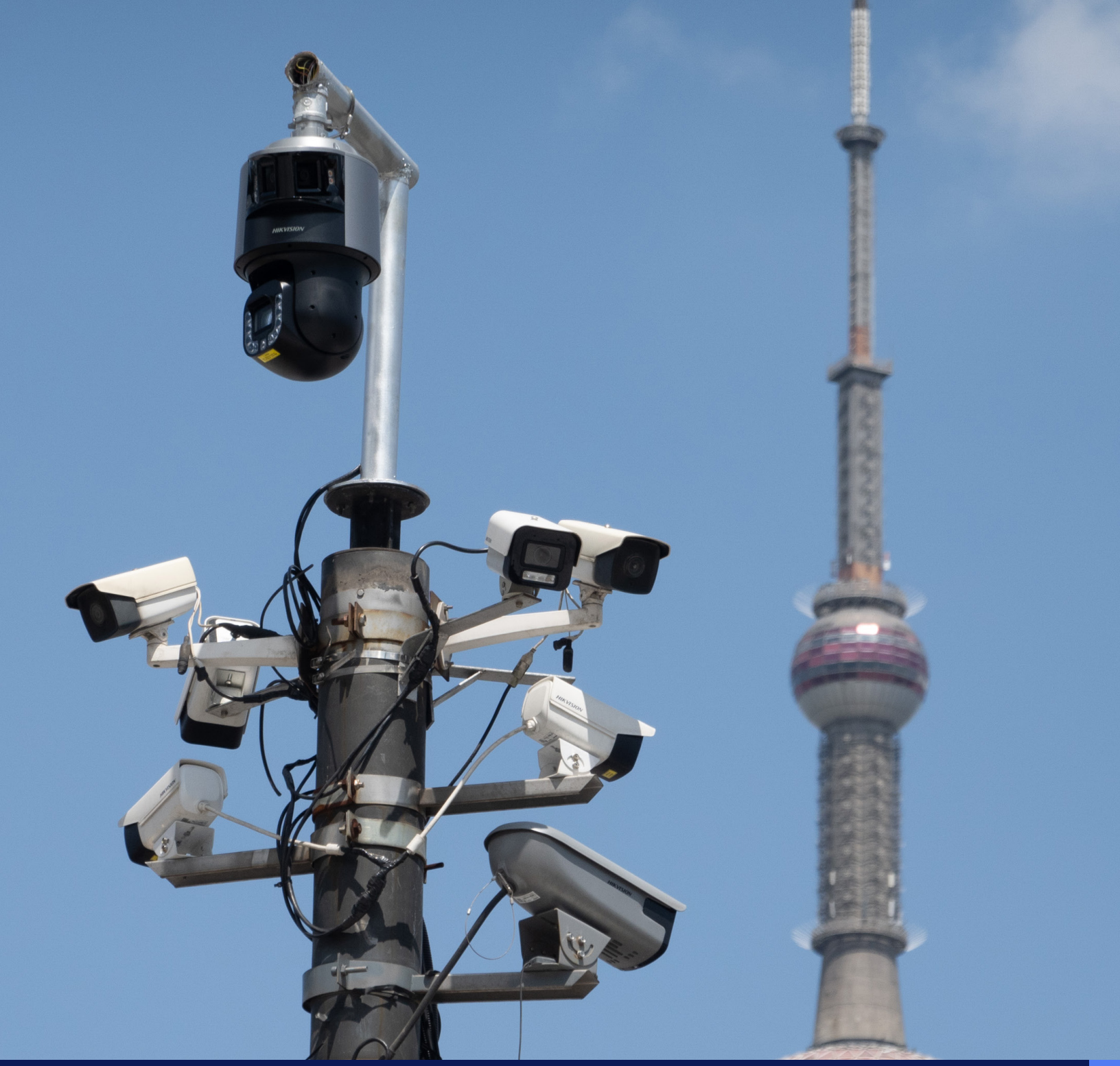


THE GLOBAL EXPANSION OF PRC SURVEILLANCE TECHNOLOGY:

IMPLICATIONS FOR HUMAN RIGHTS AND INTERNATIONAL GOVERNANCE

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

TextOre

The Global Expansion of PRC Surveillance Technology: Implications for Human Rights and International Governance

ACKNOWLEDGEMENTS

This report is a collaboration between the International Republican Institute's Countering Foreign Authoritarian Influence (CFAI) Practice and TextOre. The report was written by TextOre Analysts led by Benjamin Weber under the editorship of former IRI Advisor Matt Schrader. We are grateful to the National Endowment for Democracy for its ongoing sponsorship of this initiative.

Although Mr. Weber was formerly employed by the State Department, his opinions and characterizations in this piece are his own and do not necessarily represent those of the U.S. government.

ABOUT THE CFAI INITIATIVE

Over the past five years, IRI has developed and implemented a framework to build resiliency against growing foreign authoritarian influence and interference through its Countering Foreign Authoritarian Influence (CFAI) practice. Under its Building Resiliency for Interconnected Democracies in Global Environments (BRIDGE) initiative, funded by the National Endowment for Democracy (NED), IRI deploys three-pronged approach to mitigate the impact of Chinese Communist Party (CCP) authoritarian influence on developing democracies:

1. Sharing research on how CCP influence impacts democratic processes with IRI's global network of partners;
2. Equipping local stakeholders with the means to conduct similar research independently, the skills to craft and message targeted advocacy campaigns based on research findings, and the tools and resources to devise and advocate for locally appropriate policy solutions to bolster democratic resilience and counter PRC authoritarian influence;
3. Catalyzing the development and adoption of policy solutions through productive dialogue with stakeholders and policymakers and targeted advocacy campaigns.

By engaging stakeholders across sectors — including government officials, political parties, media, private enterprise, and civil society activists — IRI's work promotes broad awareness of authoritarian tactics and the keys to shoring up vulnerable democratic institutions. The research presented in this report is part of a growing compendium of case studies documenting the CCP's varied authoritarian influence tactics across countries and the elements of effective democratic resilience, which directly informs BRIDGE programming.

ABOUT TEXTORE

TextOre (textore.net) is an open-source intelligence (OSINT) solutions provider with deep expertise in international security and geopolitics, media monitoring and analysis, influence and interference operations, leadership and organization tracking, and geospatial and network analysis. TextOre's work for clients spans multiple areas and languages across the globe, with extensive depth and experience in the China/East Asia and Russia/Eurasia regions.

TABLE OF CONTENT

EXECUTIVE SUMMARY

Countries around the world are increasingly adopting surveillance technology developed in the People's Republic of China (PRC), helping Beijing realize important policy goals. These include normalizing its own surveillance-heavy version of national social control among other nations, having access to "back doors" built into PRC-developed technology to access data from other countries, and influencing international governance of emerging technologies. This report assesses how and to what extent the spread of PRC-developed surveillance technology helps Beijing get closer to the realization of these goals in various countries around the world. It also identifies the PRC state and corporate actors that develop these new technologies and train authorities in other countries on their use.

While the report assesses that there does not appear to be a unified PRC strategy to export tech-enabled repression, China's activities in this sector merit scrutiny for several reasons:

- The PRC and like-minded states are trying to shape emerging international standards in ways that could undermine civil liberties and privacy protections.
- PRC-based surveillance technology companies are among the largest in the world, with large overseas footprints.
- The PRC lacks laws regulating to whom its companies sell surveillance technology, and for what purpose.
- PRC-based companies' inability to refuse the demands of the PRC state make data generated, transmitted by, or stored on PRC-developed surveillance technology more vulnerable to illicit use by PRC security or intelligence agencies.

The report arrives at these conclusions through a three-part analysis. Part 1 examines the PRC's strategies to achieve a leading role in surveillance and other associated technologies, including efforts to shape international rules and technical standards. Part 2 explores the role of PRC-based technology companies, including an effort to evaluate their alignment with state goals. Part 3 examines PRC surveillance technologies through three country case studies: Kyrgyzstan, Ecuador, and Malaysia.

This analysis shows the spread of increasingly global surveillance technology driven by PRC companies' commercial acumen backed by strong state direction and support. The PRC prioritizes sovereign governments' absolute control over surveillance tech and the data it collects, while placing little or no emphasis on protecting citizens from state violations of their privacy. This approach, combined with PRC-based firms' strong appetite for commercial risk, means that China's surveillance companies sell to developing markets often ignored by competitors. Through its technology sales, the PRC is willing to enable repressive state behavior that companies from the United States or Europe might balk at, out of reputational or legal concerns. And while PRC's efforts to achieve a commanding position in international and multilateral standards-setting bodies have not been entirely successful, Chinese companies' market success could set technical standards through sheer dominance of the market. Layered on top of these risks is the ever-present concern that – because PRC firms are unable to deny state demands for their data – the PRC state might misappropriate data collected through PRC-provided surveillance systems abroad, either for espionage or to surveil regime opponents overseas.

KEY DEFINITIONS AND CONCEPTS

The PRC exports two main categories of surveillance technology: to support host-country law enforcement and security agencies; and exports for Smart City programs, which include policing as one element among several. Internationally-recognized definitions of certain key terms are given below:

SMART/SAFE CITY PLATFORMS

The Organisation for Economic Co-operation and Development (OECD) defines Smart Cities as "initiatives or approaches that effectively leverage digitalisation to boost citizen well-being and deliver more efficient, sustainable and inclusive urban services and environments as part of a collaborative, multi-stakeholder process."[1] A 2015 World Bank brief described Smart Cites as possessing two key elements: service provision through integrated data collection from services like transportation and waste collection; and better customer experiences through better communication with service providers.[2]

FACIAL RECOGNITION SYSTEMS

The European Union (EU) defines facial recognition as "the automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorisation of those individuals."[3] The American Civil Liberties Union (ACLU) describes facial recognition systems as "built on computer programs that analyze images of human faces for the purpose of identifying them. Unlike many other biometric systems, facial recognition can be used for general surveillance in combination with public video cameras, and it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject." The ACLU warns that the "biggest danger is that this technology will be used for general, suspicion less surveillance systems."[4]

SMART POLICING

Smart policing is an element of a Smart City, spanning areas from traffic enforcement to predicting and responding to criminal activity. The U.S. Department of Justice's Bureau of Justice Assistance contends that "smart policing represents a strategic approach that brings more 'science' into police operations by leveraging innovative applications of analysis, technology, and evidence-based practices."[5] Smart policing is one of the most controversial elements of the Safe City platform, sparking extensive debate about the balance between the capacity of advanced surveillance technologies and their impact on civil liberties. In particular, there are questions over who can access, and for what purpose, data captured by routine surveillance. The potential for PRC security agencies to force PRC-based companies to share data generated, transmitted by, or stored on technology they develop makes these questions particularly acute in their case.

PART 1: THE PRC AND THE GLOBAL MARKET FOR SURVEILLANCE TECHNOLOGIES

A CONSTELLATION OF CONCERNING FACTORS

Research conducted for this report report identified a collection of interrelated risks associated with growing commercial success around the world by PRC-based surveillance technology companies. Concerns include:

1. PRC efforts to capture the international market for surveillance technology and, in so doing, set international standards through dominance of the market.
2. PRC initiatives to shape international technical standard setting bodies like the International Telecommunications Union.
3. PRC initiatives to shape international technological governance in bodies like the United Nations.
4. PRC state financial support for the export of surveillance technology.
5. The lack of any human rights-related export controls or end-user vetting in the PRC export system.
6. Authoritarian leaders' acceptance of the sophistication and efficacy of the PRC's surveillance systems.

Growing PRC influence on the international sale and use of surveillance technology could therefore make it harder to reverse existing trends, wherein many repressive governments have easy access to surveillance technology with little real oversight of its use. In addition, it could increase the risk that Beijing could turn PRC-developed surveillance tech to malignant ends, such as intelligence gathering, commercial espionage, or monitoring regime opponents overseas without other governments' knowledge or consent.

Drive to Capture the Market

Publicly released PRC documents underscore China's interest in building and marketing emerging technologies as part of the "great rejuvenation of the Chinese nation" (a term that describes Beijing's desire to catch up with and surpass the power and development level of countries like the United States).[6] In its Made in China 2025 strategy, the CCP lays out its ambition to "build China into a manufacturing powerhouse that leads the development of the global manufacturing industry, with a dominant position in a number of cutting-edge technical fields."[7] The official news service Xinhua boasted in September 2022 that China's digital economy had reached USD7.1. trillion, making it the second largest participant in a global market worth USD38.1. trillion.[8]

PRC rhetoric about the promise of technological advancement, which accompanies and promotes this strategy, features three primary narratives. The first is an almost messianic view of the potential for technology to improve lives, framed in the context of an interconnected and collaborative world. This theme is very much at the center of Chinese President Xi Jinping's vision of a Digital Silk Road (DSR) component to the PRC's larger Belt and Road Initiative. Speaking at the 2017 Belt and Road Forum, Xi sketched an expansive vision of cutting-edge technologies along the DSR, integrating these technologies into industry and finance, and training young people to reap the benefits.[9] In its 14th Five-Year Plan (2021), the PRC promised to "provide technology, equipment, services, and other digital assistance to underdeveloped countries and allow all countries to share the dividends of the digital age," adding that "we will actively promote online cultural exchanges and mutual learning."[10] These themes of common objectives have also been a feature of the annual Wuzhen Summit, an effort to position China as a center of international technology collaboration and innovation.[11]

The second narrative casts the PRC as a critical competitor in a market that has been unfairly dominated by Western companies. A document titled "China's Positions on International Rules-making in Cyberspace," released by the Ministry of Foreign Affairs (MFA) on 20 October, 2021, contends that current management of the internet is "unbalanced and unjust."[12] In a speech to the China Academies of Science and Engineering earlier the same year, Xi warned that, "scientific and technological innovation has become the main battlefield of the international strategic game, and the competition around the commanding heights of science and technology is unprecedentedly fierce. We must maintain a strong sense of vigilance and make adequate preparations in thoughts and work."[13] China has therefore invested heavily in indigenous innovation while emphasizing internationally the "unjust" market dominance of US- and EU-based companies, along with the risk that those firms will grant access to data collected overseas to foreign security services. In particular, Beijing has repeatedly cited close collaboration between U.S. intelligence agencies and some U.S. telecommunications companies as justification for prohibiting the export of data generated inside China.

The final narrative focuses on the risks the PRC views as inherent to the internet and social media, abetted by hostile foreign governments: terrorism and foreign meddling in domestic political processes under cover of "human rights." As Xi put it at the September 2022 Samarkand Summit of the Shanghai Cooperation Organization (SCO) – a multilateral convening organization begun by the PRC as an alternative to western-led organizations in China's near abroad -- "we should guard against attempts by external forces to instigate 'color revolution,' jointly oppose interference in other countries' internal affairs under any pretext, and hold our future firmly in our own hands."[14] The final summit communique connected these dots, stressing absolute state sovereignty over the flow of data within national borders, and emphasizing that international data and cyber governance issues should be governed by the UN (a preferred forum for China and many like-minded countries).[15]

Focus on Setting International Technical Standards

Alongside its efforts to capture the market, the PRC has also sought to set global technical standards on technology use. Efforts to influence standard setting in international fora served two goals for the PRC: 1) creating a pathway to advance the "China model" of governance on issues such as digital censorship and surveillance; and 2) providing PRC companies with a strategic advantage, since industry standards can mandate the use of patented technologies. Thus, as far back as 2015, the Made in China 2025 strategy made the international promotion of PRC-developed technical standards a national goal.[16] March 2020 instructions from the Standardization Administration of China said the PRC state and corporations should "accelerate the conversion of China's advantageous technical standards into international standards and continue to promote the release of Chinese versions of [International Standards Organization] and [International Electrotechnical Commission] standards."[17] As the Asia Society Policy Institute (ASPI) observed, "by exporting its technologies, signing memoranda of understanding (MOUs) for the harmonization of standards, and developing other standards harmonization mechanisms, Beijing is propagating its own technology standards in project host states."[18]

Achieving these goals involves engagement at the ISO and at technical standards bodies, including the International Telecommunication Union (ITU), 3rd Generation Partnership Project (3GPP), and the Institute of Electrical and Electronics Engineers (IEEE). A number of observers have sounded an alarm at the rise of PRC influence in these bodies.[19] ASPI noted that the PRC and companies receiving state support can subsidize participation in these bodies, strengthening China's ability to set the agenda.[20] In addition, ASPI noted China's ability to make sure that PRC participants vote as a bloc.[21] China is explicit that its goal is to lead these organizations, but while TextOre research did find extensive efforts by PRC companies to engage those bodies on standards-setting, it did not find a dominant PRC presence at the major international technology governance organizations.[22] This may change if PRC companies continue to expand their market position.[23]

International Technology Governance

The PRC state has consistently identified the UN as the appropriate forum for international technology rules-making.[24] China seems to be equally worried (a) that foreign technology companies operating in China will accede to foreign government demands to provide data collected in China; and (b) that unregulated free expression on the internet could destabilize CCP one-party rule. The PRC has expressed these concerns in public statements defining its position on international technological rules-making.

For example, the *International Strategy of Cooperation on Cyberspace* released by the PRC Ministry of Foreign Affairs in 2017, argues against "interference in other countries' internal affairs by abusing ICT and massive cyber surveillance activities."[25] The document supports the "discussion on privacy protection at the UN General Assembly and the Human Rights Council, and calls for establishing relevant principles for protecting individual privacy in cyberspace." [26] The strategy makes no mention of human rights or freedoms of speech, expression, or association. Instead, the document explicitly balances "[citizens'] rights to be informed, to participate, to express and to supervise" against the statement that "freedom and order are both necessary in cyberspace."[27] This position is consistent with PRC domestic governance, in which the state claims to uphold freedoms of speech while ruthlessly suppressing free expression in the name of "order" or "stability."

China has sought to build a coalition of like-minded states to advance these views in the UN, including through the SCO. In January 2015, the Permanent Representatives to the UN of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan (all SCO member states) submitted a draft international code of conduct for information security to the UN Secretary General. The text downplays the importance of human rights in several ways:

- Language supporting "respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries." [28] This may, at first glance, seem neutral or even respectful of fundamental freedoms. However, the PRC often responds to criticism of its repressive policies with demands that other countries respect the "diversity" of its "distinct" system, in an attempt to undermine the idea that freedom of speech or association are "universal" human rights.
- The code calls on states "not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability." It also calls for efforts "in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds." [29] The PRC state routinely treats fact-based criticism of its regime as an existential threat to national stability, dealing harshly with civil society organizations and groups advocating for the rights of Uyghurs and Tibetans. While the code follows the UN Panel of Governmental Experts in averring that citizens' rights offline should also be protected online, and professes "to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information," it also invokes an expansive application of Article 19 of the International Covenant on Civil and Political Rights, which allows governments to impose restrictions for respect of the rights or reputations of others, or for the protection of national security, or of public order, or of public health or morals.[30]

PRC State Support for Export of Surveillance Technology

PRC surveillance tech companies are competitive participants in global commercial markets, as is discussed in detail in Part 2 below. However, state support for the industry plays an important role in its global expansion, enabling exports through generous financing. In its 2017 *International Strategy of Cooperation on Cyberspace*, the PRC explicitly pledged to support companies as they compete in international markets, particularly in developing countries.[31] Significant state support for PRC-based exporters of surveillance technology is problematic, since companies that accept such financing may be more willing to promote the PRC state's repressive international technological agenda.

To quantify the degree of this support, TextOre examined a comprehensive dataset on PRC state financing of projects overseas assembled by a team at the College of William & Mary, and found state support for the export of surveillance technology in the form of outright grants (often from the Ministry of Commerce), standard and concessionary loans (from the Ministry of Commerce, the Export-Import Bank of China, and China Development Bank), and preferred buyer's credits from the Export-Import Bank. TextOre research did not, however, identify a preference for financing surveillance technology exports *over* other exports.

The PRC's Insufficient Technology Export Control Regime

TextOre's examination of PRC export laws and regulations found few controls on the export of surveillance technology.[32] Despite a significant revision of the PRC's primary export control law in 2020, the country does not have any laws restricting the export of technologies to purchasers who might use them for political repression, or other violations of human rights. Rather, the *Export Control Law of the People's Republic of China* (2020 edition) stipulates that exporters must apply for licenses for items that:

1. endanger national security or national interests.
2. can be used for the design, development, production or use of weapons of mass destruction and their delivery vehicles; or
3. are used for terrorist purposes.[33]

Many companies, including Western businesses, compete in the surveillance technology market, whose general absence of legal and regulatory has been criticized by the UN Human Rights Council, NGOs, and public observers. In 2019 the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression called for a moratorium on the international sale of surveillance equipment pending robust standards informed by the UN Guiding Principles on Business and Human Rights,[34] saying:

> "Surveillance of individuals – often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression – has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings.[35]"

In response to these concerns, some countries are adopting national standards. Both the U.S.[36] and the EU[37] have adopted new control measures, including banning surveillance technology exports to countries under arms embargos. They also coordinate through the U.S.-EU Trade & Technology Council Export Control Working Group.[38] In 2017, the multilateral Wassenaar Arrangement adopted some controls impacting surveillance technology,[39] but the PRC is not a member.[40] Press and civil society groups have also provided much-needed scrutiny, and their attention has increased pressure on governments to adopt stricter controls. However, more work is clearly needed: in August 2021, Special Rapporteurs and Independent Experts convened as part of

the UN's Human Rights Council repeated the 2019 call for a moratorium pending development of "a robust regulatory framework to prevent, mitigate and redress the negative human rights impact of surveillance technology."[41]

The PRC legal system has made strides in protecting individuals *inside* China against the misuse of surveillance technology by entities *other than the state* – one recent landmark court ruling required technology companies to justify their use of facial recognition and set specific rules about consent agreements.[42] However, no regulations or court rulings have touched the PRC state's unlimited capacity to surveil individuals or to collect their private data, which itself relies on the cooperation of major PRC technology companies.

Exporting Digital Repression?

Journalists, researchers, and activists have extensively documented the effectiveness of the PRC's digital surveillance at suppressing dissent. This, combined with the growing global footprint of PRC surveillance technology companies, has given rise to concern that China might seek to export this "success" to other authoritarian regimes, who would be ready adopters of PRC-developed tools of digital repression.[43]

In this context, the PRC's development of surveillance technology designed to identify supposedly "problematic" ethnic groups on the basis of their distinct appearance is particularly concerning. The UN Special Rapporteur's 2019 report observed that:

> Credible reporting suggests that the Government of China, using a combination of facial recognition technology and surveillance cameras throughout the country, "looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review."[44]

TextOre research has not found evidence that PRC-based companies sold surveillance technology to other authoritarian regimes specifically to identify and repress ethnic minorities. However, recipients of PRC surveillance technology have used it toward authoritarian ends with support from PRC-based companies. In two cases documented by The Wall Street Journal, in Uganda and Zambia, Huawei and other PRC-based companies have cooperated with authorities in other countries to suppress activity by opposition parties and independent political activists. In Uganda, authorities requested and received technical assistance from Huawei in cracking the encrypted communications used by opposition candidate Bobi Wine, while in Zambia, the company helped authorities to access the social media accounts of opposition media in the name of combatting "fake news."[45]

PART 2: PRC SURVEILLANCE FIRMS RESPOND TO STATE INCENTIVES, GROWING GLOBAL MARKET

PRC-based firms need no encouragement from the state to maximize their profits by selling their technology abroad. However, contrary to public statements by the PRC and by many of the companies involved, TextOre's examination of open-source evidence suggests that PRC-based technology companies do indeed heed state direction at home while taking advantage of a permissive regulatory environment abroad.

As is the case with PRC-based companies in many industries, it can be difficult to untangle the impacts of market incentives and state support on the behavior of PRC-based developers of surveillance technology. While the PRC state clearly has an export promotion strategy which focuses on growing national brands, it is also important to note that PRC-developed technology is in demand, both at home and abroad. New York-based risk advisory firm Eurasia Group notes that "Chinese companies are primarily responding to—and benefitting from—demand in developing countries for more telecommunications infrastructure, which often includes the security components of smart cities. The Chinese technology stack is offered as a package deal, encouraging reliance on PRC-based technologies. These dependencies have the potential to make it more difficult for other technology companies to do business in BRI [Belt and Road Initiative] countries."[46] Privacy International, a pro-privacy charity based in the U.K., views PRC-based tech firms initiatives as market-driven, noting that "in reality, PRC-based surveillance companies, including those that are partially state-owned[47]... function as commercial actors abroad and do not receive direct state support to facilitate a vast majority of their commercial transactions... Hikvision, Dahua, and Uniview dominate the international market for CCTVs, in large part because their surveillance equipment is cheaper than international competitors and of comparable quality."[48]

CORPORATE-STATE CONNECTIONS

Some of China's largest makers of surveillance technology deny that they cooperate inappropriately with the PRC state. Remarks by Huawei CEO Ren Zhengfei in a June 2019 interview with the *Financial Times* are typical of many such companies. Ren refuted U.S. claims that the company has ties to the PRC's People's Liberation Army (PLA) and Ministry of State Security (MSS), stating that "[Huawei's] relationship with the Chinese government is very simple: We abide by the law and pay taxes in accordance with the law."[49]

Despite this, outside reporting indicates that major PRC technology companies such as Baidu and Alibaba do cooperate very closely with PRC intelligence agencies, providing them with data storage and analysis capabilities to supplement their in-house tools.[50] Moreover, while Beijing has nominally prohibited PRC tech companies such as Huawei from installing "backdoors" that would allow the country's intelligence agencies clandestine access to PRC-developed technology,[51] governments and NGOs around the world have documented numerous cases of Huawei equipment with backdoors or pre-loaded with malware.[52] The unique nature of state-corporate relations in China all but ensures close coordination on these issues.

The close nexus between the PRC state and surveillance technology companies is exemplified by companies' willingness to develop technology to automatically identify and track members of the Uyghur ethnic group. (The PRC state has targeted Uyghurs with a surveillance technology-driven campaign of imprisonment and reeducation that credible outside observers have labeled genocide.[53]) Hikvision, a state-owned company that sells video surveillance equipment, unintentionally revealed an "ethnic minority" detection capability during the 2018 AI Cloud World Summit in Hangzhou, while in 2019 Hikvision marketed a "smart" camera that could identify "the racial attributes of the analyst's target," such as Uyghur or Han.[54]

Similarly, a 2021 report by surveillance technology group IPVM identifies Huawei, Hikvision, Alibaba, Baidu, and Dahua, as some of the PRC-based surveillance technology companies designing tools to identify certain races or ethnicities. IPVM uncovered one national standard issued in 2017 that "requested face recognition systems detect 'personal attributes' including 'ethnicity' and 'skin color,'" noting that while such features may be listed as "recommended" they are, in fact, treated as "mandatory."[55] According to a confidential 2018 Huawei document, a Megvii, a PRC-based tech firm, facial recognition system function designed to raise an alarm when it identifies a member of the Uyghur minority had "passed inspection" for its compatibility with Huawei systems, and thus could be included in packages of surveillance technology sold by Huawei.[56] Huawei and the Chinese Academy of Sciences submitted a patent application describing a facial recognition system designed to identify ethnically Han and Uyghur people in surveillance footage; a similar patent application for a Megvii system noted its ability to "directly connect to the facial recognition that has been built by the public security organ."[57]

INDUSTRY AND SMART CITY TECHNOLOGY

Many PRC-based ICT companies trumpet their successes in helping build so-called "Smart Cities." The PRC is a major player in the global market for Smart City technology, in large part as a response to state demands for digital systems to surveil and manage urban areas. These tools are dual-use by nature; although they can be used for benign purposes such as traffic management or infrastructure maintenance, privacy and surveillance advocates point out they are also powerful potential tools of authoritarian control. The PRC state has pioneered both uses, through deep cooperation with PRC-based developers of Smart City technology.

Huawei positions itself as a leader in the field (its marketing materials sometimes substitute the term "safe city" for smart city). According to Huawei marketing materials, "Smart Cities enhance city management and promote technological innovation… [by] using advanced technologies—including 5G, Artificial Intelligence (AI), Internet of Things (IoT), cloud computing, and big data analytics."[58] As of November 2021, Huawei claimed it had built over 160 smart cities in over 100 countries.[59] A 2019 analysis by the Center for Strategic and International Studies (CSIS), a Washington DC-based think tank, strengthened concerns that Huawei may be facilitating the diffusion of this technology to non-democratic regimes in the Global South. CSIS analyzed Huawei's foreign smart city agreements in 52 countries, and found that "71 percent of Huawei's safe city agreements are in countries with an average Freedom House rating of 'partly free' (44 percent) or 'not free' (27 percent) … 59 percent of Huawei's agreements are with countries in Asia (37 percent) or sub-Saharan Africa (22 percent)," and "71 percent of Huawei's agreements are in lower-middle-income (42 percent) and upper-middle-income (29 percent) countries."[60]

TRAINING IN SURVEILLANCE TECHNOLOGIES

PRC-based ICT companies train foreign clients, including law enforcement and security agencies, on the use of surveillance technology. Although this is common commercial practice for many providers of surveillance technology, PRC-based providers' tight integration with PRC state priorities makes their provision of this training particularly problematic.

Major PRC-based developers of surveillance technology providing this form of training include:

Meiya Pico

Meiya Pico, a Chinese cybersecurity company, claims to have trained over 50,000 law enforcement officers, primarily from countries in the Global South.[61] In 2002, the company also founded the Meiya Pico Information Security Academy in Xiamen and claims that, as of 2018, its 60 instructors trained over 110,000 people in over 2,000 sessions, including participants from ASEAN countries, Bangladesh, and China's own national police force, the Ministry of Public Security.[62] In October 2019, the U.S Department of Commerce placed Meiya Pico on its Entity List for complicity with human rights violations in Xinjiang, prohibiting the company from transacting with U.S. businesses and persons.[63]

Huawei

Huawei runs a training program through its Seeds for the Future, which offers ICT programming to foreign students.[64] Huawei also does international outreach at conferences; the company held a Safe City Africa Summit directed toward government officials in Cape Town in April 2015., followed by one in Dubai two years later.[65] [66]

Hikvision

Hikvision offers virtual certification programs directed at security technicians, from people just beginning their careers in security to managers. The certifications appear to be directed at corporate rather than government clients.[67] In March 2021, Hikvision hosted the 2021 AI Cloud Summit in Hangzhou with the theme of "cooperatively building Smart Cities (sic) and empowering digital enterprises."[68]

PART 3: CASE STUDIES

The three case studies below, Kyrgyzstan, Ecuador, and Malaysia, show how countries from a broad range of geographic locations, and with very different relationships with the PRC, can nonetheless end up availing themselves of PRC surveillance technology in ways that have raised marked concern among activists and observers. Key among all these studies is the fact that none of the governments in question were *pushed* by Beijing to misuse the technology. Rather, they simply made use of the technology and training on offer.

ECUADOR

Ecuador Snapshot

Freedom House Total Score	71/100 (Free)[69]
Freedom on the Net Score	62/100 (Partly Free)[70]
Freedom House Determination	Free[71]
Diplomatic Relations with the PRC Started	1980[72]
BRI Initiative Signed	2018[73]
Status of Extradition Agreement with the PRC	Signed in 2016, not ratified[74]
Host Government Under U.S. Sanctions? (i.e., barred from USG assistance in security)	No[75]

As early as 2008, the Ecuadorian government sought out PRC support to develop surveillance infrastructure, largely focused on ECU-911, a nationwide system of surveillance cameras built by Huawei and China National Electronics Import & Export Corporation (CEIEC) and deployed throughout the country, ostensibly to fight crime. Despite claims by both PRC and Ecuadorian officials that the system has reduced crime,[76] researchers remain skeptical,[77] and civil rights organizations have claimed that previous Ecuadorian presidential administrations used the system to target human rights activists.

According to a report published by Harvard University's Davis Center for Russian and Eurasian Studies, "China treated Ecuador as a flagship program to see how effective and profitable exporting digital surveillance could be and found a high demand from the developing world."[78] As noted in the report – at least from the PRC's perspective -- the model has proven successful and "Ecuador will continue to be the litmus test for predicting the trajectories of similar states that seek the benefits of improving suppressive capacity through technology." In this context, it is perhaps noteworthy that the ECU-911 failed to avert a catastrophic upsurge in violent crime in the country, that began in 2021 and shows little sign of abating.[79]

Police Training

Ecuador and the PRC cooperate on issues of law enforcement, combatting drug trafficking, and smuggling.[80]Ecuadorean participation in PRC police training programs is focused on addressing drug trafficking which, along with fighting crime and disaster relief, was touted as a primary benefit of Ecuador's surveillance infrastructure prior to a recent surge of drug-related violence in the country.[81]

Ecuador sent law enforcement officers to Chinese-language courses at Beijing Foreign Studies University in 2009. [82] The program is a year-long program, with training focused on combating drug trafficking, smuggling, terrorism, and communications fraud.[83] Mid- to high-level Ecuadorian police officers took an advanced course at Zhejiang Police College, that included visits to local police stations, as well as Hikvision's headquarters in Hangzhou.[84]

ICT Companies

Consecutive Ecuadorian governments have reached out to PRC officials and ICT companies in developing its surveillance systems. After the Ecuadorian government launched pilot programs for the Eagle Eyes System [Sistema Ojos de Águila] in Quito and Guayaquil in 2002, a delegation traveled to Beijing to inspect surveillance for the 2008 Summer Olympic Games.[85] In 2011, faced with high crime rates, then-President Rafael Correa sought the help of PRC military attachés and bypassed public bidding to secure a PRC state-funded surveillance system, ECU-911, in exchange for Ecuadorian oil.[86] Correa's successor, Lenín Moreno, accused Correa's administration of using the system in "perverse" ways to spy "on political adversaries and citizens (whom) they wanted to put pressure on."[87] But as Moreno's administration investigated the allegations, ECU-911 surveillance footage sharing with domestic intelligence reportedly continued.[88]

ECU-911 centers across the country are equipped with products and services from Huawei and CEIEC, and Ecuadorean leaders have been quick to praise the companies.[89] Following a devastating April 2016 earthquake in the country's northwest, Ecuadorian Security Minister César Navas thanked CEIEC for its work on the ECU-911 system, which he credited with a major role in the rescue effort.[90] Correa reiterated such appreciation to Xi during a November 2016 visit to the ECU-911 headquarters, where the two leaders inaugurated an artificial intelligence lab.[91] In a January 2015 meeting with Huawei Rotating CEO Guo Ping, Correa expressed his gratitude for the company's investments and his hope for continued support.[92] Correa and Guo also discussed youth training programs, which Huawei initiated at several Ecuadorian universities in November 2015.[93] Moreno offered similar remarks of gratitude and hope during a December 2018 meeting with Huawei Vice President of Public Relations Xue Man. Visiting the company's research and development center in Beijing, Moreno learned about Huawei's Smart City and Safe City products and met with Ecuadorians studying in China as part of Huawei's Seeds for the Future program.[94]

Despite such praise, Ecuador's comptroller general alleged in 2017 that PRC state-owned companies including CEIEC overcharged the government by $32 million,[95] and civil society groups have raised the alarm over potential misuse of ECU-911 technology that could infringe on citizens' basic rights. According to a November 2016 report by the Quito-based digital rights group Usuarios Digitales (Digital Users), ECU-911's Deputy Director of Technology and Innovation Antonio Ruales confirmed the use of facial recognition technology. Citing ECU-911's previous acquisition of Russian vocal and facial recognition technology and its use in southern Ecuador to monitor large public events, the group expressed concern that the technology could be used to identify and target regime opponents.[96] In June 2022, 27 civil society organizations signed a statement decrying human rights violations through surveillance systems such as ECU-911, citing incidents such as the installation of Hikvision cameras outside of the headquarters of a prominent indigenous rights' advocacy organization.[97] Ecuadorian journalist and activist Martha Roldós notes a lack in "capacity to demand information from China."[98] The same report noted that Mario Pazmiño, a retired army colonel and critic of the Correa administration, claims that the secret police detail that used to follow him has been replaced by an ECU-911 camera installed outside his home.

KYRGYZSTAN

Kyrgyzstan Snapshot

Freedom House Total Score	27/100 (Not Free)[99]
Freedom on the Net Score	53/100 (Partly Free)
Freedom House Determination	Not Free
Diplomatic Relations with the PRC Started	1992[100]
BRI Initiative Signed	2013[101]
Status of Extradition Agreement with the PRC	Signed in 1998, effective in 2004[102]
Host Government Under U.S. Sanctions? (i.e., barred from USG assistance in security)	No[103]

Kyrgyzstan is a founding member of the SCO, with an ambitious technology component to its development agenda that has included outreach to partners around the world, and close security relationships with Russia and the PRC. Kyrgyzstan's reliance on PRC-developed surveillance technology has raised significant human rights concerns. Huawei and CEIEC have both curried favor with the Kyrgyz government by helping build the country's digital infrastructure and by installing surveillance cameras with facial recognition technology at no extra cost. Local activists and NGOs have voiced concerns about backdoors in the hardware and potential infringement of Kyrgyz citizens' privacy (see ICT section below), in part because the government has embraced the use of PRC-provided products while offering few details regarding where data generated inside Kyrgyzstan will be stored and who will have access to it. These concerns nevertheless do not appear to have meaningfully impeded the companies' progress. This, combined with cooperation between Kyrgyz and Chinese police forces on "counterterrorism" (often used by the PRC to mean monitoring and harassment of Uyghurs in countries bordering China), mean that Kyrgyzstan is likely to remain at high risk for misuse of PRC-provided surveillance technology.

Police Training

PRC police have trained Kyrgyz public security officers on counterterrorism, which Kyrgyzstan's government cites to justify its collaboration with PRC-based ICT companies. (Kyrgyzstan shares a long border with Xinjiang.) TextOre research did not uncover examples of Kyrgyz authorities using PRC-provided training to target border crossers with surveillance technology from China. However, border control cooperation between the two countries has raised concern. China and Central Asia researcher Niva Yau cites examples of Kyrgyz security personnel circumventing protocols and granting PRC officials' requests to return Uyghurs crossing the border. Yau posits that the "strong relationship" between the two sides has been "shaped during training programs in China."[104]

PRC training of Kyrgyz police dates to as early as October 2009, when 15 countries sent law enforcement personnel to Chinese language courses at Beijing Foreign Studies University.[105] Shandong Police College – located in the PRC province of Shandong -- has also hosted several counterterrorism training sessions for foreign security personnel, with curricula including digital surveillance. Trainings in 2012, 2015, and 2018 included a focus on transnational terrorism, "information-guided policing," cyberterrorism countermeasures, an advanced SCO-organized course on counterterrorism, and another course on what the PRC calls the "three evils" (terrorism, separatism, and religious extremism).[106] This combination of subjects shows strong willingness on the part of Kyrgyz police to engage with PRC security and policing priorities.

ICT Companies

PRC-based ICT companies operating in Kyrgyzstan, including Huawei, CEIEC, and Meiya Pico,[107] tailor their products and services to fit buyers' needs. The Kyrgyz government has cited counterterrorism, public safety, and digital infrastructure as reasons to work with foreign providers of ICT and surveillance technology.

In a June 2017 meeting with then-President Almazbek Atambayev's Chief of Staff Sapar Isakov, Huawei expressed its readiness to support Kyrgyzstan's Taza Koom digital transformation.[108] After signing an agreement with Huawei in January 2018 to build Smart City infrastructure in Bishkek, Kyrgyzstan's capital, and one other city, the Kyrgyz government stated that the project would "effectively fight against criminal and terrorist threats" and said that Huawei would be required to comply with "personal data protection and cybersecurity requirements in accordance with the law of the Kyrgyz Republic."[109] The agreement further stipulated that two other companies – PRC-based Beijing China Veterans Lingxin Capital Management and Iran-based Aka Minerals and Mining LLC – would train Kyrgyz officials on how to use the new systems.

Although six months later, for unclear reasons, the Kyrgyz government set aside its agreement with Huawei, choosing instead to turn to the Russian surveillance equipment developer Vega,[110] Huawei has continued to play a significant role in the country's surveillance infrastructure development. In October 2019, Huawei took part in opening a Bishkek police command center equipped with facial recognition technology supplied free of charge by CEIEC.[111] In a May 2021 meeting with Kyrgyzstan's Minister for the Promotion and Protection of Investments, Huawei's representatives proposed creating a data processing center combining Kyrgyzstan's separate state information systems into one – meaning, essentially, that the systems through which all Kyrgyz state data was transmitted, stored, and accessed would be built by Huawei.[112]

After Vega installed traffic cameras in 2018, CEIEC agreed to integrate a network of surveillance cameras with facial recognition technology at no additional cost to Kyrgyzstan. According to Kyrgyzstan's Ministry of Internal Affairs, the March 2019 agreement with CEIEC "is in the public domain and is not secret.... The Chinese company is responsible for the delivery of equipment, installation and configuration in the command center, and provision of advisory services for the installation of peripheral equipment. The project is being implemented without spending the state budget of the Kyrgyz Republic through international cooperation."[113]

The facial recognition software has raised concerns among civil rights activists in Kyrgyzstan, specifically regarding foreign access to data and the potential targeting of activists. According to Tattu Mambetalieva[1] of Kyrgyzstan's Civil Initiative on Internet Policy,[2] "all Chinese technology comes with 'open ports' because Chinese companies need to update the software remotely. Otherwise, it would be too costly for them. So there is a big question about whether they'll have access to the [CCTV] data."[114] "Accordingly, there is a very big risk that they, having delivered such a product to us, ...will have access to this data."[115] The Civil Control Committee, a group of over 70 NGOs monitoring government projects, has therefore called for a moratorium on the use of facial recognition technology.[116] Dinara Osharukhunov,[3] a member of the Committee adds that "[i]t is quite possible that law enforcement agencies can provide and even blackmail and say that they will collect (information), and this will be used against a civil activist, against any political opponent of the authorities."[117]

1 Татту Мамбеталиева
2 Гражданская Инициатива Интернет Политики
3 Динара Ошурахунова

MALAYSIA

Malaysia Snapshot

Freedom House Total Score	51/100 (Partly Free)[118]
Freedom on the Net Score	58/100 (Partly Free)[119]
Freedom House Determination	Partly Free[120]
Diplomatic Relations with the PRC Started	1974[121]
BRI Initiative Signed	Yes
Status of Extradition Agreement with the PRC	None observed
Host Government Under U.S. Sanctions? (i.e., barred from USG assistance in security)	No[122]

Malaysia's relationship with the PRC is complex, involving mature economic ties coupled with political concerns regarding the South China Sea and China's treatment of the Uyghurs (although the Malaysian stance on this issue has been inconsistent). Malaysia is the most economically and technologically developed of the three case countries and is keen to develop Smart Cities using advanced technologies, including from PRC-based firms. Compared to Kyrgyzstan and Ecuador, Malaysia appears to be less reliant on PRC-based ICT companies for surveillance infrastructure, from both a financial and a technological standpoint.

However, despite close collaboration between Malaysian and PRC law enforcement bodies on counterterrorism and border control training, the PRC has not always been able to count on the cooperation of Malaysian governments on issues such as the extradition of Uyghurs. Malaysian officials have also expressed concerns about tech giants such as Huawei while insisting on the integrity of their country's security standards in its procurement processes. Moreover, as argued by American anthropologist Darren Byler there are deep divisions among Chinese Malaysians with "resistance to new infrastructure development among some who see it as Chinese state overreach into Malaysian society."[123] Nevertheless, under the leadership of politicians such as Deputy Prime Minister Ahmad Zahid bin Hamidi, who called for Malaysia to emulate China's use of surveillance and bilateral exchanges on deradicalizing terrorist suspects,[124] Malaysia has participated in police training in China and collaborated with PRC-based ICT firms on building surveillance infrastructure across the country.

Police Training

The Malaysian government has shown interest in PRC counterterrorism and counter-radicalization techniques and has sent personnel to PRC training courses on border control, anti-drug trafficking, and counterterrorism. In 2017, on a visit to promote bilateral cooperation on counterterrorism, policing, and surveillance, Deputy Prime Minister Zahid met with a number of senior PRC security and policing officials.[125] During a press conference at the conclusion of the visit, Zahid said that China agreed to the possibility of advanced border control system technology transfer, and would host a delegation of Malaysian representatives of the National Security Council, the National Border Security Agency, the Immigration Department, and the police.[126] Ahmad Zahid also claimed that the PRC was interested in exchanges between its officers and Malaysian counterparts on rehabilitation related to terrorism. "With regard to rehabilitation," he said, "actually Malaysia too can share its experience in deradicalizing detainees," characterizing Malaysia's approach as effective, given its attention to psychology and religion.[127] Subsequently, the PRC has hosted a number of Malaysian law enforcement officials for training. In August and September 2018, Yunnan Police College held a training course on border control and immigration capacity-building for Malaysian officers at Yunnan Police College[128] and then later an anti- drug delegation from Malaysia in December 2019.[129] In July 2019, the Criminal Investigation Police University of China held a counterterrorism training course for Malaysian personnel.[130]

Exchanges on border control and counterterrorism have notable implications for members of China's Uyghur ethnic minority. According to Lindsey Ford of the Brookings Institution, "China has… used its law enforcement partnerships to extend its domestic counterterrorism efforts, leaning on neighbors such as Thailand and Malaysia to extradite Uyghur Muslims back to China."[131] Credible external observers have described Beijing's crackdown on its Uyghur minority – justified on "counterterrorism" grounds – as genocide.[132]

ICT Companies

Developing Smart Cities has been an enduring goal in Malaysia, and major PRC-based technology companies have worked closely with Malaysian government entities on both smart cities and other aspects of Malaysia's developing digital infrastructure. In May 2015, Huawei launched a smart city program in Malaysia, offering "end-to-end security with ubiquitous network access, a convergent command center, video surveillance cloud, and mobile policing."[133] At the launch, Malaysian Communications and Multimedia Minister Ahmad Shabery conveyed the government's desire to "use today's platform to get the ecosystem to start thinking about the way ahead in using technology for a 'Smart Malaysia,' with the end goal of complementing and enabling all other nation-building initiatives."

In January 2018, Alibaba partnered with two Malaysian government agencies to launch the Malaysia City Brain initiative, which Alibaba described as "the first time for the City Brain solution to be adopted overseas."[134] The system offers Malaysia tools to analyze data through video and image recognition, data mining, and machine learning. City Brain is used in traffic management. It collects data by connecting with emergency dispatch, traffic command, traffic light control, and other urban management systems.[135] In February 2018, the Shanghai-based Yitu Technology made news in Malaysia when a quasi-public security company, Auxiliary Force Sdn Bhd (AFSB), began using the company's wearable cameras with facial recognition technology.[136] AFSB CEO Dato' Rosmadi Bin Ghazali called the collaboration "a significant step forward" in AFSB's efforts to "leverage artificial intelligence to increase public safety and security" and incorporate "real-time facial recognition and instant alerts to the presence of persons of interest from criminal watch lists."[137] As of September 2020, Yitu was also set to provide its facial recognition technology for Alibaba's City Brain platform in Kuala Lumpur.[138]

In recent years, Malaysia has also extended its cooperation with PRC-based companies on cybersecurity. In September 2018, Xly Salvationdata Technology Inc., a PRC-based provider of law enforcement data collection and recovery products, hosted a video surveillance training session in China for officials from several Malaysian government agencies, including Malaysia's National Cyber Security Agency. In addition to Xly's own products, the training covered integration and use of products from larger providers of surveillance technology such as Hikvision.[139] And in 2020, Malaysia announced a partnership with Huawei to create Southeast Asia's first cybersecurity lab. That partnership saw CyberSecurity Malaysia, the country's digital security agency, collaborate with Huawei and Celcom Axiata, a major Malaysian telecom company, on "cybersecurity capacity building, standards and certifications, as well as 'cybersecurity governance'."[140]

CONCLUSION

The growth in smart technology is outpacing the governance and regulatory structures that strike a balance between harnessing its benefits, achieving the policy goals, and safeguarding societal rights. There are clear benefits from the use of surveillance technology, from safety and security to easing traffic congestion and improving trash collection. At the same time, surveillance technology presents equally big risks to privacy and personal and political liberty. In democratic societies, politicians, civil society organizations, and thought leaders are all part of important discussions about finding the right balance. The process is likely to be a long and evolutionary one, and it will face challenges not only from those who would prefer to use technology to maintain "order," but also those who see the profits to be realized in a rapidly growing market.

For several reasons, the PRC poses a particular challenge to achieving the balance described above. One challenge is the Chinese government's dominance at home. It has the sole authority to regulate and use surveillance technology, without check by law or civil society. It has been clear that it sees a comprehensive surveillance capability as crucial to achieving its security and social welfare management goals: clean, safe, efficient, and prosperous communities under the unwavering surveillance of PRC authorities. It uses technology to enable its genocide in Xinjiang, and it is no less willing to blanket the rest of the country with continuous, intrusive surveillance. That model is a living demonstration to other would-be authoritarians who might trade democratic values for the supposed benefits of "order."

Second, while the PRC has been clear that international organizations such as the UN should work to forbid uses of technology not explicitly permitted by sovereign governments, it has not imposed similar restrictions on the surveillance technologies it sells abroad. This, coupled with China's push for market dominance mean that any efforts to manage surveillance technology can easily be thwarted. Repressive governments can simply turn to PRC-based suppliers. PRC-based firms appear to be willing to train their clients to use technology in whatever way they wish.

Third, the drive to dominate the market includes a push to shape technical standards for equipment and software. As the PRC makes surveillance tools available to repressive governments without oversight, those governments will be able to suppress segments of their populations. While the PRC's drive to advance its standards through UN and industry-led transnational bodies merits concern, that effort can be countered through vigilance and by building like-minded coalitions among other stakeholders. The risk is far greater that PRC-developed standards will become industry norms simply through ubiquity, since government support helps PRC-based firms capture markets.

Finally, China's wide-ranging espionage efforts, both commercial and state-directed, are well documented. This, as well as its growing willingness to pursue its opponents overseas, means there will continue to be a risk that the PRC government will access PRC-made equipment or data stored on PRC-made servers, built by PRC-based firms, to track activists and subvert other states' sovereignty.

The international community is unlikely to succeed in imposing binding restrictions on PRC behavior. It can, however, create disincentives – such as reputational risks, or risks to PRC-based firms' ability to access markets in democratic societies -- that could alter the PRC state's calculus. Three factors will determine success or failure in these efforts:

International conventions: Nations that are concerned about the risks of unregulated trade in surveillance technology (and that might want a level playing field for their own companies in a regulated market) must work with industry and civil society to implement recommendations such as those made by the UN Special Rapporteur. They also must ensure that the standards set by multilateral regulatory bodies reflect ethical principles and best practices. If they do these things, they may succeed in integrating the technology ecosystem into the larger rules-based international order. Failure leaves this space under-governed, meaning

that those who capture the most markets will set the technical standards and normalize an anything-goes environment in the use of surveillance technology.

Support for civil society: In the case studies and in other instances in which local communities have objected to the use of surveillance technology (PRC-made or otherwise), a combination of activists, civil society organizations, and the media have been crucial in spotlighting their concerns. Engaging with these groups, via support for their work and enlisting them as partners, will help ensure that smart technology serves positive social goals. Failure to do so, or worse, allowing repressive governments to do what they want without repercussion, will normalize repression through surveillance.

Monitoring and countermeasures: Companies working through export controls and end-user monitoring may find it difficult to counter China's global reach. Producing better quality technology may offer an advantage, but only in upper-income countries. Tools that allow governments and individuals to counteract infiltration via PRC-made systems could become a viable new market. Governments that might turn a blind eye to the PRC tracking its opponents might object to it targeting their own citizens or threatening their national security or economic interests. A state with no interest in contesting the situation in Xinjiang, and which might accept an extradition request for a Chinese activist, would presumably oppose Chinese agencies or hackers using PRC-made technology to undercut local industries.

APPENDIX: PRC LAW ENFORCEMENT INSTITUTIONS INVOLVED IN TRAINING FOREIGN COUNTERPARTS

TextOre research has mapped the PRC's training relationships around the world and with Ecuador, Kyrgyzstan, and Malaysia, and reached the following conclusions:

1. PRC police training has not prioritized advanced surveillance techniques over other law enforcement concerns (usually anti-drug or counterterrorism) in its relationships in other countries;
2. Chinese companies appear to have offered training for specific "smart" platforms. There is no indication from course materials or advertising that trainers are connected to PRC law enforcement. Research indicates, however, that the Chinese companies can access MPS facilities to give clients a look at their products at work.

Several PRC institutions have played prominent roles in establishing training relationships with law enforcement in the countries selected for case study. They are outlined below.

International Law Enforcement Yancheng Training Base

The Ministry of Public Security established this base in 2017, located in Yancheng, a city in Jiangsu Province that has been specifically designated by the Ministry as a center for international law enforcement cooperation.[141] A report by the *China Youth Daily* newspaper indicate that the base hosts training and conferences for international police, including repeat visits from senior officers from Indonesia, Pakistan, and South Korea, suggesting that the base may be building institutional relationships.[142] Publicly available information indicates that surveillance technology is part of the discussion. Training classes visit police technology centers. A class from the Guinea-Bissau palace guard training program visited a "big data command service center" [大数据指挥服务中心][143] in May 2018. As detailed in the Kyrgyzstan case study, the Yancheng Municipal Public Security Bureau and its training base have held an exchange focused on Yancheng's Safe City program.

Shandong Police College

The Shandong Police College [山东警察学院], was founded as the CCP's first police training institute in 1946 and is an active hub for international law enforcement training.[144] The curriculum includes topics ranging from martial arts[145] to tactics for handling "large-scale public incidents" (a phrase Beijing uses to describe large anti-government protests).[146] Between 2006 and 2024, the college held 160 training courses for 3,345 students from 99 countries, as well as students from international organizations such as the African Union (AU) Anti-Terrorism Center [非盟反恐中心].[147] The Kyrgyzstan case study provides further examples of training on combatting terrorism.

Zhejiang Police College

Zhejiang Police College [浙江警察学院], claims to have graduated close to 30,000 students to work in public security in Zhejiang Province and the Tibet Autonomous Region. It claims to have held nearly 200 training programs for over 4,000 participants representing 115 countries and regions.[148] As detailed in the Ecuador case study, the training at the college includes visits to local police stations, as well as to Hikvision's headquarters in the provincial capital city of Hangzhou.

Criminal Investigation Police University of China

Founded in 1948, the Criminal Investigation Police University of China says it has provided training to more than 2,700 criminal investigation professionals from over 100 countries.[149] The university hosted a counterterrorism training course for Malaysian officers in July 2019,[150] and Bishkek-based researcher Niva Yau (2022) notes that Kyrgyz training at the Criminal Investigation Police University of China involved field visits to China National Electronics Import & Export Corporation (CEIEC) [中国电子进出口总公司], a state-owned enterprise that specializes in defense electronics and public security systems.[151]

Yunnan Police College

The Yunnan Police College [云南警官学院] emphasizes cooperation with Asian countries such as Thailand, Cambodia, Laos, and Myanmar; it has hosted training on anti-drug trafficking, border control, and transportation management for nearly 3,000 law enforcement officers from over 70 countries.[152] As detailed in the Malaysia case study, the college has held multiple training courses for Malaysian officers and its home province is the site of close cooperation between the PRC and Malaysia in surveillance technology and counterterrorism.

Beijing Foreign Studies University

While not a police academy, the prestigious Beijing Foreign Studies University [北京外国语大学] has trained law enforcement from Kyrgyzstan, Ecuador, and Malaysia since October 2009.[153] The program is the MPS's only Chinese language-based year-long training program for foreign police officers. It is said to play an important role in law enforcement cooperation, transnational crimefighting, and maintaining regional peace. Much of its training is on combatting drug trafficking, smuggling, terrorism, and communications fraud.[154]

ENDNOTES

1 Tadashi Matsumoto, Jonathan Crook, and Kensuke Tanaka. "Trends for Smart City Strategies in Emerging Asia." OECD (2019), 4. https://www.oecd-ilibrary.org/content/paper/4fcef080-en, accessed 22 August 2022.

2 Specifically, the World Bank mentioned: A technology-intensive city, with sensors everywhere and highly efficient public services, thanks to information that is gathered in real time by thousands of interconnected devices. (For example, trash cans have sensors that indicate when they are full, and trash collectors follow a specific route based on this information.). All buildings are "intelligent," with smart meters and energy saving systems, and transport is painless.

Victor Mulas, Eva Clemente, and Arturo Muente-Kunigami, "Smart Cities," World Bank Brief, 08 January 2015, https://www.worldbank.org/en/topic/digitaldevelopment/brief/smart-cities.print.

3 Article 29 Data Protection Working Party, "Opinion 02/2012 on facial recognition in online and mobile services." 00727/12/ENWP 192, adopted 22 March 2012. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, accessed 09 September 2022.

4 The ACLU adds that "State motor vehicle agencies possess high-quality photographs of most citizens that are a natural source for face recognition programs and could easily be combined with public surveillance or other cameras in the construction of a comprehensive system of identification and tracking." American Civil Liberties Union, "Face Recognition Technology." https://webcache.googleusercontent.com/search?q=cache:g-WFQ6wo_K0J:https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology&cd=13&hl=en&ct=clnk&gl=se, accessed 09 September 2022.

5 Bureau of Justice Assistance, "Smart Policing Initiative." U.S. Department of Justice, https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/SmartPolicingFS.pdf Accessed 09 September 2022

6 Among these, see ENG: "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," New America, October 2018, newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/; CHN: PRC State Council, "新一代人工智能发展规划," PRC Government official website [in Chinese], 08 July 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

7 ENG: Center for Security and Emerging Technology, "Notice of the State Council on the Publication of "Made in China 2025" [国务院关于印发《中国制造2025》的通知} Georgetown University, 08 March 2022, https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf. CHN: "国务院关于印发《中国制造2025》的通知," PRC Government official website [in Chinese], 08 May 2015, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

8 "Digital trade spurs growth in Belt and Road partner countries," Xinhua [in English], 07 September 2022, https://english.news.cn/20220907/9c3a91bf167f450db8cdc4febdbbe6cb/c.html.

9 Xi declared that "We should pursue innovation-driven development and intensify cooperation in frontier areas such as digital economy, artificial intelligence, nanotechnology and quantum computing, and advance the development of big data, cloud computing and Smart Cities so as to turn them into a digital silk road of the 21st century. We should spur the full integration of science and technology into industries and finance, improve the environment for innovation and pool resources for innovation. We should create space and build workshops for young people of various countries to cultivate entrepreneurship in this age of the internet and help realize their dreams." Xi Jinping, "Work Together to Build the Silk Road Economic Belt and The 21st Century Maritime Silk Road," speech at the opening of the Belt and Road Forum, 14 May 2017, PRC Ministry of Foreign Affairs official website [in English], 15 May 2017, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/201705/t20170527_678618.html

10 Center for Security and Emerging Technology, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," [translation from the Chinese], Georgetown University, 12 May 2021, https://cset.georgetown.edu/publication/china-14th-five-year-plan/

11 See Xi's comments here: "Xi sends congratulatory letter to inauguration of World Internet Conference organization," Xinhua, https://www.wuzhenwic.org/2022-07/13/c_788406.htm; and here: "Xi sends congratulatory letter to inauguration of World Internet Conference organization" https://www.wuzhenwic.org/2021-09/26/c_663873.htm.

12 Ministry of Foreign Affairs of the People's Republic of China, "China's Positions on International Rules-making in Cyberspace," 20 October 21. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html, accessed 09 September 2022. The PRC expressed similar themes in a 08 September 2020 Statement - https://www.mfa.gov.cn/ce/ceus/eng/zgyw/t1812951.htm.

13 Zichen Wang, "Xi Jinping's Speech on Science & Tech on May 28, 2021," (Chinese Academy of Sciences and Chinese Academy of Engineering) [English translation with Chinese text] Pekingology, 08 Jun 2021, https://www.pekingnology.com/p/xi-jinpings-speech-on-science-and

14 ENG: "Full text of Xi's speech at SCO Samarkand summit," Xinhua [in English], 16 September 2022, https://english.news.cn/20220916/9a25ddd0a86848a09ef0b2a4e499a52d/c.html

CHN: "习近平在上海合作组织成员国元首理事会第二十二次会议上的讲话（全文）," PRC Government official website [Chinese-language source], 16 September 2022, http://www.gov.cn/xinwen/2022-09/16/content_5710294.htm

15 Specific pronouncements included : "The member states believe it is unacceptable to interfere in countries' internal affairs under the pretext of combating terrorism and extremism, as well as the unacceptability of using terrorist, extremist and radical groups for deceptive purposes."; "The member states emphasize the key role of the UN in countering threats in the information space and creating a safe, fair and inclusive information space built on the principles of respect for state sovereignty and non-interference in the internal affairs of other countries."; "They consider it important to ensure equal rights for all countries to regulate the internet and the sovereign right of states to manage it within their national segment." "The Samarkand Declaration of the Heads of State Council of the Shanghai Cooperation Organisation," Shanghai Cooperation Organization official website [in English], 16 September 2022, 3-4, https://eng.sectsco.org/load/914622/.

16 The strategy aims to "encourage and support enterprises, scientific research institutes, and industry organizations that participate in the formulation of international standards and accelerate the process of the internationalization of China's standards." "鼓励和支持企业、科研院所、行业组织等参与国际标准制定，加快我国标准国际化进程。" ENG: Center for Security and Emerging Technology, "Notice of the State Council on the Publication of "Made in China 2025" [国务院关于印发《中国制造2025》的通知} Georgetown University, 08 March 2022, https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf; CHN: "国务院关于印发《中国制造2025》的通知," PRC Government official website [in Chinese], 08 May 2015, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

17 加快我国优势技术标准向国际转化，持续推动发布ISO、IEC标准中文版。... 推进中外标准的相互比对、认可、采用，促进标准体系兼容。That said, the document also calls for China to "Carry out the conversion of international standards and promote the conversion and application of advanced and applicable international standards in China." [开展国际标准转化行动，推动先进适用国际标准在我国转化应用。] ENG: Standardization Administration of China, "Notice of Standardisation Administration of China on Releasing 'Main Points of National Standardisation Work in 2020,'" SAC Issue [2020] No. 8,translated by Seconded European Standardization Expert in China (SESEC), 20 March 2020, https://www.sesec.eu/app/uploads/2020/04/Main-Points-of-National-Standardisation-Work-in-2020.pdf; CHN: "国家标准化管理委员会关于印发《2020年全国标准化工作要点》的通知, Standardization Administration of China [in Chinese], 10 March 2020, http://www.sac.gov.cn/sbgs/sytz/202003/P020200313308102642552.pdf

18 Daniel R. Russel and Blake H. Berger, "Stacking the Deck: China's Influence in International Technology Standards Setting," Asia Society Policy Institute, 2021, 8, https://asiasociety.org/sites/default/files/2021-11/ASPI_StacktheDeckreport_final.pdf.

19 Among others, see Russel and Berger; and comprehensive research by Julia Voo, "Shaping Global Technology Governance: Why the U.S. Must Adopt a Proactive Approach to Technical Standards for Long Term Security," Working Paper for the Penn Project on the Future of U.S.-China Relations [updated Spring 2021], https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2021/04/Julia-Voo_Shaping-Global-Technology-Governance_Updated.pdf

20 Russel and Berger, 22 and 24. Voo further contends that the subsidies for proposal incentivize the submission of proposals in quantity over quality, which can tax the resources of the organizations. Voo, 27.

21 Russel and Berger, 26.

22 TextOre examined the public-facing websites of the ITU, Institute of Electrical and Electronics Engineers (IEEE), 3rd Generation Partnership Project, and International Electrotechnical Commission (IEC) and their subsidiary units. Of these, IEEE's Council on RFID does have a significant PRC leadership presence, and the head of the IEC is also from the PRC. Otherwise, the bodies appear far more dominated by Americans.

23 While it is notable that China is not listed as a participant in the IEC affiliate country program (https://www.iec.ch/acp), Chinese firms, particularly Huawei, have been very active in engaging these bodies. Sue Rudd, Director Networks and Service Platforms service at Strategy Analytics, reported that "Huawei, Ericsson and Nokia – made more significant contributions to 5G standards [at 3GPP] than other studied companies. Huawei leads in terms of overall contributions to the end-to-end 5G standards, while Ericsson leads in TSG/WG chairmanship and Nokia in approved/agreed ratio of 5G contribution papers." Strategy Analytics, "Infrastructure Giants Lead 5G Standardization," 17 March 2020, https://news.strategyanalytics.com/press-releases/press-release-details/2020/Strategy-Analytics-Infrastructure-Giants-Lead-5G-Standardization/default.aspx. CSIS also observed that "China sends the largest delegation to the ITU's various study groups and is also represented by Huawei and other state-owned enterprises that are members. Working through these study groups, with the support of high-level ITU leadership, Huawei has introduced some 2,000 new standard proposals to ITU study groups on topics including 5G, cybersecurity, and artificial intelligence." Kristen Cordell, "The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of," CSIS, 14 December 2020, https://www.csis.org/analysis/international-telecommunication-union-most-important-un-agency-you-have-never-heard.

24 Center for Security and Emerging technology, "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," [translation from the Chinese], Georgetown University, 12 May 2021, 50, https://cset.georgetown.edu/publication/china-14th-five-year-plan/

25 Other principles expressed include "peace" (meaning, not using or allowing the internet to be used for hostile purposes), "sovereignty" (meaning, the right of all states to set rules and governance withing their own borders), "shared governance" (meaning, the international community needs to work together to manage jointly and distribute equitably basic internet resources and put in place a multilateral, democratic and transparent global governance system, so that the internet will be a place of open resources and shared responsibilities governed through cooperation.), and "shared development" (meaning, everyone should benefit, and those benefits are achieved through cooperation). Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace," Xinhuanet News, 01 March 2017. http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm, accessed 14 September 2022.

26 Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace," Xinhuanet News, 01 March 2017. http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm, accessed 14 September 2022.

27 "Certain States politicize technology and cybersecurity issues, willfully suppress other States' ICT enterprises and impose unfair and unjust barriers on global ICT supply chain and trade, jeopardizing global development and cooperation." Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace," Xinhuanet News, 01 March 2017. http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm, accessed 14 September 2022.

28 "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." United Nations A/69/723, 13 January 2015, 4. https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf, accessed 09 September 2022.

29 "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." United Nations A/69/723, 13 January 2015, 5. https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf, accessed 09 September 2022.

30 "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General." United Nations A/69/723, 13 January 2015, 5. https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf, accessed 09 September 2022.

31 "Keeping in mind the Belt and Road Initiative, China will encourage and support Chinese Internet companies, together with those in the manufacturing, financial and ICT sectors, to take the lead in going global, participate in international competition in line with the principle of fairness, explore international market and build cross-border industrial chain. Chinese companies will be encouraged to actively engage in capacity building of other countries and help developing countries with distance learning, remote health care and e-business among others to contribute to their social development." Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace," Xinhuanet News, 01 March 2017. http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm, accessed 14 September 2022.

32 TextOre examined the full 2001 catalogue of controlled items and the revision from YYYY. PRC Ministry of Commerce and PRC Ministry of Science and Technology, "中国禁止出口限制出口技术目录" (中华人民共和国对外贸易经济合作部、科学技术部二00一年第十六号令), PRC Ministry of Commerce official website [Chinese-language source], 12 December 2001, http://www.mofcom.gov.cn/aarticle/b/e/200207/20020700031702.html [Translation via Google for the technical terms]; "《中国禁止出口限制出口技术目录》调整内容" PRC Ministry of Commerce official website [Chinese-language source], 28 August 2020, http://images.mofcom.gov.cn/fms/202008/20200828200911003.pdf; Translations via Google and Ben Murphy, "Revisions to the Content of the Catalog of Prohibited or Restricted Technology Exports," Georgetown Center for Security and Emerging Technology, 31 August 2020, https://cset.georgetown.edu/publication/revisions-to-the-content-of-the-catalog-of-prohibited-or-restricted-technology-exports/

33 "Export Control Law of the People's Republic of China (2020 edition)," [Unofficial translation, attributed to Covington & Burling] China Law Translate, 19 October 2020, https://www.chinalawtranslate.com/en/export-control/#_Toc54004248. Original Chinese Text: http://www.xinhuanet.com/politics/2020-10/18/c_1126624518.htm. These terms are reflected in draft MOFCOM implementing regulations – see Frank Pan, Ivy Tan, and Tina Li, "China: Long-awaited draft implementing rules released pursuant to the new Export Control Law," Baker McKenzie, 16 May 2022, https://sanctionsnews.bakermckenzie.com/china-long-awaited-draft-implementing-rules-released-pursuant-to-the-new-export-control-law/

34 Ibid., 20.

35 Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [A/HRC/41/35], United Nations General Assembly, 28 May 2019, 1, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement

36 "This interim final rule outlines the progress the United States has made in export controls pertaining to cybersecurity items, revised Commerce Control List (CCL) implementation, and requests from the public information about the impact of these revised controls on U.S. industry and the cybersecurity community. Specifically, this rule establishes a new control on these items for National Security (NS) and Anti-terrorism (AT) reasons, along with a new License Exception Authorized Cybersecurity Exports (ACE) that authorizes exports of these items to most destinations except in the circumstances described. These items warrant controls because these tools could be used for surveillance, espionage, or other actions that disrupt, deny or degrade

the network or devices on it." U.S. Department of Commerce, Bureau of Industry and Security, "Information Security Controls: Cybersecurity Items," Federal Register Vol. 86, No. 201, Thursday, 21 October 2021, https://www.govinfo.gov/content/pkg/FR-2021-10-21/pdf/2021-22774.pdf. See also this power point presentation about BIS efforts to exert greater human rights-related controls over surveillance technology: https://www.bis.doc.gov/index.php/documents/2022-update-conference/3074-2022-update-conference-surveillance-and-human-rights-fpd-final-draft-060622-knv-occ-6-29-22/file

37 European Union, "Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021, setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)," Official Journal of the European Union Vol 64 [in English], 11 June 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN.

38 "U.S. – EU Trade & Technology Council Stakeholder Meeting (Summary)" U.S. Department of Commerce, Bureau of Industry and Security official website, 27 October 2021, https://www.bis.doc.gov/index.php/policy-guidance/u-s-eu-ttc.

39 Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," Lawfare, January 5, 2018, https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research. The UN Special Rapporteur welcomed these improvements but found them inadequate on their own. Report of the Special Rapporteur (2019), 17.

40 "About Us," Wassenaar Arrangement official site, https://www.wassenaar.org/about-us/#about-us

41 The experts: Irene Khan, Special Rapporteur on the promotion and protection of the right to freedom of expression; Mary Lawlor, Special Rapporteur on the situation of human rights defenders; Clement Nyaletsossi Voulé, Special Rapporteur on the rights to freedom of peaceful assembly and of association; and the UN Working Group on human rights and transnational corporations and other business enterprises (known as the Working Group on Business and Human Rights), Surya Deva (Chairperson), Elzbieta Karska (Vice-Chairperson), Githu Muigai, Dante Pesce, and Anita Ramasastry. "Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech," Press release, UN Office of the High Commissioner for Human Rights, 12 August 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379

42 Eva Dou, "China built the world's largest facial recognition system. Now, it's getting camera-shy," The Washington Post, 30 July 2021, https://www.washingtonpost.com/world/facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html

43 To offer one particularly harrowing recounting, Charlie Campbell, "'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World," *Time*, November 21, 2019, https://time.com/5735411/china-surveillance-privacy-issues/

44 Report of the Special Rapporteur (2019), 5.

45 Parkinson, Bariyo, and Chin, 2019.

46 Paul Triolo, Clarise Brown, and Kelsey Broderick, "The Digital Silk Road: Expanding China's Digital Footprint." Eurasia Group 8 (2020), 2. https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint.pdf, accessed 24 August 2022.

47 These would include Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision) [杭州海康威视数字技术股份有限公司; Zhongxing Telecommunication Equipment Corporation (ZTE) [中兴通讯股份有限公司; and Zhejiang Dahua Technology Co., Ltd. (Dahua) [浙江大华技术股份有限公司.

48 Lorand Laskai, How China is Supplying Surveillance Technology and Training around the World. Privacy International (February 2019), 7. https://privacyinternational.org/advocacy/3216/how-china-supplying-surveillance-technology-and-training-around-world, accessed 25 August 2022.

49 "Ren Zhengfei's Interview with the Financial Times." *In His Own Words: Dialogues with Ren*, vol. 2, Huawei, Aug. 2019, https://www-file.huawei.com/-/media/corp/facts/pdf/in-his-own-words-dialogues-with-ren-volume-ii.pdf?la=en, p. 190.

50 Dorfman, Zach. "Tech Giants Are Giving China A Vital Edge in Espionage." Foreign Policy, December 23, 2020. https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

51 "...at the Munich Security Conference, Yang Jiechi, a member of the Political Bureau of the Communist Party of China (CPC) Central Committee and Director of the Office of the Foreign Affairs Commission of the CPC Central Committee, made it very clear that the Chinese government never requires companies to install backdoors. Premier Li Keqiang then reiterated this position at a press conference following a recent session of the National People's Congress. Recently, when Premier Li visited our booth at this year's 16+1 Summit in Croatia, he even directly told our staff not to install backdoors. This is testament to their support for us when it comes to never stealing intelligence from other countries or companies. Therefore, we can sign 'no backdoor, no-spy' agreements with any country."

52 RWR Advisory Group, 2018.

53 Simmons, Keir, Laura Saravia and Yuliya Talmazan. "China guilty of genocide, crimes against humanity against Uyghurs, watchdog finds." NBC News, December 9, 2021. https://www.nbcnews.com/news/china/china-guilty-genocide-crimes-humanity-uyghurs-watchdog-finds-rcna8157.

54 Healy, Conor. "Uyghur Surveillance & Ethnicity Detection Analytics in China." Expert Report Presented to the Uyghur Tribunal, IVPM, 20 August 2021, https://uyghurtribunal.com/wp-content/uploads/2021/09/Conor-Healy.pdf, p. 13-4.

55 Healy, Conor. "Uyghur Surveillance & Ethnicity Detection Analytics in China." Expert Report Presented to the Uyghur Tribunal, IVPM, 20 August 2021, https://uyghurtribunal.com/wp-content/uploads/2021/09/Conor-Healy.pdf, p. 4-5.

56 Healy, Conor. "Uyghur Surveillance & Ethnicity Detection Analytics in China." Expert Report Presented to the Uyghur Tribunal, IVPM, 20 August 2021, https://uyghurtribunal.com/wp-content/uploads/2021/09/Conor-Healy.pdf, p. 6.

57 Healy, Conor. "Uyghur Surveillance & Ethnicity Detection Analytics in China." Expert Report Presented to the Uyghur Tribunal, IVPM, 20 August 2021, https://uyghurtribunal.com/wp-content/uploads/2021/09/Conor-Healy.pdf, p. 6-7.

58 "Smart City Solution Service." *Huawei*, https://e.huawei.com/en/services/industry-consulting-and-application-integration/smart-city, accessed 13 Oct. 2022.

59 "The Future Is On — The Nervous System of a Smart City." *Huawei*, https://e.huawei.com/en/solutions/industries/government/smart-city, accessed 13 Oct. 2022;"Mapping Huawei's Smart Cities Creep." *Privacy International*, 17 Nov. 2021, https://privacyinternational.org/long-read/4689/mapping-huaweis-smart-cities-creep.

60 Hillman, Jonathan E. and Maesea McCalpin. "Watching Huawei's 'Safe Cities'." *Center for Strategic and International Studies*, 4 Nov. 2019, https://www.csis.org/analysis/watching-huaweis-safe-cities.

61 "Announcement of 'Entity List.'" *Meiya Pico*, 24 Oct. 2019, https://www.meiyapico.com/announcement-of-entity-list_n28.html.

62 "Information Security Academy [信息安全学院]." *Meiya Yi'an* [美亚亿安], https://www.myeant.com/school/index.html.

63 "Announcement of 'Entity List.'" *Meiya Pico*, 24 Oct. 2019, https://www.meiyapico.com/announcement-of-entity-list_n28.html.

64 "Huawei - Seeds for the Future - History." *Huawei*, Dec. 2021, https://www.huawei.com/minisite/seeds-for-the-future/history.html.

65 "Huawei 'Safe City' Africa Summit Concludes [华为'平安城市'非洲峰会闭幕]." *People's Daily Online* [人民网], 30 Apr. 2015, http://world.people.com.cn/n/2015/0430/c1002-26928572.html.

66 "Huawei Global Safe City Summit Proposes C-C4ISR Cooperation Protection Method, Will Become the Core of the Global Public Security Industry's Digitization Transformation [华为全球平安城市峰会提出 C-C4ISR 协作防护方式 将成为全球公共安全行业数字化转型核心]." *Huawei* [华为], 27 Apr. 2017, https://www.huawei.com/cn/news/2017/4/c-c4isr-public-safety-solutions.

67 https://www.hikvision.com/en/support/training/

68 The English-language translation was less explicit and simply read "Building on AI's Momentum.""Hikvision hosts 2021 AI Cloud Summit to boost digital transformation of industries." *Hikvision*, 2 Apr. 2021, https://www.hikvision.com/en/newsroom/latest-news/2021/hikvision-hosts-2021-ai-cloud-summit-to-boost-digital-transformation-of-industries/.

69 "Ecuador: Freedom in the World 2022 Country Report." *Freedom House*, https://freedomhouse.org/country/ecuador/freedom-world/2022.

70 Ibid.

71 Ibid.

72 Castro, Diana. "Ecuador." *The People's Map of Global China*, 31 Mar. 2021, https://thepeoplesmap.net/country/ecuador/.

73 Ibid.

74 "Collection of Treaties and Agreements (Up to October 2018) [条约与协定汇总(截至2018年10月)]." *Yangguang Jianwu Wang* [阳光检务网], 12 Dec. 2018, http://www.gd.jcy.gov.cn/jcyw/sfxz/flfgytyxd/201812/t20181212_2440091.shtml.

75 "U.S. Relations with Ecuador." *U.S. Department of State*, 10 Aug. 2022, https://www.state.gov/u-s-relations-with-ecuador/.

76 "Ecuador ECU911 Project [厄瓜多尔ECU911项目]." *China Youth Online* [中青在线], 11 May 2017, http://m.cyol.com/content/2017-05/11/content_16057601.htm; Rollet, Charles. "Ecuador's All-Seeing Eye Is Made in China." *Foreign Policy*, 9 Aug. 2018,

https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

77 "Surveillance Tech in Latin America: Made Abroad, Deployed at Home." *Access Now*, 8 Aug. 2021, https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/.

78 Stryker, Cian. "Digital Silk Road and Surveillance Technology in Central Asia." *Digital Silk Road in Central Asia: Present and Future*, ed. Nargis Kassenova and Brendan Duprey, Davis Center for Russian and Eurasian Studies, 2021, https://daviscenter.fas.harvard.edu/digital-silk-road.

79 Freeman, Will. "A Surge in Crime and Violence Has Ecuador Reeling." *Council on Foreign Relations*, 14 June 2023. https://www.cfr.org/blog/surge-crime-and-violence-has-ecuador-reeling

80 "PRC Ambassador to Ecuador Chen Guoyou Meets with Ecuadorian Government Minister Pazmiño [驻厄瓜多尔大使陈国友会见厄政府部长帕斯米尼奥]." *Embassy of the People's Republic of China in the Republic of Ecuador* [中华人民共和国驻厄瓜多尔共和国大使馆], 12 Jan. 2021, http://ec.china-embassy.gov.cn/sgxw/202101/t20210112_4233236.htm; "PRC Ambassador to Ecuador Chen Guoyou Meets with Newly Appointed Ecuadorian Government Minister Vela [驻厄瓜多尔大使陈国友拜会厄新任政府部长贝拉]." *Embassy of the People's Republic of China in the Republic of Ecuador* [中华人民共和国驻厄瓜多尔共和国大使馆], 6 Aug. 2021, http://ec.china-embassy.gov.cn/sgxw/202108/t20210806_9047392.htm.

81 "Explainer: Why has Ecuador become so violent?" *Reuters*, 10 Aug. 2023, https://www.reuters.com/world/americas/why-has-ecuador-become-so-violent-2023-08-10/.

82 "Law Enforcement Liaison Chinese-Language Training Program Opening Ceremony Is Held at the University [执法联络员汉语培训项目开学典礼在我校举行]." *Beijing Foreign Studies University* [北京外国语大学], 23 Oct. 2009, https://news.bfsu.edu.cn/article/534/cate/4.

83 "Public Security Bureau: Beijing Foreign Studies University Law Enforcement Liaison Training Program Holds Its Eighth Opening Ceremony [公安部-北外执法联络员培训项目第八期开学典礼举行]." *Beijing Foreign Studies University* [北京外国语大学], 28 Oct. 2013, https://news.bfsu.edu.cn/article/5648/cate/0.

84 "Chinese Translators Provide Spanish Translation for Ecuadorian Mid- to High-Level Police Officer Advanced Course at Zhejiang Police Academy [中译翻译为浙江警察学院厄瓜多尔中高级警官研修班提供西班牙语翻译]." *Hangzhou Join Translation Co., Ltd.* [杭州中译翻译有限公司], 27 Oct. 2016, http://www.fanyishang.com/content/2362.html.

85 Mozur, Paul, et al. "Made in China, Exported to the World: The Surveillance State." *New York Times*, 24 Apr. 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

86 Mozur, Paul, et al. "Made in China, Exported to the World: The Surveillance State." New York Times, 24 Apr. 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

87 Ortiz, Sara. "Lenín Moreno Says that the 911 ECU Was Used in a 'Perverse' Way for Espionage [Lenín Moreno dice que el ECU 911 se usó de manera 'perversa' para espionaje]." *El Comercio*, 25 Apr. 2019, https://www.elcomercio.com/actualidad/lenin-moreno-ecu-911-espionaje.html.

88 Mozur, Paul, et al. "Made in China, Exported to the World: The Surveillance State." *New York Times*, 24 Apr. 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

89 "Ecuador ECU911 Project [厄瓜多尔ECU911项目]." *China Youth Online* [中青在线], 11 May 2017, http://m.cyol.com/content/2017-05/11/content_16057601.htm.

90 "ECU911 Played Large Role in Ecuador Earthquake [ECU911系统在厄瓜多尔地震中作用巨大]." *CCID* [中国电子信息产业发展研究院], 5 May 2016, https://www.ccidgroup.com/info/1097/21091.htm.

91 Rollet, Charles. "Ecuador's All-Seeing Eye Is Made in China." *Foreign Policy*, 9 Aug. 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/; Wang, Lingxiao. "Chinese President Pledges Further Support for Ecuador's Post-Quake Rebuilding." *CCTV English*, 19 Nov. 2016, http://www.english.cctv.com/2016/11/19/ARTIgpww0NlxNkcPWLOaOkbR161119.shtml

92 "Ecuadorian President Correa Meets with Huawei Rotating CEO Guo Ping [厄瓜多尔总统科雷亚会见华为轮值CEO郭平]." *Huawei*, 6 Jan. 2015, https://www.huawei.com/cn/news/2015/01/hw_411141.

93 "Ecuador." *Huawei*, https://www.huawei.com/en/sustainability/win-win-development/social-contribution/seeds-for-the-future/ecuador. Archived at https://archive.ph/kNKCK and accessed 16 Sept. 2022.

94 "Ecuadorian President: Huawei's Abilities in Technological Innovation Are Praiseworthy, Hopes to Import More of Huawei's Advanced Technology to Benefit Ecuador [厄瓜多尔总统：华为的科技创新能力值得赞赏，希望引进更多华为先进科技造福厄瓜多尔]." *Huawei*, 13 Dec. 2018, https://www.huawei.com/cn/news/2018/12/ecuador-president-visit-huawei-2018.

95 Rollet, Charles. "Ecuador's All-Seeing Eye Is Made in China." *Foreign Policy*, 9 Aug. 2018, https://foreignpolicy.

com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

96 "#AlertaDigitalEC #Ecuador 3,500 ECU911 Cameras Would Have Facial Recognition [#AlertaDigitalEC #Ecuador 3,500 cámaras del ECU911 tendrían reconocimiento facial]." *Usuarios Digitales*, 11 Nov. 2016, http://www.usuariosdigitales.org/2016/11/11/alertadigitalec-ecuador-3500-camaras-del-ecu911-tendrian-reconocimiento-facial/.

97 "Civil Society Organizations Reject Attempts to Silence and Criminalize Social Movements in the Context of Protest in Ecuador and Demand That Human Rights Be Respected [Organizaciones de la Sociedad Civil Rechazan Intentos de Silenciar Y Criminalizar Movimientos Sociales en El Contexto de Protesta en Ecuador Y Exigen Que SE Respeten Los Derechos Humanos]." *Sursiendo*, 17 Jun. 2022, https://sursiendo.org/2022/06/organizaciones-exigen-respeto-derechos-humanos-ecuador/.

98 Mozur, Paul, et al. "Made in China, Exported to the World: The Surveillance State." *New York Times*, 24 Apr. 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

99 "Kyrgyzstan: Freedom in the World 2022 Country Report." *Freedom House*, https://freedomhouse.org/country/kyrgyzstan/freedom-world/2022.

100 Schulz, Dante. "China-Kyrgyzstan Relations." *Caspian Policy Center*, 25 Feb. 2022, https://www.caspianpolicy.org/research/security-and-politics-program-spp/china-kyrgyzstan-relations.

101 Hedlund, Stefan. "China finds investment in Kyrgyzstan a risky necessity." *GIS*, 11 Apr. 2019, https://www.gisreportsonline.com/r/kyrgyzstan-china/.

102 "Collection of Treaties and Agreements (Up to October 2018) [条约与协定汇总(截至2018年10月)]." *Yangguang Jianwu Wang* [阳光检务网], 12 Dec. 2018, www.gd.jcy.gov.cn/jcyw/sfxz/flfgytyxd/201812/t20181212_2440091.shtml.

103 "U.S. Relations with Kyrgyzstan." *U.S. Department of State*, 27 Jul. 2022. https://www.state.gov/u-s-relations-with-kyrgyzstan/.

104 Yau, Niva. "Chinese Governance Export in Central Asia." *Security and Human Rights*, 2 Feb. 2022, https://brill.com/view/journals/shrs/aop/article-10.1163-18750230-bja10009/article-10.1163-18750230-bja10009.xml.

105 "Law Enforcement Liaison Chinese-Language Training Program Opening Ceremony Is Held at the University [执法联络员汉语培训项目开学典礼在我校举行]." *Beijing Foreign Studies University* [北京外国语大学], 23 Oct. 2009, https://news.bfsu.edu.cn/article/534/cate/4.

106 "Kyrgyz Republic Ministry of Internal Affairs Counterterrorism Training Course Concludes at the College [吉尔吉斯共和国内务部反恐培训班在我院结业]." *Shandong Police College* [山东警察学院], Sept. 2012, http://www.sdpc.edu.cn/info/1024/8224.htm; "[2015年吉尔吉斯斯坦反恐研修班在我院结业]." *Shandong Police College* [山东警察学院], *Shandong Police College* [山东警察学院], 15 Jun. 2015, http://www.sdpc.edu.cn/info/1024/9020.htm; "[上合组织国家反恐研修班在我院结业]." *Shandong Police College* [山东警察学院], 27 Apr. 2018, https://www.sdpc.edu.cn/info/1026/5099.htm.

107 In February 2019, Meiya Pico's website shared a PRC state media report about an SCO-organized cyber counterterrorism exercise. Although the story does not detail Meiya Pico's involvement, the company's logo is visible on computer monitors in accompanying photographs of the event. This potentially substantiates information on a map on Meiya Pico's website labeling Kyrgyzstan among 30 countries, including Ecuador and Malaysia, as recipients of the company's digital training. "SCO Joint Anti-Cyber Terrorism Exercise Held in Xiamen-------CGTN by Meng Qingsheng." *Meiya Pico* [美亚柏科], 26 Feb. 2019, https://www.meiyapico.com/sco-joint-anti-cyber-terrorism-exercise-held-in-xiamen-cgtn-by-meng-qingsheng_n9.html&cd=1&hl=en&ct=clnk&gl=id."Training Center." *Meiya Pico* [美亚柏科], https://www.meiyapico.com/training-center_d18. Accessed 13 Sept. 2022.

108 "Chief of Staff of the President Sapar Isakov Met with Representatives of Huawei [Руководитель Аппарата Президента Сапар Исаков встретился с представителями компании Huawei]." *President of the Kyrgyz Republic* [Президент Кыргызской Республики], 2 Jun. 2017, http://www.president.kg/ru/sobytiya/novosti/5024_rukovoditel_apparata_prezidenta_sapar_isakov_vstretilsya_s_predstavitelyami_kompanii_huawei.

109 "The Government Has Signed an Investment Agreement with 'Huawei Technologies Co., Ltd.' to Implement the Smart City Security Project [Өкмөт коопсуздук боюнча «Акылдуу шаар» долбоорун ишке ашыруу үчүн «Huawei Technologies Co., Ltd» компаниясы менен инвестициялык келишимге кол койду]." *Cabinet of Ministers of the Kyrgyz Republic* [Кыргыз Республикасынын Министрлер Кабинети], 12 Jan. 2018, https://www.gov.kg/ky/post/s/km-t-koopsuzduk-boyuncha-akyilduu-shaar-dolboorun-ishke-ashyiruu-ch-n-huawei-technologies-co-ltd-kompaniyasyi-menen-investitsiyalyik-kelishimge-kol-koydu.

110 Umarov, Temur. "China Looms Large in Central Asia." *Carnegie Endowment for International Peace*, 30 Mar. 2020, https://carnegiemoscow.org/commentary/81402; Hoagland, Richard et al. "China's Growing Influence in Central Asia Through Surveillance Systems." *Caspian Policy Center*, Sept. 2020, https://api.caspianpolicy.org/media/uploads/2020/09/PB-Chinas-growing-influence-in-CA-through-surveillance-systems.pdf.

111 Hoagland, Richard et al. "China's Growing Influence in Central Asia Through Surveillance Systems." *Caspian Policy Center*,

Sept. 2020, https://api.caspianpolicy.org/media/uploads/2020/09/PB-Chinas-growing-influence-in-CA-through-surveillance-systems.pdf.

112 "Meeting of the Minister for the Promotion and Protection of Investments of the Kyrgyz Republic Shykmamatov A.N. with Huawei Technologies Bishkek Co., Ltd. [Встреча министра по продвижению и защите инвестиций кыргызской республики шыкмаматова А.н. С компанией «Huawei Technologies Bishkek Co., Ltd»]." *Investment Portal of the Kyrgyz Republic* [Инвестиционный портал Кыргызской Республики], 19 May 2021, https://invest.gov.kg/2021/05/19/встреча-министра-по-продвижению-и-защ/.

113 "Ministry of Internal Affairs: Intelligent Systems and Advanced Technologies Are Being Introduced to Improve Public and Road Safety [МВД: Осуществляется внедрение интеллектуальных систем и передовых технологий в целях повышения общественной и дорожной Безопасности]." *Ministry of Internal Affairs of the Kyrgyz Republic* [МВД Кыргызской Республики], 28 Aug. 2019, https://mvd.gov.kg/index.php/rus/mass-media/all-news/item/9632-poyasneniya-po-sotrudnichestvu-mvd-s-kitajskoj-kompaniej.

114 Bowdler, Neil and Current Time. "Kyrgyz Police Embrace Chinese Face-Recognition Technology." *Radio Free Europe*, 1 Nov. 2019, https://www.rferl.org/a/kyrgyzstan-police-embrace-chinese-face-recognition-tech/30248431.html.

115 "Facial Recognition Cameras Appeared on the Streets of Bishkek. China Installed Them for Free [На улицах Бишкека появились камеры распознавания лиц. Китай установил их бесплатно]." *Radio Azattyk* [Радио Азаттык], 1 Nov. 2019, https://rus.azattyk.org/a/kyrgyzstan_cameras_china_2019/30247449.html.

116 Zhumakadyr kyzy, Bermet. "Right to Privacy in Kyrgyzstan." *Europe-Central Asia Monitoring*, 21 Jan. 2020, https://eucentralasia.eu/right-to-privacy-in-kyrgyzstan/.

117 "Facial Recognition Cameras Appeared on the Streets of Bishkek. China Installed Them for Free [На улицах Бишкека появились камеры распознавания лиц. Китай установил их бесплатно]." *Radio Azattyk* [Радио Азаттык], 1 Nov. 2019, https://rus.azattyk.org/a/kyrgyzstan_cameras_china_2019/30247449.html.

118 Freedom House, "Malaysia." *Freedom in the World 2021.* https://freedomhouse.org/country/malaysia/freedom-world/2021, accessed 23 August 2022.

119 Ibid.

120 Conclusion based on both Freedom House scores.

121 Embassy of Malaysia, Beijing, "Overview of Malaysia-China Relations." https://www.kln.gov.my/web/chn_beijing/history, accessed 23 August 2022.

122 "U.S. Relations with Malaysia." *U.S. Department of State*, 19 Apr. 2022, https://www.state.gov/u-s-relations-with-malaysia/.

123 Byler, Darren. "Surveillance Infrastructure Effects." *China Made* [中国制造], https://chinamadeproject.net/surveillance-infrastructure-effects/, accessed 4 Oct. 2022.

124 Weber, Valentin. "The Worldwide Web of Chinese and Russian Information Controls." *Open Technology Fund*, 17 Sept. 2019, https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf; Harun, Abdul Aziz and Bernama. "DPM: Chinese Crime-Fighting Methods Worth Emulating." *Malaysiakini*, 15 Jan. 2017, https://www.malaysiakini.com/news/369309.

125 "Deputy Prime Minister Visits China Beginning Tomorrow [副揆明起赴华访问]." *Oriental Daily* [东方日报], 9 Jan. 2017, https://www.orientaldaily.com.my/news/nation/2017/01/09/179553; "[Special Correspondent] Deputy Prime Minister Arrives in Beijing to Consolidate Malaysia-China Counterterrorism Ties [【特派】副揆抵北京　巩固马中防恐联系]." Oriental Daily [东方日报], 10 Jan. 2017, https://www.orientaldaily.com.my/index.php/news/nation/2017/01/10/179736.

126 Andres, Leslie. "Border Control: China Agrees to Transfer Tech, Shares Yunnan's Experiences, Says Zahid." New Straits Times, 14 Jan. 2017, https://www.nst.com.my/news/2017/01/204178/border-control-china-agrees-transfer-tech-shares-yunnans-experiences-says-zahid.

127 Harun, Abdul Aziz and Bernama. "DPM: Chinese Crime-Fighting Methods Worth Emulating." *Malaysiakini*, 15 Jan. 2017, https://www.malaysiakini.com/news/369309.

128 "Yunnan Police College Holds 2018 Malaysia Border Control and Immigration Capacity Building Training Course [云南警官学院举办2018年马来西亚边境管理与移民能力建设培训班]." *Yunnan Police College* [云南警官学院], 30 Aug. 2018, https://www.ynpc.edu.cn/site/ypoa/wjpx/info/2018/23759.html.

129 "Malaysia Drug Prohibition Delegation Visits Yunnan Police College [马来西亚禁毒代表团到访我院]." *Yunnan Police College* [云南警官学院], 24 Dec. 2019, https://www.ynpc.edu.cn/site/ypoa/gjhz/info/2019/26754.html.

130 "Criminal Investigation Police University of China Holds 2019 Malaysia Counterterrorism Training Course Closing Ceremony [学院举行2019年马来西亚反恐培训班结业典礼]." *Criminal Investigation Police University of China* [中国刑事警察学院], 5 Jul. 2019, http://www.cipuc.edu.cn/info/2697/4491.htm.

131 Ford, Lindsey W. "Extending the Long Arm of the Law: China's International Law Enforcement Drive." *The Brookings Institution*, 15 Jan. 2021, https://www.brookings.edu/blog/order-from-chaos/2021/01/15/extending-the-long-arm-of-the-law-chinas-international-law-enforcement-drive/.

132 Simmons, Keir, Laura Saravia and Yuliya Talmazan. "China guilty of genocide, crimes against humanity against Uyghurs, watchdog finds." NBC News, December 9, 2021. https://www.nbcnews.com/news/china/china-guilty-genocide-crimes-humanity-uyghurs-watchdog-finds-rcna8157.

133 "Huawei Rolls out Smart City Solution in Malaysia." *Digital News Asia*, 20 May 2015, https://www.digitalnewsasia.com/business/huawei-rolls-out-smart-city-solution-in-malaysia.

134 "Alibaba Cloud Launches Malaysia City Brain to Enhance City Management," *Alibaba Cloud*, 29 Jan. 2018, https://www.alibabacloud.com/press-room/alibaba-cloud-launches-malaysia-city-brain-to-enhance-city-management, accessed 25 August 2022.

135 "Alibaba Cloud Launches Malaysia City Brain to Enhance City Management," *Alibaba Cloud*, 29 Jan. 2018,

https://www.alibabacloud.com/press-room/alibaba-cloud-launches-malaysia-city-brain-to-enhance-city-management, accessed 25 August 2022.

136 Tan, CK. "Malaysian Police Adopt Chinese AI Surveillance Technology." *Nikkei Asia*, 18 Apr. 2018, https://asia.nikkei.com/Business/Companies/Chinas-startup-supplies-AI-backed-wearable-cameras-to-Malaysian-police.

137 Li, Tao. "Malaysian Police Wear Chinese Start-up's AI Camera to Identify Suspected Criminals." *South China Morning Post*, 20 Apr. 2018, https://www.scmp.com/tech/social-gadgets/article/2142497/malaysian-police-wear-chinese-start-ups-ai-camera-identify.

138 Andersen, Ross. "The Panopticon Is Already Here." *The Atlantic*, Sept. 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

139 "Malaysian Clients Return to XLY for Visit and Training [马来西亚客户再次莅临效率源参观培训]." Sohu [搜狐], 30 Sept. 2018, https://www.sohu.com/a/257093413_100124117.

140 "Malaysia and Huawei Open Southeast Asia's First Cyber Security Center to Support 5G Growth [Malaysia dan Huawei membuka pusat keselamatan siber pertama di Asia Tenggara untuk menyokong pertumbuhan 5G]." *ASEAN Today*, 26 Feb. 2020, https://www.aseantoday.com/2021/02/malaysia-and-huawei-open-southeast-asias-first-cybersecurity-center-to-support-5g-growth/?lang=ms.

141 "First International Law Enforcement Training Base Licensed by the Ministry of Public Security Opens in Yancheng". **[**首个公安部授牌的国际执法培训基地落户盐城]. *China Youth Daily*, April 12 2018, https://web.archive.org/web/20240327140023/ https://shareapp.cyol.com/cmsfile/News/201804/12/share74661.html?t=1543681818&nid=. Archived March 24 2024.

142 Ibid.

143 "International style! Yancheng welcomes African guests and friends - Guinea-Bissau presidential palace guard training class comes to Yancheng for inspection and exchange." [国际范儿！盐城喜迎非洲宾朋 ——几内亚比绍总统府卫队培训班来盐考察交流]. *Jiangsu Police*. June 3 2018. https://web.archive.org/web/2/ https://www.sohu.com/a/233924974_100135080. Archived March 24 2024.

144 "Introduction to the College". [学院介绍]. Shandong Police College. https://web.archive.org/web/20230923233804/http://www.sdpc.edu.cn/xygk/xyjj.htm. Archived Sept 23 2023.

145 Ibid.

146 "2018 Guinea Large-Scale Public Incident Management Advanced Course Begins at the College [2018年几内亚大型公共突发事件处置研修班在我院开班]." Shandong Police College [山东警察学院], 11 Nov. 2019, https://web.archive.org/web/20210725101728/http://wjpxb.sdpc.edu.cn/info/1046/1614.htm. Archived July 25 2021.

147 "Introduction to the College". [学院介绍]. Shandong Police College. https://web.archive.org/web/20230923233804/http://www.sdpc.edu.cn/xygk/xyjj.htm. Archived Sept 23 2023.

148 "College Introduction [学院简介]." *Zhejiang Police College* [浙江警察学院], https://www.zjjcxy.cn/zhu/xyjj/index.html, accessed 30 Nov. 2022.

149 "School Introduction [学校简介]." *Criminal Investigation Police University of China* [中国刑事警察学院], www.cipuc.edu.cn/

xxgk1/xxjj.htm, accessed 30 Nov. 2022.

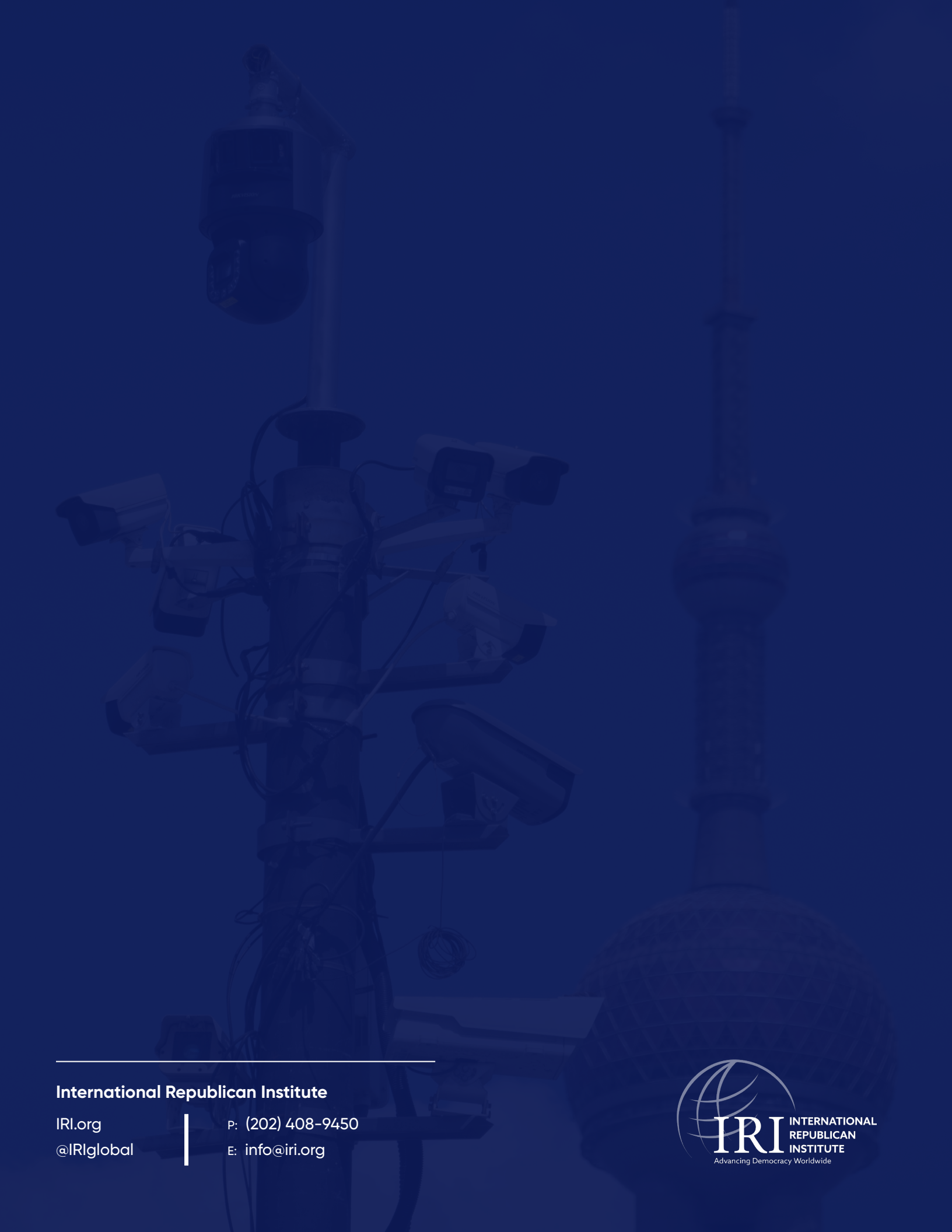
150 "Criminal Investigation Police University of China Holds 2019 Malaysia Counterterrorism Training Course Closing Ceremony [学院举行2019年马来西亚反恐培训班结业典礼]." *Criminal Investigation Police University of China* [中国刑事警察学院], 5 Jul. 2019, http://www.cipuc.edu.cn/info/2697/4491.htm.

151 Yau, Niva. "Chinese Governance Export in Central Asia." *Security and Human Rights*, 2 Feb. 2022, https://brill.com/view/journals/shrs/aop/article-10.1163-18750230-bja10009/article-10.1163-18750230-bja10009.xml.

152 Xu Nan [徐南]. "Yunnan Police College Introduction [云南警官学院简介]." *Yunnan Police College* [云南警官学院], 16 Jun. 2015, https://www.ynpc.edu.cn/site/ypoa/xyjj/info/2015/3860.html.

153 "Law Enforcement Liaison Chinese-Language Training Program Opening Ceremony Is Held at the University [执法联络员汉语培训项目开学典礼在我校举行]." Beijing Foreign Studies University [北京外国语大学], 23 Oct. 2009, https://news.bfsu.edu.cn/article/534/cate/4.

154 "Public Security Bureau: Beijing Foreign Studies University Law Enforcement Liaison Training Program Holds Its Eighth Opening Ceremony [公安部-北外执法联络员培训项目第八期开学典礼举行]." *Beijing Foreign Studies University* [北京外国语大学], 28 Oct. 2013, https://news.bfsu.edu.cn/article/5648/cate/0.



International Republican Institute

IRI.org
@IRIglobal

P: (202) 408-9450
E: info@iri.org

INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide