Hertie School
Centre for
International Security

Security Tech Brief

May 2023: Exporting Chinese Surveillance Technology

The West Balkans and Chinese Surveillance Technology

Hertie School
Centre for
International Security

Security Tech Brief:

Exporting Chinese Surveillance Technology

In recent years, the People's Republic of China has begun exporting surveillance technology it uses domestically to countries abroad through strategic policies (such as the Belt and Road Initiative) and via Chinese companies (such as Huawei). Serbia has welcomed Chinese investments in surveillance technologies, but a Huawei project to install 1000 cameras with face-and license-plate-recognition technology in Belgrade has triggered a public backlash. There is no indication so far that this technology is being misused – e.g. to target minorities or spy on opposition politicians – but observers point out that little is known about how the Serbian authorities are using this technology. Another key concern is that the Chinese government might gain access to sensitive information through Chinese-linked technology used by European governments (such as surveillance cameras on military sites). For instance, in November 2022, the British government instructed its departments to stop installing Chinese-made security cameras in sensitive areas, citing security concerns.

History of Chinese Engagement in Serbia:

2009 ● China and Serbia establish a strategic partnership, with the aim of deepening cooperation between the two states in various areas. While prior engagement was constrained, the states stressed the broadening of friendly relations between China and Serbia as a shared aspiration.

2014 ● Pupin Bridge construction is completed, China's first major infrastructure project in the region. In 2014, Chinese authorities arrest a hit-and-run suspect that fled from Serbia to China, prompting increased dialogue on further cooperation in the security field between the two countries.

2017 ● Huawei becomes a partner for the Serbian government in advancing digitalisation. The company becomes the Ministry of Interior's partner in the security field, establishing smart surveillance.

2019 ● The Serbian Ministry of the Interior installs 1,000 Huawei surveillance cameras with face-recognition technology in 800 locations around Belgrade, the capital of Serbia. Serbian authorities have provided few details about the contract with Huawei, triggering a public backlash.

Geopolitics in the Western Balkans:

The confrontation between China and the U.S. about global digital infrastructure is reproduced in the Western Balkans. In 2020, the U.S. launched the Clean Network Initiative (CNI) to secure digital trust standards across a coalition of democracies, explicitly naming the Chinese government (and associated companies) as a threat.

Bosnia and Herzegovina

- Not in EU (candidate status)
- Not a NATO member (MAP status)
- Did not sign the CNI
- 29 Chinese projects

Montengro

- Not in EU (candidate status)
- NATO member
- Did not sign CNI
- 9 Chinese projects

Albania

- Not in EU (candidate status)
- NATO member
- Signed the CNI
- 8 Chinese projects

Serbia

- Not in EU (candidate status)
- Not a NATO member
- Did not sign CNI, but pledged to ban "untrusted vendors" of 5G technology through agreement signed with Kosovo
- 61 Chinese projects

Kosovo

- Not in EU (potential candidate status)
- Not a NATO member
- Signed the CNI
- 0 Chinese Projects

North Macedonia

- Not in EU (candidate status)
- NATO member
- Signed the CNI
- 15 Chinese projects

Information about number of Chinese projects based on: https://china.balkaninsight.com/

Chinese surveillance technology

Over the last two decades, Chinese leadership has come to understand the importance of information collection, processing, and analysis for military power purposes.[1] Domestically, with the rapid increase in internet usage among the population, the government has utilised the cyber domain as a crucial aspect of their strategy, thereby tightening its presence and control of Chinese cyberspace.[2] China has been building up "the world's biggest digital surveillance network" for years.[3] The most evident manifestation of this lies in the networks of CCTV cameras equipped with facial and object recognition technology. However, other surveillance technologies also exist. While the government justifies this endeavour under the pretext of deterring crime, improving security, and maintaining "social stability"[4], others argue that this is done with the goal of tightening totalitarian control[5], i.e. building a digital authoritarian state.[6] Some describe it as arising from an uneasiness among Chinese leadership about what might occur when the "country's citizens go unwatched".[7]

By using technologies such as facial and object recognition, artificial intelligence, predictive policing software, and smartphone forensic systems, China has developed a nation-wide digital surveillance system. Chinese cities take up eight spots on the world's top 10 most surveilled cities[8], as the government has installed at least 200 million surveillance cameras across its urban and rural areas.[9] Authorities claim that the country's facial recognition system is capable of scanning "China's population of about 1.4 billion people in a second".[10] This means that authorities can track the population, i.e. their identity in public spaces, behaviour, location, movement, and other identifying information about their phones.[11] However, some experts doubt the sophistication of the surveillance system[12], mentioning bureaucratic barriers as a coordination problem for implementation.[13]

[1] Joe McReynolds, "China's Military Strategy for Network Warfare" China's Evolving Military Strategy, edited by Joe McReynolds, Brookings Institution Press, 2016, pp. 214–65. JSTOR, http://www.jstor.org/stable/10.7864/j.ctt21kk0ng.10

[2] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State" Journal of Democracy, vol. 30 no. 1, 2019, p. 53-67, https://doi:10.1353/jod.2019.0004

[3] Joyce Liu, "In Your Face: China's All-Seeing State", BBC News, December 10, 2017. https://www.bbc.com/news/av/world-asia-china-42248056

[4] See also: 2015 National Policy Document on "public safety video-surveillance construction, networking, and applications": http://web.archive.org/web/20160616221428/https://www.ndrc.gov.cn/zcfb/zcfbtz/201505/t20150513_691578.html

[5] Ross Andersen, "The Panopticon Is Already Here", The Atlantic, September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

[6] Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers", December 17, 2019, https://www.nytimes.com/2019/12/17/technology/china-surveillance.html

[7] Jessica Batke, Mareike Ohlberg, "State of Surveillance", China File, October 20, 2020, https://www.chinafile.com/state-surveillance-china

[8] Phoebe Zhang, "Cities in China most monitored in the world, report finds", South China Morning News, 19 August, 2019, https://www.scmp.com/news/china/society/article/3023455/report-finds-cities-china-most-monitored-world

[9] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras", New York Times, July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

[10] See: https://twitter.com/PDChina/status/978444380066390016

[11] Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers".

[12] Further reading: https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta?t=1654073214557

[13] Grady McGregor, "The world's largest surveillance system is growing—and so is the backlash", Fortune, November 3, 2020, https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/

History of surveillance

2003 Chinese leadership identified the public safety concerns that came along with urbanisation – insufficient urban population control, and the over-aggregation of population and industries in some large cities.[14] The government then formulated policy goals targeted toward maintaining social order, reducing the crime rate, and improving overall happiness in the city, whose achievement would involve security monitoring through technical means.

2005 The Ministry of Public Security and the Ministry of Industry and Information Technology jointly launched the Skynet project, which had the aim of installing CCTV systems in cities.[15] Skynet was piloted through the program "Strengthening Police with Science and Technology", which was launched in 21 pilot cities. Three years later, the number of cities included in the project reached 38 cities and has been growing steadily since.[16]

2015 Sharp Eyes was an upgrade to the previous Skynet project, as the transition to a market-based economy presented the leadership with new challenges and required new technologies. Moreover, while SkyNet largely focused on cities, Sharp Eyes was meant to target rural areas as well.[17] Officially launched in 2015 by a number of ministries and commissions, its stated goals included a 100% coverage of Chinese public spaces by 2020.[18] An integral part of Sharp Eyes was that the population was involved in the monitoring as well, as they could observe security footage within their local grid and report any misbehaviour or crime. Moreover, the technology used for Sharp Eyes varied significantly – private and government-owned surveillance cameras, both with and without facial or licence plate recognition technology, as well as software collecting "virtual identities", such as MAC addresses, phone numbers, or WeChat accounts.[19]

'Smart Cities' are a global phenomenon, understood to mean cities that possess technologies that use data to optimise city functioning, such as mobility, security, digital economy, and so on.[20] However, these technologies are often deployed for surveillance purposes, such as facial recognition, or automatic data mining.

[14] See more: http://www.qianjia.com/html/2017-03/20_267576.html
[15] Zhang Zihan, "Beijing's guardian angels?", Global Times, 10 October, 2012, https://www.globaltimes.cn/content/737491.shtml
[16] See more: http://www.qianjia.com/html/2017-03/20_267576.html
[17] Dahlia Peterson, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space", Centre for Security and Emerging Technology, Georgetown University, March 2, 2021, https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/
[18] Dahlia Peterson, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space"
[19] Dahlia Peterson, "How China harnesses data fusion to make sense of surveillance data", Brookings, September 23, 2021, https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/
[20] Robert Muggah, "Smart' Cities Are Surveilled Cities", FP, April 17, 2021, https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/

Surveillance technologies

Government usage has been the main driver of surveillance camera use in China, making it the world's fastest-growing user of the technology.[21] The cameras are equipped with facial recognition and intelligent analysis, meaning that people or objects and their features can be identified and recognized by the technology. This identification is then matched to an extensive face-data database that can generate analyses in real time, such as the size of a crowd, individuals' gender, characteristics of clothes, or vehicles.[22] In China, this technology is ubiquitous, even reaching classrooms and universities, raising concerns about academic freedom and privacy.[23] Often, facial recognition technology is used in tandem with other surveillance technologies, such as covert mobile phone trackers. In the Zhengzhou, the policy reportedly set up surveillance cameras combined with IMSI catchers (devices that collect identification codes from mobile phones).[24] This way, citizens' facial and mobile phone data is collected, and matched with varying levels of confidence to a specific person in a large-scale dataset. In other regions, additional data on licence plates, phone numbers, and other information is incorporated into the dataset as well. A surveillance technology brochure encompasses this idea simply: "People pass by and leave a shadow, the phone passes and leaves a number. The system connects the two". While happening on a large scale in China, similar practices have been noted in Western countries as well, such as by the New York City Police.[25]

Recent developments in the technology have seen a move beyond mere facial-recognition technology, as now, companies such as Taigusys produce "emotion recognition technology".[26] By using face muscle movements, vocal tones, and other signals, the technology allegedly infers a citizen's emotional state.[27] Scientists and scholars, however, point out the flaws in this, arguing that it is based on pseudo-science, and criticising it for endangering human rights. Non-democratic regimes could use the plethora of data on their population to track, identify, and target political opponents or members of minority groups. For example, a recent document showed that a Huawei facial recognition software used by the Chinese

[21] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State" Journal of Democracy, vol. 30 no. 1, 2019, p. 53-67, https://doi:10.1353/jod.2019.0004

[22] Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State"

[23] Zhang Zihan, "Beijing's guardian angels?", Global Times, October 10, 2012, https://www.globaltimes.cn/content/737491.shtml; An example from 2018 displays the sophistication of the facial-recognition technology. Namely, a criminal suspect was spotted and identified in a concert crowd of 60,000 people by the facial recognition technology. https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/

[24] Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers".

[25] Joseph Goldstein, "New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says", New York Times, February 11, 2016, https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html

[26] Michael Standaert, "Smile for the camera: the dark side of China's emotion-recognition tech", The Guardian, March 3, 2021, https://www.theguardian.com/global-development/2021/mar/03/china-positive-energy-emotion-surveillance-recognition-tech

[27] This has been happening simultaneously with the ideological discourse on "positive energy" in China, which encouraged its citizens to act positively, speak positively, and, presumably as a result, think positively – https://journals.sagepub.com/doi/full/10.1177/1868102619899409.

government can identify members of the Uyghur Muslims – an oppressed minority group[28] – and set off an alarm to local authorities to flag their presence. Journalists are also being targeted by surveillance technologies. A recently uncovered "traffic light" surveillance system in the Henan province classifies identified journalists into different color-coded categories, depending on the government's level of concern, meaning that the system can alert local authorities if a certain journalist enters their region.[29] Similar technologies have been used for foreign students and migrant women.[30]

To solidify their mass surveillance tactics, the Chinese government has turned to other forms of biometric data as well, namely voice and speech biometric data. With the pretext of identifying voices of those speaking during criminal activity[31], the Chinese government began collecting data on the voice patterns of its population. The technology can access voice data from phone calls, identify speech patterns, and identify the speakers without their knowledge. These efforts began in 2012, when the Ministry of Public Security established a national voice pattern database and selected the Anhui providence to test the program.[32]

A major actor seemingly collaborating with the Ministry of Public Security is the company iFlytek. It produces an overwhelming majority – 80 percent – of China's speech recognition software.[33] In only three years, 70,000[34] voice patterns have been collected.[35] Collecting data on voice patterns is only one part of the Chinese government's strategy to collect "multi-modal"[36] data on citizens – connecting voice data to fingerprints, facial data, ethnicity, and location. While governmental collection of biometric data is not illegal, it must adhere to the limitations enshrined in the International Covenant on Civil and Political Rights.[37] It is unclear to what extent iFlytek cooperates with the Chinese government, nor whether the data is being shared with government ministries. In iFlytek's customer privacy statement, confidentiality is ensured, but personal information may be disclosed "according to the demands of the relevant

[28] Human Rights Watch, "Break Their Lineage, Break Their Roots: China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims", April 19, 2021, https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting

[29] James Clayton, "China surveillance of journalists to use 'traffic-light' system", BBC News, November 29, 2021, https://www.bbc.com/news/technology-59441379

[30] James Clayton, "China surveillance of journalists to use 'traffic-light' system".

[31] Further reading (Mandarin): https://www.xueshu.com/jcjs/201204/7264986.html

[32] Human Rights Watch, "China: Voice Biometric Collection Threatens Privacy", October 22, 2017, https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy

[33] Human Rights Watch, "China: Voice Biometric Collection Threatens Privacy"

[34] Compared to the size of other databases, the voice pattern database seems to be the least advanced. The national police database covers circa 1 billion faces, and 40 million DNA samples. http://www.nciic.com.cn/fileHandle.do?action=read&objectID=20090303111108890

[35] Human Rights Watch, "China: Voice Biometric Collection Threatens Privacy", October 22, 2017, https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy

[36] Further reading (Mandarin): http://www.zgg.org.cn/zggxx/dshsk/dshhd/201205/t20120518_355390.html

[37] This means that governments may not use such data for administrative purposes or investigation of minor offences and must also inform citizens if their data is being used. For more information see: https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy

government departments”[38], and in the event of the government requesting information, iFlytek is not required to inform its users about it.

The “Chinese Model” as an export

China currently leads the world in exporting telecommunications, office, and telecom equipment and Chinese companies are the principal exporters of AI intelligence technology worldwide.[39] Parts of these exports are the surveillance technologies China uses domestically. Since 2016, President Xi Jin-ping has been globally promoting the “China model” for configuring social governance systems. Yet, critics view the model as a euphemism for comprehensive state repression in what some call “digital authoritarianism”.[40] Nevertheless, since 2016, the Chinese government has signed 116 deals with cities around the globe to construct city infrastructure like the Chinese “Safe”- and “Smart Cities” programs.[41] Many of these cities are part of the BRI. Chinese companies, such as Hikvision, Huawei, and ZTE have supplied artificial intelligence surveillance technology to a wide variety of countries – ranging from Australia to Myanmar.[42] In Kenya, for example, a Huawei-built system of surveillance cameras analyses cars and their passengers going in and out of the countries’ capital.[43] There are several explanations for China’s surveillance technology exports. Perhaps, China exports to unattractive markets for the West.[44] Potentially, China targets specific regions such as the Balkans hoping to create a domino effect that would allow it to gain a foothold in the European market. Safe and Smart Cities have also been understood as a vehicle for China to export its political values to the rest of the world.[45]

Finally, China might be pursuing this strategy to access information (such as population or infrastructure data) which could potentially be used for political advantage or blackmail. Several pathways exist through which China could retrieve sensitive data from actors such as Taiwan, the EU, or NATO. China is already collecting mass amounts of open-source data to support Chinese intelligence, military, security, and state operations.[46] In Taiwan, despite a ban, digital video recorders with Chinese Hikvision

[38] Human Rights Watch, “China: Voice Biometric Collection Threatens Privacy”.

[39] Ausma Bernot, “Digital authoritarianism not just a China problem”, Lowy Institute, September 22, 2021, https://www.lowyinstitute.org/the-interpreter/digital-authoritarianism-not-just-china-problem; Steven Feldstein, “How Much Is China Driving the Spread of AI Surveillance?” The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 2019, pp. 13–15. JSTOR, http://www.jstor.org/stable/resrep20995.7

[40] Adrian Shahbaz, “The Rise of Digital Authoritarianism”, Freedom House, 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

[41] While the difference between these two is mostly blurred, “Safe Cities” largely utilise cameras and other surveillance technology to monitor the local population, while “Smart Cities” also include technologies for automating a wider array of city functions, such as transport, garbage collection, and utility networks.

[42] Yuan Yung and Madhumita Murgia, “Facial recognition: how China cornered the surveillance market”, Financial Times, December 6, 2019, https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385

[43] Huawei reports that crime rates have decreased, while local officials see the impact as less strong. See: Yung and Murgia, “Facial recognition: how China cornered the surveillance market”

[44] Yung and Murgia, “Facial recognition: how China cornered the surveillance market”.

[45] James Kynge, Valerie Hopkins, Helen Warrell, and Kathrin Hille, “Exporting Chinese surveillance: the security risks of ‘smart cities’”, Financial Times, June 9, 2021, https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

[46] See for example: Wesley Rahn, “Data leak exposes China's new 'hybrid warfare'”, Deutsche Welle, September 29, 2020, https://www.dw.com/en/zhenhua-data-leak-exposes-chinas-new-hybrid-warfare/a-55083540; which is based on Christopher Balding, “Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua”, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691999

motherboards are still sold by local suppliers.[47] Moreover, the device's remote operating software is managed by Hikvision, which means that the Chinese government could technically store and access uploaded images.[48] In the U.S., several China-based companies have been investigated by the FBI and labelled as security risks following suspicious data transmission to China.[49] The British government has blocked further installations of Chinese-made security cameras in sensitive buildings, such as ministries, while US telecommunication regulators restricted Chinese equipment in the nation's communication network.[50] With the advent of 5G, members of the EU and NATO are also sensitive. Chinese law permits the government to gain access to the data of any private company in China.[51] This could be an issue for countries such as Belgium, where the telecommunications grid uses Chinese technology, putting mobile communications used by EU and NATO administrations at risk.[52] In Germany, Chinese equipment is also present in the network system, possibly endangering the mobile traffic of, for example, NATO troops based in Germany.[53] While there are currently no indicators that China is using acquired data for political advantage, this could be a factor in international conflict in the future.

Chinese surveillance technology in the West Balkans

While Chinese projects are present in most West Balkan states[54], Serbia is the leading beneficiary in the region. Since 2013, China has initiated 136 projects in the Balkans region, ranging from infrastructure and energy to security. Out of the total number, 61 – a majority – are implemented in Serbia[55]. The Serbian government is welcoming Chinese investments, loans, and cultural exchange programmes as well as "strategic cooperation" in the realms of security and digitalization.[56] A potential explanation for Serbia's openness could be that its foreign policy is largely guided by a "four-pillar" principle[57], where the Serbian government seeks cooperation, support, and resources from not just the EU and the US, but also from Russia and China. While some critics refer to the approach as neutrality, others see it as "sitting on too many chairs".[58] This often leads to friction, what has been especially pronounced following the recent

[47] Elaine Huang, "Despite ban, Chinese surveillance equipment infiltrating Taiwan in plain sight", Commonwealth Magazine, September 30, 2022, https://english.cw.com.tw/article/article.action?id=3301

[48] Elaine Huang, "Despite ban, Chinese surveillance equipment infiltrating Taiwan in plain sight"

[49] Brian Krebs, „FBI Raids Chinese Point-of-Sale Giant PAX Technology", Krebs on Security, October 26, 2021, https://krebsonsecurity.com/2021/10/fbi-raids-chinese-point-of-sale-giant-pax-technology/; Kirsty Needham and Clare Baldwin, "China's gene giant harvests data from millions of women", Reuters, July 7, 2021, https://www.reuters.com/investigates/special-report/health-china-bgi-dna/

[50] Nik Martin, "US bans Chinese telecom, surveillance cameras", Deutsche Welle, November 26, 2022, https://www.dw.com/en/us-bans-chinese-telecom-surveillance-cameras/a-63895206

[51] Julia Pallanch and Amy Yanan Zhang, "China, 5G, and NATO Security", GMF, October 27, 2021, https://www.gmfus.org/news/china-5g-and-nato-security

[52] Julia Pallanch and Amy Yanan Zhang, "China, 5G, and NATO Security"

[53] Julia Pallanch and Amy Yanan Zhang, "China, 5G, and NATO Security"

[54] See more https://china.balkaninsight.com/

[55] Balkan Investigative Reporting Network, "China in the Balkans", 2021, https://china.balkaninsight.com/

[56] Bojan Stojkovski et al., "China in the Balkans: Controversy and Cost", December 15, 2021, https://balkaninsight.com/2021/12/15/china-in-the-balkans-controversy-and-cost/

[57] European Parliament, Policy Department of the Directorate-General for External Policies, "Serbia's cooperation with China, the European Union, Russia and the United States of America", 2017, https://www.europarl.europa.eu/cmsdata/133504/Serbia%20cooperation%20with%20China,%20the%20EU,%20Russia%20and%20the%20USA.pdf

[58] Rade Rankovic, "Spoljna politika Srbije: Neutralnost ili sedenje na više stolica (Serbia's Foreign Policy: Neutrality or Sitting Inbetween Several Chairs)", Voice of America, June 11, 2021, https://www.glasamerike.net/a/srbija-rusija-kina-amerika-eu-spoljna-politika-odnosi/5925504.html

Russian invasion of Ukraine. Namely, Serbia remains one of two European countries – aside from Belarus – which has not imposed sanctions on the Russian regime.[59] During a recent visit to Belgrade, German Chancellor Olaf Scholz implied that Serbia's EU accession path is brought into question given Belgrade's ties with Moscow.[60]

However, the four-pillar approach is a strategic choice. When talking about Serbia's foreign interests, a Serbian local political analyst highlighted the importance of both "the East and the West". Relationships with "the East" are important for matters of territorial integrity and national interests – mainly regarding Kosovo, whose independence has not been recognized by Serbia[61] – while "the West" is crucial with regards to economic cooperation.[62] As a result, the Serbian Ministry of Foreign Affairs often highlights the importance of Sino-Serbian cooperation and partnership, often referred to locally as a "Steel Partnership".[63] Only recently has Sino-Serbian cooperation been established in the field of security. Previously, China had been investing in infrastructure and energy projects, largely as part of the strategic BRI. Compared to the other Balkan states, Serbia is the biggest recipient of Chinese FDI as well – amounting to 10 billion USD.[64] The first major Chinese-funded infrastructure project in the region was completed in 2014 – the Pupin bridge in Belgrade.[65] Chinese investments took off after 2016, and 90 percent of all Chinese-funded projects were between 2016 and 2019.[66]

The early beginning of Sino-Serbian cooperation in the security realm can be traced to 2009, when Serbia and China signed a strategic partnership agreement, which had a general goal of enhancing information and communication technology systems to improve the safety of citizens and create a "safe society".[67] Few concrete actions followed the partnership. A key moment occurred in 2014, when a hit-and-run vehicle incident made news in Serbia, bringing the connection between technology and safety into the spotlight. The suspect – a Serbian citizen – ran over and killed a 21-year-old in Belgrade, then escaped

[59] Aleks Eror, "Serbia's sanctions standoff with the EU", Politico, June 16, 2022, https://www.politico.eu/article/serbia-sanction-standoff-eu/

[60] Michael Nienaber and Misha Savic, "Scholz Tells Serbia It Must Decide Between Europe and Russia ", Bloomberg, June 10, 2022, https://www.bloomberg.com/news/articles/2022-06-10/scholz-tells-serbia-it-must-decide-between-europe-and-russia

[61] N1 Serbia, "Vučić: Ne planiram da menjam stav, sedam novih država povuklo priznanje Kosova (Vucic: I don't plan on changing my position, seven new countries withdrew Kosovo recognition)", August 27, 2022, https://rs.n1info.com/vesti/vucic-ne-planiram-da-menjam-stav-sedam-novih-drzava-povuklo-priznanje-kosova/

[62] Rade Rankovic, "Spoljna politika Srbije: Neutralnost ili sedenje na više stolica (Serbia's Foreign Policy: Neutrality or Sitting Inbetween Several Chairs)".

[63] Serbian Ministry of Foreign Affairs, "Čelično prijateljstvo i strateško partnerstvo Srbije i Kine (Steel Friendship and Strategic Partnership of Serbia and China)", October 28, 2021, https://www.mfa.gov.rs/lat/mediji/saopstenja/celicno-prijateljstvo-i-stratesko-partnerstvo-srbije-i-kine

[64] China Global Investment Tracker, https://www.aei.org/china-global-investment-tracker/. While Serbian officials claim that Chinese investments amount to 10 billion USD, some have questioned this number. Namely, data from the National Bank of Serbia shows a significantly smaller number – 1,6 billion USD. Read more (BCS): https://www.slobodnaevropa.org/a/kineske-investicije-u-srbiji-obecano-i-realizovano/30826927.html.

[65] Zoran Glavonjić and Milan Nešić, "Beograd dočekao Pupinov most preko Dunava, prvi posle 80 godina (Belgrade welcomed Pupin's Bridge over the Danube – the First in 80 Years)", Radio Free Europe, December 18, 2014, https://www.slobodnaevropa.org/a/beograd-docekao-pupinov-most-preko-dunava-prvi-posle-80-godina/26751132.html

[66] Mila Đurđević, "Kineske investicije u Srbiji: Jaz između obećanog i realizovanog (Chinese Investments in Serbia: the Gap Between the Promised and the Realised)", September 8, 2020, Radio Free Europe, https://www.slobodnaevropa.org/a/kineske-investicije-u-srbiji-obecano-i-realizovano/30826927.html

[67] Prague Security Studies Institute, "The Sum of All Fears – Chinese AI Surveillance in Serbia", December 2020, https://www.pssi.cz/download//docs/8447_the-sum-of-all-fears-chinese-ai-surveillance-in-serbia.pdf; Đorđe Krivokapić, "A Disturbing Marriage: Serbia and China Team Up on Digital Surveillance", CEPA, January 27, 2022, https://cepa.org/a-disturbing-marriage-serbia-and-china-team-up-on-digital-surveillance/

the crime scene. Soon after, the perpetrator left Serbia, and escaped for Turkey, moving to Hong Kong, and finally reaching China in the span of a few days.[68] Upon discovery, Serbian authorities provided the Chinese government with photos of the alleged criminal, and after three days, Chinese police arrested him.[69] This reportedly impressed Serbian officials, and talks between Serbian and Chinese political leaders ensued soon after. The talks concluded in the signing of a Strategic Partnership Agreement in 2017 with Huawei.[70] While the document is confidential and thus unavailable to the public, Huawei has since become a strategic actor in helping Serbia develop its digital transformation.[71]

In 2019, the Ministry of Interior (MOI) announced that 1,000 Huawei surveillance cameras would be installed in 800 locations across Belgrade as part of a "Safe City" project.[72] The MOI stated that these cameras would be equipped with face and license plate-recognition technology, and that police cars and personnel will be carrying them in the future as well.[73] Throughout its conception and adoption, the project has lacked transparency. The Serbian government kept details of the "Safe City" contract with Huawei confidential – details regarding the cost, location, and functionality of the cameras remained unknown to the public.[74] When citizens organized in opposition and requested that information, the government refused to provide it. Further inquiries by the citizen-led SHARE Foundation on a possible impact assessment of the technology on citizen privacy were met with inconsistent statements.[75]

Local implications

The build-up of the surveillance camera network raised legal issues as well. Since Serbian jurisprudence does not currently regulate video surveillance on a systemic level, relevant regulations must be put in place by the government.[76] In 2021, the government published a draft of an updated Police Law which gives the police authority to use facial data in three distinct cases: to identify those breaching the law, those on arrest warrants, and those where there is reasonable suspicion that they have committed a

[68] Gordana Andrić, "Chinese Arrest Belgrade Hit-and-Run Suspect", Balkan Insight, September 2, 2014, https://balkaninsight.com/2014/09/02/belgrade-hit-and-run-suspect-arrested-in-china/

[69] Bojan Stojkovski, "Big Brother Comes to Belgrade", Foreign Policy, June 18, 2019, https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/

[70] Prague Security Studies Institute, "The Sum of All Fears – Chinese AI Surveillance in Serbia"

[71] Radio Free Europe, "Huawei otvorio centar za inovacije i razvoj digitalizacije u Beogradu (Huawei opens Innovation Centre in Belgrade)", September 14, 2020, https://www.slobodnaevropa.org/a/30838169.html

[72] N1 Serbia, "Stefanović: Hiljadu kamera sa softverima za prepoznavanje lica i tablica (Stefanović: A Thousand Face- and Numberplate-Recognition Cameras", January 30 2019, https://rs.n1info.com/vesti/a456247-stefanovic-hiljadu-kamera-sa-softverima-za-prepoznavanje-lica-i-tablica/

[73] N1 Serbia, "Stefanović: Hiljadu kamera sa softverima za prepoznavanje lica i tablica.

[74] Radio Free Europe, "Koga i zašto snimaju Huawei kamere u Beogradu? (Whom and why are the Huawei cameras recording?)", September 16, 2019, https://www.slobodnaevropa.org/a/huawei-kamere-beograd-mup-kina/30162793.html

[75] Share Foundation, "Huawei zna sve o kamerama u Beogradu – I nije im teško da to i kažu (Huawei knows everything about the cameras in Belgrade and has no issues sharing it)", March 29, 2019, https://www.sharefoundation.info/sr/huawei-zna-sve-o-kamerama-u-beogradu-i-nije-im-tesko-da-to-i-kazu/

[76] According to the Commissioner for Information of Public Importance and Personal Data Protection, this is especially important for video surveillance given the sensitive nature of the data collected by the technology, and the potential to be misused. See: Radio Free Europe. "Poverenik za RSE: Za video nadzor u Srbiji potreban poseban zakon (Video-surveillance in Serbia needs special regulation)", September 20, 2021, https://www.slobodnaevropa.org/a/poverenik-huawei-kamere-odgovor/31469201.html

crime.[77] Still, activists warn about potential misuse of personal data. Late last year, several cities in Serbia saw large protests against pollution, and many activists reported receiving mailed fines after the protest without having their data taken on site by the police.[78] This raised fears that the government used the surveillance technology to identify protestors, something that the authorities denied. Activists also criticize the law's broad provisions which leave much space for interpretation. For example, the draft law is unclear about who has access to citizen data.[79] Given these doubts, activists have informally organized around the "thousand cameras campaign" to advocate for the protection of privacy. [80]

Regional implications

Concern about Chinese technology exports to Serbia have also reached the European Parliament. In April 2021, a group of MEPs formally wrote to Aleksandar Vulin – the Serbian Minister of Interior – expressing concerns about Belgrade being "the first city in Europe to have the vast majority of its territory covered by mass surveillance technologies".[81] Another growing concern is the state of Serbian democracy in the context of these surveillance technology imports. Some observers questioned whether Beijing is targeting Serbia due to its partially free political rights and civil liberties.[82] Specifically, a recent study noted a correlation between a larger Chinese economic impact and a decrease in legal and governance standards in Central and Eastern Europe.[83] By exploiting this opportunity, China could use and promote its surveillance technology to further an authoritarian style of governance in Serbia. There is no indication so far that this technology is being misused – e.g., to target minorities or spy on opposition politicians – but observers point out that very little is known about how the Serbian authorities are using this technology, or how they can guarantee the safety of their citizens.[84]

Additionally, there are immediate implications for unresolved sovereignty issues in the region. In 2021, Belgrade financed the installation of small surveillance cameras with facial recognition technology[85], digital recorders, and other equipment in some Kosovar communities where Pristina's control is not as

[77] Radio Free Europe, "Zašto kamere menjaju Zakon o policiji u Srbiji? (Why do surveillance cameras change the police law in Serbia?"), September 17, 2021, https://www.slobodnaevropa.org/a/kamere-huawei-srbija-beogra-policija/31465283.html

[78] Read more (BCS): https://www.slobodnaevropa.org/a/poverenik-huawei-kamere-protesti-u-srbiji/31599997.html

[79] Radio Free Europe, "Zašto kamere menjaju Zakon o policiji u Srbiji?; For more legal issues, read further: https://hiljade.kamera.rs/en/law-society/

[80] SHARE Foundation, Thousands of Cameras, See: https://hiljade.kamera.rs/en/home/

[81] Alessandra Briganti, "Serbia's smart city has become a political flashpoint", Wired, August 10, 2021, https://www.wired.co.uk/article/belgrade-huawei-cameras; also see: Georgi Gotev, "MEPs sound the alarm over Chinese mass surveillance project in Belgrade", EURACTIV, June 3, 2021, https://www.euractiv.com/section/china/interview/meps-sound-the-alarm-over-chinese-mass-surveillance-project-in-belgrade/

[82] Read more: https://freedomhouse.org/country/serbia

[83] Reid Standish, "New Study Says China Using Investments To Buy Political Influence In Central, Eastern Europe", Radio Free Europe, September 9, 2021, https://www.rferl.org/a/chinese-investments-central-eastern-europe/31452615.html

[84] Alessandra Briganti, "Serbia's smart city has become a political flashpoint"

[85] Radio Free Europe, "Kineske kamere sa američke crne liste preko Srbije ušle na Kosovo (US-blacklisted Chinese surveillance cameras enter Kosovo through Serbia)", December 30, 2021, https://www.slobodnaevropa.org/a/kamere-srbija-kosovo-kina/31633032.html

strong.[86] The Kosovar government claim they have no information on Serbia's actions. The technology was purchased from Dahua, a Chinese company previously blacklisted by the U.S. Furthermore, Kosovo has strong diplomatic ties with the U.S., while Serbia does not recognize Kosovo's independence. However, so far, Kosovar experts regard this as an isolated development highlighting territorial disputes, rather than a coordinated attempt to place blacklisted technology in pro-U.S. Kosovo.[87]

International implications

The confrontation between China and the U.S – most prominently, the race to establish dominance over global digital infrastructure – is reproduced on a smaller scale in the Balkans.[88] In the region, China has strategized its influence through the Chinese Digital Silk Road project, an important part of China's BRI aiming to expand connectivity in partner countries.[89] China's growing influence has caused concern among EU and NATO members; some Western Balkan countries are on track for EU membership, and others are NATO members.[90] To counter this, the U.S. launched the Clean Network Initiative in 2020 to "safeguard the nation's assets including citizens' privacy and companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party".[91]

In the Western Balkans, stances on the issue differ greatly, largely dependent on the respective country's relationship to China and the West. Albania, a NATO member, signed the Clean Network Initiative. Fellow NATO member Montenegro did not. EU membership candidate North Macedonia joined the initiative, unlike Bosnia and Herzegovina, another EU membership candidate. Kosovo, unrecognized by both Serbia and China, signed the initiative. Serbia is not part of the initiative despite U.S. pressure to limit Chinese influence in its digital infrastructure.[92] In 2020, leaders of Serbia and Kosovo signed a list of commitments related to the Belgrade-Pristina dialogue process, which included a clause on restricting "untrusted vendors" of 5G technology and removing such existing equipment.[93] While no reference has been made to any specific party, the clause implicitly refers to China and Huawei. However, only a few days after signing the pledge, Huawei opened an Innovation and Development Centre in Belgrade.[94]

[86] Radio Free Europe, "Serbia's Back-Door Bid To Embed Chinese Snooping Tools In Kosovo", January 8, 2022, https://www.rferl.org/a/serbia-embed-chinese-cameras-kosovo/31645126.html

[87] Radio Free Europe, "Serbia's Back-Door Bid To Embed Chinese Snooping Tools In Kosovo"; Radio Free Europe, Kineske kamere sa američke crne liste preko Srbije ušle na Kosovo.

[88] Jeanne Whalen and Chris Alcantara, "Nine charts that show who's winning the U.S.-China tech race", Washington Post, September 21, 2021, https://www.washingtonpost.com/technology/2021/09/21/us-china-tech-competition/

[89] Stefan Vladisavljev, "Surveying China's Digital Silk Road in the Western Balkans", War on the Rocks, August 3, 2021, https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans/

[90] See for example this report about Chinese weapon exports to Serbia: https://apnews.com/article/russia-ukraine-europe-china-serbia-nato-682ab79c4239f14ecc1133ff5c7addc9

[91] See for example: https://2017-2021.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/index.html

[92] Stefan Vladisavljev, "Surveying China's Digital Silk Road in the Western Balkans".

[93] Majda Ruge, "Serbia's 5G deal with Washington: The art of muddling through", European Council on Foreign Relations, September 22, 2020, https://ecfr.eu/article/commentary_serbias_5g_deal_with_washington_the_art_of_muddling_through/

[94] Saša Dragojlo, "China's Huawei Opens Tech Centre, Consolidating Presence in Serbia", Balkan Insight, September 15, 2020, https://balkaninsight.com/2020/09/15/chinas-huawei-opens-tech-centre-consolidating-presence-in-serbia/