PRIVACY INTERNATIONAL

How China is supplying surveillance technology and training around the world

February 2019

How China is supplying surveillance tools, technology, and training around the world

i. Anti-Cyberterrorism Cooperation

To a large extent, formalised Chinese cyber diplomacy over the past decade has focused on combating 'cyberterrorism,' a category of online activities that corresponds with China's unusually broad definition of terrorism.[1] The focus on cyber terrorism originated from the Shanghai Cooperation Organization (SCO), which has centred around eradicating the "three evils"--"terrorism, separatism, and extremism." The SCO's anti-terrorism efforts have increasingly focused on online activities of terrorists as the threat from Uighur separatists has gone online. In October 2015, China conducted its first joint cyber anti-terrorism exercise in Xiamen, China for SCO member states.[2]

In recent years, China has sought to extend its cyberterrorism cooperation beyond the SCO, utilising multilateral bodies like the UN, BRICS, and the Asia-Pacific Economic Cooperation (APEC). In September 2014, at the UN Security Council Summit on Terrorism, Chinese Foreign Minister Wang Yi noted that "social media has become a battlefield for terrorist and extremist groups to instigate their ideology, a tool to plot terrorist attacks and a platform to recruit terrorists." He called on the UN to put forward "resolute measures" to limit the spread of extremist content on social media. China's 2016 National Cyber Strategy expressed Beijing long-term goal of ratifying an international treaty for countering terrorism in cyberspace.

ii. Cybersecurity and Content Moderation Assistance

Beyond cyber terrorism cooperation, China is increasingly willing to spread its model of information management and cyber governance through bilateral channels. After selecting Tanzania for a pilot country for a Belt and Road Initiative capacity building program in 2015, Tanzania's National Assembly began passing restrictions on internet content and blogging, a decision which appears to be influenced by technical assistance that Chinese government provided.[3] In Russia, Chinese top cyber officials helped promote China's version of internet controls in 2016, around the time that Russia's parliament was drafting Yarovaya's law. [4] Zambia is currently drafting a cyberlaw that would emulate China's approach to policing the web.[5]

---

[1] China defines terrorism as anything that causes "chaos in the social order."'China: Legal Definition of Terrorist Activities Clarified," Library of Congress, http://www.loc.gov/law/foreign-news/article/china-legal-definition-of-terrorist-activities-clarified/

[2] "SCO hosts first joint online counter-terrorism exercise in China," China Military, Oct. 15, 2015, http://english.chinamil.com.cn/view/2015-10/15/content_7130465.htm

[3] Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," The Atlantic, Jun. 28, 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

[4] Samuel Wade, "Chinese Cyberchiefs Preach Net Sovereignty in Moscow," China Digital Times, April 27, 2016, http://chinadigitaltimes.net/2016/04/chinese-cyberchiefs-preach-Internet-sovereignty-moscow/.

[5] Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain," Bloomberg Businessweek, Jan. 20, 2019, https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain.

In total, Freedom House reports 38 cases of foreign officials or media elites participating in Chinese training on media and information management since 2017.[6] China has been particularly active at spreading its model to Belt and Road Initiative (BRI) countries and has offered technological solutions to help foreign governments manage the web. In November 2017, the CAC held a "cyberspace management seminar for BRI countries officials" in Beijing.[7] The event was co-hosted with iiMedia, a Chinese company that specialises in third-party data mining related to online media. The company demoed its big data media management platform for foreign guests. The platform is advertised as offering comprehensive control of public opinion, including providing early-warnings for "negative" public opinions and helping guide the promotion of "positive energy" online. It is unclear which countries' representatives attended, or whether iiMedia was able to sell any foreign governments on its public opinion product.

Despite these known cases, there is extremely limited public information about Chinese exchanges and cooperation with foreign governments over censorship and internet issues. Several NGOs have reported that Cambodian censors have traveled to China for training.[8] When Vietnam passed its cybersecurity law in 2017, many observers noted the striking similarities between the law and China's 2016 Cybersecurity Law.[9] Freedom House connects a series of Chinese training sessions with Vietnamese officials in 2016 and 2017 to the passage of the cybersecurity law.[10] Yet, it is unclear whether the law was developed through direct consultation with Chinese policymakers, or merely designed to emulate China's cybersecurity law.

Beijing has also attempted to control the media environment in BRI countries, cultivating ties with media outlets by providing their staff with all-expenses-paid trips to China and other forms of inducement.[11]

iii. Military and Security Assistance

The China-Africa White Paper, published in 2015, stated that China would play a role in "maintaining and promoting peace and security in Africa," including through helping African countries improve their counter-terrorism capabilities.[12] During his 2015 UN General Assembly speech, President Xi Jinping promised $100 million in security assistance to African Union countries over a five year period.[13] The first major disbursement of that aid was made in February 2018, when China provided

---

[6] Freedom House, "Freedom On the Net 2018: The Rise of Digital Authoritarianism," Pg. 9, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

[7] "一带一路"沿线国家政府网络监管部门官员代表团到访艾媒," iiMedia, Nov. 14, 2017, http://www.iimedia.cn/59716.html.

[8] Based on insight from interactions with journalists.

[9] "Vietnam's Cybersecurity Draft Law: Made in China?," The Vietnamese, Nov. 8, 2017, https://www.thevietnamese.org/2017/11/vietnams-cyber-security-draft-law-made-in-china/.

[10] PI could not find evidence that Chinese officials had a direct role in drafting Vietnam's Cybersecurity Law.

[11] For example, see "Cambodia's Fresh News: is it journalism with Chinese characteristics?," SCMP, June 3, 2018, https://www.scmp.com/news/asia/east-asia/article/2149029/cambodias-fresh-news-it-journalism-chinese-characteristics

[12] "Full Text: China's second Africa policy paper," China Daily, May 12, 2015, http://www.chinadaily.com.cn/world/XiattendsParisclimateconference/2015-12/05/content_22632874.htm

[13] "Read the full text of Xi Jinping's first UN address," Quartz, Sept. 29, 2015, https://qz.com/512886/read-the-full-text-of-xi-jinpings-first-un-address/

$25 million in military equipment to an AU logistics base.[14] China provided another $30 million USD to build a military training center in Tanzania.[15] It unclear what type of equipment was transferred in both cases—further investigation is warranted.

China has also built up security cooperation with African countries through forums like the annual Forum on China-Africa Cooperation (FOCAC) and the new China-Africa Defense Forum. The first-ever China-Africa Defense Forum concluded in July 2018 with a resolution to increase cooperation in areas like counter-terrorism, cybersecurity, and technology projects like safe cities.[16] Whether this resolution will yield tangible cooperation remains to be seen.

iv. Drones and Satellites

Military-grade drones are a growing export for China. In October 2018, China sold Pakistan 48 Wing Loong II, a cutting-edge reconnaissance, strike and multi-role endurance UAV similar to the MQ-9 Reaper drone.[17] The year before China sold the Wing Loong II to the UAE and Egypt expressed interest in purchasing up to 300 Wing Loong II UAVs.[18] The Wing Loong II is only China's latest strike-capable drone available for export. Since 2014, China has sold the Caihong-4, China's most popular UAV, to over 30 countries.[19]

The primary appeal of the Wing Loong II and the CH-4 appears to be less the surveillance capabilities of the UAVs than their ability to project lethal force.[20] U.S. export controls on armed drones have created a large market opportunity for Chinese drones that offer attack capabilities. Reports suggest that the Caihong-4 has been used for targeted killings in Iraq and Yemen over the past few years.[21]

---

[14] Michael Kovrig, China Expands Its Peace and Security Footprint in Africa," International Crisis Group, https://www.crisisgroup.org/asia/north-east-asia/china/china-expands-its-peace-and-security-footprint-africa

[15] "China Global Security Tracker N.03," IISS, Sept. 13, 2018, https://www.iiss.org/blogs/analysis/2018/09/china-global-security

[16] "What to know about China's ties with Africa, form aid to infrastructure," South China Morning Post, July 22, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2156279/what-know-about-chinas-ties-africa-aid-infrastructure;" "首届中非防务安全论坛"中国的国防科技工业"专题交流活动在京举行," July 2, 2018, http://www.sohu.com/a/238834970_313834

[17] "China to sell 48 high-end military drones to Pakistan, The Economics Times, Oct. 10, 2018, https://economictimes.indiatimes.com/news/defence/china-to-sell-48-high-end-military-drones-to-pakistan/articleshow/66129500.cms

[18] https://thediplomat.com/2018/10/china-pakistan-to-co-produce-48-strike-capable-wing-loong-ii-drones/

[19] "China spreads its global wings via armed drone sales to Middle East," The Sydney Morning Herald, Oct. 4, 2018, https://www.smh.com.au/world/middle-east/china-spreads-its-global-wings-via-armed-drone-sales-to-middle-east-20181004-p507sp.html; 无人机领域军民融合升温 彩虹无人机完成上市," China Net, Feb. 13, 2018, http://military.china.com.cn/2018-02/13/content_50506858.htm

[20] "UAE deploys Wing Loong II UAV to Eritrea," Jane's 360, https://www.janes.com/article/82382/uae-deploys-wing-loong-ii-uav-to-eritrea

[21] "Egyptian Air Force Signs Agreement To Buy Chinese Drones," DefenseWorld.Net, Dec. 7, 2018, https://www.militarytimes.com/news/your-military/2018/10/03/chinese-armed-drones-now-flying-over-mideast-battlefields-heres-why-theyre-gaining-on-us-drones/; and "伊拉克军官介绍中国无人机实战：260 次打击弹无虚发," Sina Military, Feb. 17, 2018, http://mil.news.sina.com.cn/jssd/2018-02-17/doc-ifyrrmye2266090.shtml

The export of Chinese commercial drones have been a boon for government and private surveillance. Chinese dronemaker DJI controls around 70% of the commercial UAV market and is known for selling sophisticated drone technology at an affordable price.[22]

In recent years, DJI has aggressively marketed its drones to police and public safety forces around the world, creating specific software applications to appeal to law enforcement.[23] In December 2018, the New York Police Department announced that it acquired 14 DJI drones for "map crime scenes, monitor large events and aid search-and-rescue operations."[24] DJI drones are reportedly used by law enforcement in Mexico, the United Kingdom, and a number of cities in the United States.[25] In June 2018, DJI announced an exclusive partnership with Axon, an Arizona-based company that markets technology and weapons to law enforcement, to sell DJI drones to law enforcement around the world.[26]

We have so far found no direct evidence that the Chinese government has been involving in facilitating the transfer of DJI drones or other commercial drones to foreign law enforcement. Security vulnerabilities and revelations that a number of DJI product send data back to China have sparked fears that the company's drones could be a vector for Chinese espionage and intelligence-gathering.[27]

Increasingly, the Chinese government is also exporting the Beidou Navigation Satellite (BDN), China's answer to the GPS, which has surveillance applications. On the Afghan border, the People's Liberation Army (PLA) has used the BNS to enhance surveillance and situational awareness over hard-to-patrol territory.[28] The BNS is poised to gain global coverage by 2020; as such, the Chinese government is looking to market the navigation system to foreign clients.[29] At the first China-Arab States Beidou System Cooperation Forum in early 2018, China signed an agreement with a number of Arab states to promote the BDS.[30] The China-Arab Beidou System/Global Navigation Satellite System Center, the first overseas Beidou "center of excellence," was opened in Tunisia in April 2018.[31] China has also signed

---

[22] "Drone giant DJI is building a new headquarters as a 'floating community' with a giant sky bridge to test drones," CNBC, San. 17, 2018, https://www.cnbc.com/2018/06/15/dji-futuristic-new-headquarters.html
[23] For example, see "How DJI Drones Empower Public Safety Teams," DJI Enterprise, https://enterprise.dji.com/civil-protection
[24] "New York Police Say They Will Deploy 14 Drones," The New York Times, Dec. 4, 2018, https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html
[25] "A Single Drone Helped Mexican Police Drop Crime 10 Percent, Wired, June 11, 2018, https://www.wired.com/story/ensenada-mexico-police-drone/
[26] "DJI And Axon Announce Drone Partnership To Strengthen Law Enforcement Tools For Public Safety, DJI Newsroom, June 5, 2018,https://www.dji.com/newsroom/news/dji-axon-air-drone-partnership-public-safety-law-enforcement
[27] "Yes, drone biz DJI's Go 4 app does phone home to China – sort of," The Register, Apr. 25, 2018, https://www.theregister.co.uk/2018/04/25/dji_data_security_audit/; For more information, see "Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government," U.S Homeland Security SAC Intelligence Los Angeles, Aug. 9, 2017, https://info.publicintelligence.net/ICE-DJI-China.pdf
[28] "China Incorporates BeiDou Navigation Satellite for Military Surveillance," EurAsian Times, Feb. 2, 2019, https://eurasiantimes.com/china-incorporates-beidou-navigation-satellite-for-military-surveillance/
[29] 今天以后，无论你走到哪里，北斗将始终伴你左右！, Military-Civil Integration in ICT Magazine, Dec. 27, 2018, https://mp.weixin.qq.com/s?__biz=MzI0NjU2NDMwNQ==&mid=2247487204&idx=1&sn=05f57a9caef9c92f4bfdfee84963bb2d&chksm=e9bc1a5adecb934ce0751d663b6f8557e8756aefd28cc67ffe1153890ed0e3f995490f622492&scene=0&xtrack=1#rd
[30] "China Global Security Tracker No. 1, MERICS, Apr. 10, 2017,https://www.merics.org/en/merics-trackers/china-global-security-tracker-1
[31] "IISS.

agreements with Malaysia, Cambodia, Iran, India, and Indonesia to use the BNS for applications ranging from policing and emergency response to smart transportation management.[32]

v. Police-to-Police Cooperation

In South Africa, an increase in police-to-police cooperation and training coincided with an increase in surveillance. Since 2005, China has opened 13 police co-op units in Johanessburg with buy-in from local politicians to accommodate Chinese nationals living in the country and build relationships with the local police force.[33] In September 2018, Johannesburg announced a major upgrade of the city's CCTV system to accommodate smart applications like facial recognition.[34] The decision was reached after a delegation of parliamentarians traveled to Shanghai to learn how to improve South African policing.[35] The delegation reportedly toured Shanghai's Public Security Bureau's 24-hour command center.

vi. The Digital Silk Road and Smart Cities

The Digital Silk Road (DSR), a subset of the BRI Initiative, has played an important role in spreading Chinese ICT equipment, including surveillance equipment, across Central Asia and North Africa. At the 2017 World Internet Conference in Wuzhen, China, representatives from Saudi Arabia, Egypt, Turkey, Thailand, Laos, Serbia, and the United Arab Emirates signed a "Proposal for International Cooperation on the 'One Belt, One Road' Digital Economy," an agreement to construct a "Digital Silk Road" to improve digital network connectivity, small and medium enterprise (SME) development, and e-commerce cooperation.

The primary goal of the DSR is to promote internet-based interconnectivity, and as such, building internet infrastructure, including undersea and land-based fiber optic cables, and mobile networks, has been a key focus. However, increasingly, China's tech unicorns are eager to bring their strengths in e-commerce, fintech, cloud computing, and other digital services to the DSR. Smart cities and "safe cities"—which heavily lean on surveillance equipment and intelligent sensors to feed data into a central computing platform —have been a niche but growing part of the DSR. ZTE claims that it has implemented smart city solutions in 60 cities across 45 countries since 2014. Huawei has also been particularly active in smart city construction.

---

[32] 北斗卫星民用市场现状与发展前景, Military-Civil Integration in ICT Magazine, May 4, 2018, https://mp.weixin.qq.com/s?__biz=MzI0NjU2NDMwNQ==&mid=2247485659&idx=2&sn=e5394d23207441f0e66d812ad09e213b&chksm=e9bc1c65decb9573bb0ae2d31beffc28a2db649f7e67956470fb64736552964367a1bb55b9f9&scene=0#rd

[33] "AFP Factcheck: No, the Chinese are not opening police stations in South Africa," AFP, Nov. 12, 2018, https://factcheck.afp.com/no-chinese-are-not-opening-police-stations-south-africa

[34] Heidi Swart, " oburg's new hi-tech surveillance cameras: A threat to minorities that could see the law targeting thousands of innocents," Daily Maverick, Sept. 28, 2018, https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/

[35] Swart.

Huawei has made a clear bet on a subset of smart city projects focused on crime fighting. This suggests that the company sees clear business potential in using smart city technology to tame crime-ridden cities around the world. 'Safe cities' are a particular configuration of the company's smart city product, which utilises intelligent CCTV systems, drones, a 4G eLTE wireless broadband network to connect devices, and a unified data center to process data. The company has implemented Safe Cities projects in Serbia, Malta, the Philippines, Mauritius, Kenya, Pakistan, and South Africa, among other countries.[36]

vi. AI and Big Data Policing

Having pioneered cutting-edge facial recognition technology at home, China is increasingly exporting the technology abroad. Freedom House's 2018 report found 18 instances of countries deploying Chinese-developed AI security systems since 2017.[37]

Notable examples include,

- In Zimbabwe, Chinese AI unicorn CloudWalk won a contract to deploy facial recognition cameras in airports and other public spaces and build a national facial recognition in what appears to be Africa's first AI surveillance project.[38] The deal is still being negotiated because CloudWalk wants to export facial data acquired through the project back to China, and the Zimbabwean government is hoping to extract a lower price in exchange for the data.
- AliCloud, the cloud computing arm of Alibaba, is building a 'City Brain' in Kuala Lumpur, Malaysia, which will use cloud computing, AI, and intelligent sensors to optimise traffic and improve urban management.[39]
- Facial recognition startup SenseTime signed three MOUs in Singapore to collaborate on R&D.[40] At the same time, the company has shown interest in bidding on a "Lamppost-as-a-Platform" pilot project to install facial recognition cameras on lampposts across the city.[41]
- Yitu, another facial recognition startup, which collaborates with public security bureaus within China, agreed to supply Malaysian police with facial recognition-enabled wearable cameras.[42]

---

[36] "Huawei Safe City Solution: Safeguards Serbia," Huawei, Aug. 28, 2018, https://e.huawei.com/en/case-studies/global/2018/201808231012; Memorandum of Understanding on Safe City signed by government and Huawei, Independent.com, Sat. 16, 2016, http://www.independent.com.mt/articles/2016-04-16/local-news/Memorandum-of-Understanding-on-Safe-City-signed-by-government-and-Huawei-6736156424; "Making Manila's 'Crown Jewel' a Safe City," Huawei, Apr. 4, 2017, https://e.huawei.com/en/case-studies/global/2017/201704261658; "Mauritius, the Inspiration for Heaven," Huawei, Jul. 7, 2018, https://e.huawei.com/en/case-studies/global/2018/201807241004; Lahore Implements Huawei Safe City Solution," Huawei—Video Library, https://e.huawei.com/se/videos/global/2018/201809121021; "Protecting Enchanted Kenya," Huawei, Mar. 14, 2016, https://e.huawei.com/en/case-studies/global/2016/201603141435.

[37] PI could not independently verify all the cases mentioned in the Freedom House report. Freedom House, pg.

[38] Prasso; and "Amy Hawkins, "Beijing's Big Brother Tech Needs African Faces," Foreign Policy, Jul. 24, 2018, https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/; and "向非洲出口黑科技 中国"鹰眼"将服务津巴布韦," S&T Daily, Apr. 12 2018, http://www.stdaily.com/kjrb/kjrbbm/2018-04/12/content_658070.shtml

[39] "Alibaba Cloud Launches Malaysia City Brain to Enhance City Management," AliCloud, Jan. 29, 2018, https://www.alibabacloud.com/press-room/alibaba-cloud-launches-malaysia-city-brain-to-enhance-city-management

[40] "Chinese AI unicorn SenseTime signs MOU with 3 Singapore organisations," Channel NewsAsia, Jun. 29, 2018, https://www.channelnewsasia.com/news/technology/chinese-ai-unicorn-sensetime-signs-mou-with-3-singapore-10484136.

[41] The current status of the bid and project is unclear. "Singapore to test facial recognition on lampposts, stoking privacy fears," Reuters, Apr. 13, 2018, https://www.reuters.com/article/us-singapore-surveillance/singapore-to-test-facial-recognition-on-lampposts-stoking-privacy-fears-idUSKBN1HK0RV.

> The company has opened up offices in South Africa and Singapore and plans to expand to Europe.[43] In September 2018, Yitu signed a strategic partnership with the UN Industrial Development Organization Shanghai's Investment and Technology Promotion Office to encourage the adoption of AI in developing countries.[44]

While media outlets have connected these instances to China's surveillance state at home, the Chinese government appears to have limited involvement in these projects and has not actively promoted AI facial recognition technology abroad so far.[45]

Indirect Assistance: Mapping State Involvement in Commercial Channels

A survey of Chinese and international source finds that a majority of Chinese security surveillance takes the form of commercial transactions. Major Chinese surveillance equipment providers like Huawei, ZTE, Hikvision, and Dahua are among the biggest providers of surveillance equipment internationally. In addition, a new generation of AI unicorns that specialise in facial recognition and object recognition like SenseTime, Yitu, and Cloudwalk have also begun competing in the international marketplace, marketing their facial recognition systems to cities and police forces abroad.

A number of media article and reports equate these companies' commercial activities abroad with directed Chinese government security assistance.[46] In reality, Chinese surveillance companies, including those that are partially state-owned (e.g. Hikvision, ZTE, Dahua), function as commercial actors abroad and do not receive direct state support to facilitate a vast majority of their commercial transactions.[47] Hikvision, for example, is the biggest provider of CCTVs to the United Kingdom but does not rely on government-to-government security assistance.[48] 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.

---

[42] "Malaysian police adopt Chinese AI surveillance technology," Nikkei Asian Review, Apr. 18, 2018, https://asia.nikkei.com/Business/Companies/Chinas-startup-supplies-AI-backed-wearable-cameras-to-Malaysian-police

[43] "Chinese facial recognition start-up eyes global opportunities beyond public security, SCMP, https://www.scmp.com/tech/start-ups/article/2121100/chinese-facial-recognition-start-eyes-global-opportunities-beyond

[44] "AI startup YITU signs deal with UN body to aid developing nations," China Daily, Sept. 20, 2018, http://www.chinadaily.com.cn/a/201809/20/WS5ba350d3a310c4cc775e757f.html

[45] There is reason to suspect that a state-bank is financing the CloudWalk deal in Zimbabwe, but PI could not independently confirm the financing arrangement.

[46] Freedom House.

[47] Indirect forms support are important to consider as well. These include direct subsidies from the government, preferential loans from state banks, and large contracts from the central government or provincial security bureaus. Together these factors have allowed Chinese surveillance manufacturers to expand abroad and dominate the international market for surveillance equipment. See Anjani Trivedi, "China's Spy-Tech Star Needs Some Covert Help," Bloomberg, Oct. 22, 2018, https://www.bloomberg.com/opinion/articles/2018-10-22/china-s-spy-tech-star-hikvision-needs-covert-help-from-beijing.

[48] Patrick Gysin, "State-controlled Chinese company is UK's biggest CCTV provider – but has NEVER been security checked," The Sun, Sept. 16, 2016, https://www.thesun.co.uk/news/1793964/state-controlled-chinese-company-is-uks-biggest-cctv-provider-but-has-never-been-security-checked/

Still, the government's role is in these companies' success abroad is important to consider. Major sources of overseas business correlate strongly with illiberal regimes where state-to-state cooperation is already strong. Channels of state-support for commercial surveillance companies include,

- **State financing.** Loans from state-banks are important enablers for overseas projects, especially in countries without the financial resources to afford cutting-edge surveillance technology. Often, surveillance equipment will be an upsell on a much larger project, like a 4G mobile network infrastructure project. Samples include,
    - According to *Dawn,* Pakistan received a loan from China's Export and Import Bank to finance a Huawei safe city project in Islamabad.[49] A Huawei smart city project in Kyrgyzstan was funded in part by a Chinese state fund.[50]
    - Ecuador received a $240 million loan from China to build the ECU 911 center, a state-of-the-art national emergency response and video surveillance system built by China National Electronics Import and Export Corporation (CEIEC).[51]
    - According to *Reuters,* Venezuela is partially relying on the Venezuela China Joint Fund—a financing program that allows Venezuela to pay for Chinese loans with crude oil shipments—to finance a ZTE identification card and monitoring system, which has been likened to China's social credit system.[52]
    - China provided a $105 million loan to Bolivia to install more than 600 CEIEC security cameras.[53]

- **Chinese commercial diplomacy.** In several cases, Chinese diplomats and officials have interceded on behalf of Chinese companies to sell foreign officials on Chinese surveillance and digital control technology. Conferences and expos, with the state's imprimatur, also appear to facilitate the expansion of Chinese surveillance technology into foreign countries:
    - *The Guardian* reported that Chinese officials interceded on Huawei behalf to help it profit from the implementation Yarovaya's law in Russia, which required data storage and server technology to fulfill the data localisation requirement of the law.[54]
    - In Malaysia, Chinese diplomats have included Alibaba CEO Jack Ma in several high-level meeting with the Malaysian government, which likely played a role in Prime Minister Datuk Seri Najib Razak decision to appoint Ma as the country's digital economy advisor in 2016.[55]

[49] "Chinese firm to provide equipment for safe city project," Dawn, Mar. 22 2014, https://www.dawn.com/news/1094735/chinese-firm-to-provide-equipment-for-safe-city-project
[50] "China's Huawei to implement Smart City project in Kyrgyzstan," 24.kg News Agency, Jan. 12, 2018, https://24.kg/english/73115_Two_Chinese_and_one_domestic_company_to_invest_in_Smart_City/
[51] Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China," Foreign Policy, Aug. 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/; and "Feature: Chinese technology brings falling crime rate to Ecuador," Xinhua, Jan. 19, 2018, http://www.xinhuanet.com/english/2018-01/19/c_136908255.htm.
[52] Augus Berwick, "How ZTE helps Venezuela create China-style social control," Reuters, Nov. 14, 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/
[53] Raquel Carvalho, "In Latin America, Big Brother China is Watching You," Dec. 21, 2018, https://www.scmp.com/week-asia/geopolitics/article/2178558/latin-america-big-brother-china-watching-you
[54] "Putin brings China's Great Firewall to Russia in cybersecurity pact," The Guardian, Nov. 29, 2016, https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact
[55] "Malaysian PM's visit to open up new prospects for bilateral ties: Chinese envoy," Xinhua, Aug. 17, 2018; "Malaysia appoints Alibaba's Jack Ma as digital economy adviser," Malay Mail, Nov. 4, 2016,

- Sengalese President Macky Sall was taken to visit Hikvision and Alibaba during a state visit to China.[56]
- Chinese officials accompanied a Pakistani delegation visiting Huawei's headquarters in Beijing.[57]

- **"Going out" policies including the Belt and Road Initiative.** State initiatives are a powerful engine for the expansion of commercial surveillance through large public works projects. In addition, telecoms and electronic companies that participate in BRI are granted access to preferential loans and buyer credits. [58]
  - According to Pakistani newspaper *Dawn,* an agreement for China-Pakistan Economic Corridor, Pakistan's leg of the Belt and Road Initiatives, included a contract to build a large-scale surveillance systems and 'safe cities' in major Pakistani cities.[59]

Authored by Lorand Laskai, who is a JD Candidate at Yale Law School.

---

https://www.malaymail.com/news/malaysia/2016/11/04/malaysia-appoints-alibabas-jack-ma-as-digital-economy-adviser/1242619

[56] "Where will African leaders who come to China go beside Beijing," The Paper, Sept. 6, 2018, https://baijiahao.baidu.com/s?id=1610870137610926678&wfr=spider&for=pc

[57] "Pakistani Delegation visits Huawei 'Safe-City Project,'" PhoneWorld, Mar. 17, 2015, https://www.phoneworld.com.pk/pakistani-delegation-visits-huawei-safe-city-project-beijing/

[58] "China's Telecommunications Footprint in Africa," Institute of Developing Economies, Japan External Trade Organization, Oct. 2009, www.ide.go.jp/English/Data/Africa_file/Manualreport /cia_09.html

[59] Khurram Husain, "Exclusive: CPEC master plan revealed," *Dawn,* Jun. 21, 2017, https://www.dawn.com/news/1333101/exclusive-cpec-master-plan-revealed

PRIVACY INTERNATIONAL

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471