SWEDISH CENTER
FOR CHINA STUDIES

Chinese overseas promotion of ‘smart city’ technologies

What’s at stake for Europe

By Miriam Tardell, July 2021

Conclusions

- China has used the covid-19 pandemic as an opportunity to promote domestic smart city technologies, exporting such systems all over the world.
- Chinese state media claim that China’s high-tech anti-epidemic measures (the *Chinese solution*) are the most efficient in the world. These “solutions” are described as a reflection of China’s systemic advantages.
- The smart city model promoted by the Chinese party-state differs greatly from that of the European Union, in that it focuses on surveillance and public security.
- Some of the cited risks with Chinese smart city technologies are that they can help to prop up authoritarian systems; that the Chinese state could gain access to sensitive data; and that critical infrastructure could become more vulnerable.
- China has launched a national plan to set the standards for the next generation of technology — the *China Standards 2035* — in which technologies for smart cities play a prominent role. The plan lays out ambitions for e.g. blockchain, cloud computing, 5G, artificial intelligence and geographic information systems (GIS).

Smart city technologies as part of the post-pandemic "Chinese solution"

Since the early stages of the Covid-19 pandemic in spring 2020, Chinese party and state media have hailed the use of China's smart city technologies as a new urban governance model for the world. *Xinhua*, *People's Daily* and the Communist Party's main ideological journal, *Qiushi*, assert that these tools form part of a more effective set of measures to contain the spread of the virus than those imposed by any other country. The use of high-technology equipment to enhance epidemic prevention and control is emphasized as a key feature of these efforts, contributing to an urban governance system that is supposedly more efficient and modern than elsewhere. Party and state media commend the "Chinese solution" ("中国答案") as an example for all to study and learn from. There is, however, limited evidence suggesting that this campaign has been successful outside China's borders.

The pandemic has enabled China to promote technologies underpinning its smart city model, including big data collection and analysis, surveillance cameras, facial recognition technology, and tracking apps. This model differs from European smart cities on several accounts. The European Commission defines smart city as a "place where traditional networks and services are made more efficient with the use of digital and telecommunication technologies" including "urban transport networks, upgraded water supply and waste disposal facilities and more efficient ways to light and heat buildings". In the EU, the use of digital tools in anti-epidemic work has been balanced against the need to respect the privacy and fundamental rights of citizens, as underlined by a common EU toolbox adopted in April 2020.

In contrast, the smart city (or "safe city") notion favored by China and featured in its handling of the covid-19 outbreak, emphasizes all-encompassing surveillance and public security in ways that are controversial in Europe. According to a brief by the European Union Institute for Security Studies (EUISS), Chinese smart city technologies have been further developed during the covid-19 crisis, using tools like AI-enabled cameras and robots for scanning the temperature of individuals and drones for broadcasting warnings to people breaking quarantine rules. The facial recognition company SenseTime has benefited from the pandemic by commercially deploying technology able to recognize an individual even when they are wearing a face mask.

An article published by Chinese news portal Sina suggests that the foundation for smart cities — such as those in Hangzhou (a city of 10M just south of Shanghai) and in Beijing's Haidian District — is close cooperation and information sharing between businesses and local governments. The purpose of this cooperation model is to integrate information systems for police, traffic, tourism and health services. In the wake of the pandemic, China's epidemic control measures backed by 5G technology and government-business cooperation have been hailed as a "new model for urban social governance" in Chinese party-state media. Shanghai's AI-enabled traffic lights have been characterized by Xinhua as a way to showcase the "systemic advantages of the socialist urban governance model" to the rest of the world.

At its core, the Chinese conception of a smart city is based on the population as a collective, meaning less concern about violations of individuals' rights. According to a 2018 paper by Australia-based scholars Fan Yang and Jian Xu, China lacks privacy laws that would protect the personal data collected in smart cities.

Seeking global influence: standard-setting and data security

China attempts to exert greater influence over international standards, including those of smart city technologies. In 2018, it launched a research project to write global standards for the next generation of technology, which culminated in the *China Standards 2035* plan

two years later. A policy document released by the Standardization Administration of China (SAC) in March 2020 is considered to be a blueprint for the plan, which is the broader strategy for advancing China's standardization efforts and its influence over international standards. The document, "Main Points of National Standardization Work in 2020," describes how smart cities are one of the key areas where China strives to develop new standards, along with other technologies closely linked to smart cities. These include blockchain, the Internet of Things (IoT), cloud computing, big data, 5G, artificial intelligence and geographic information systems (GIS).

These efforts also entail increasing Chinese influence over international standardization bodies, not least the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). China has, in fact, increased its sway in such organisations through successful lobbying to appoint Chinese nationals to leading positions. For example, the International Telecommunications Union (ITU) has been led by China's Zhao Houlin since 2014. Similarly, the joint working group on smart cities under the ISO/IEC is headed by several Chinese officers. In March 2020, the ITU adopted new standards for smart cities and smart residential communities modelled on Xiong'an New Area in China's Hebei province.

China also wants to establish new international standardization organizations and technical committees and to improve information-sharing nationally between civilian and military organizations. An analysis by Horizon Advisory — a consultancy based in Washington, DC — suggests that China is seizing the opportunity provided by the pandemic to increase its influence over standard-setting in these areas.

Last but not least, China attempts to control the narrative in international standard-setting. In part, this is related to data security, where there have been concerns in Europe and democracies elsewhere over the management of personal data by Chinese companies. In September 2020, in an apparent response to such concerns, China's government launched a "Global Initiative on Data Security," which stressed the right for states to govern data as they wish, based on "mutual respect."

European concerns over Chinese smart city technologies

In the years that preceded the covid-19 pandemic, China was already actively promoting its smart city technologies overseas. In a report prepared for the U.S.-China Economic and Security Review Commission in January 2020, analysts identified 398 cases of smart cities technologies being exported by 34 Chinese firms to 106 countries. Some of these examples were to be found in Europe and among them, the most comprehensive smart cities projects were found in Germany. Duisburg, a European hub for the *Belt and Road Initiative* (BRI), signed an agreement with Huawei in 2018 to develop e-Government infrastructure based on cloud computing as well as an IoT network powered by 5G. Another city, Gelsenkirchen, cooperates with Huawei to set up Germany's first "Safe City solution" which centers around an information platform that uses Big Data analysis and video processing to improve coordination between security and emergency services.

In the wake of the pandemic, China is increasingly promoting and exporting technologies underpinning its own smart city model to European cities (where technology-enabled monitoring is a priority), often branding these as "anti-epidemic tools". Huawei is in the process of installing some 8,000 surveillance cameras in Belgrade as part of a "safe city" partnership with the Serbian capital. The project was launched in 2019 and underlines an increasingly intimate relationship between the Chinese and Serbian governments, not least after the covid-19 outbreak in Wuhan.

In March 2020, Chinese drone manufacturer Ehang signed an agreement with the city of Seville to jointly develop Spain's first smart air traffic control system. Some European

municipalities struggling to cope with the pandemic have adopted technological solutions offered by China to help monitor and reinforce restrictions. DJI, China's leading drone manufacturer, claims that its products have been employed in French, Spanish and Italian cities for their patrolling and disinfecting functions. DJI also runs a special support programme with preferential deals for police and health departments in Europe and the US.

China's promotion of (especially 5G) technologies during the covid-19 outbreak has increased concern in Europe. Chinese telecom gear maker Huawei's current and future presence in Europe will continue to be in focus as EU member states implement key measures in the EU toolbox for 5G security released in January 2020. A subsequent report on Member States' implementation of the toolbox showed that risk for interference by third countries in 5G supply networks was perceived as the most relevant and least mitigated risk with existing measures.

In March 2020, Huawei claimed to have donated wireless network equipment to Italian hospitals, generating criticism in the EU Parliament over security concerns. In an apparent response to Huawei's various covid-19-related activities in Europe the EU's foreign policy chief, Josep Borrell, urged Europeans to be mindful of the geopolitical component in the 'politics of generosity'.

This discussion has continued and intensified in Europe over the past year. In May 2021, the UK National Cyber Security Centre (NCSC) issued guidance for local councils on how to mitigate security risks in their smart city projects. In recent years, such deals have been cancelled at the last minute by local councils after security concerns in contracts with Chinese suppliers, including a "smart places" services plan by Bournemouth council that allowed e-commerce giant Alibaba to access large amounts of data. The NCSC's guidance highlights how suppliers from some countries "may be subject to influence from those governments to access and exfiltrate data from UK connected places, in support of those countries' security and intelligence services."

Implications for Europe

While the pandemic has provided additional opportunities for some Chinese companies to market smart city technologies in Europe, there are prominent examples where EU member states have refrained from adopting such systems over security concerns. Decisions by some European countries to consider national security when selecting vendors for their future 5G networks, for example, constitute a setback for Huawei, ZTE and other Chinese companies.

According to experts cited by the *Financial Times*, China's smart (or safe) city systems come with three specific risks. Firstly, they could contribute to "digital totalitarianism" in recipient countries, by which the model for urban governance favored by the Communist Party would be legitimised and replicated, thereby posing a normative challenge to the EU's interests over the long term.

Secondly, the Chinese state and businesses could gain access to sensitive data. China's version of smart cities focuses on improved public security while largely disregarding individual rights and privacy

Finally, in extreme circumstances, Chinese actors could be able to shut down a city's operations.

The issue of potential risks associated with the provision of smart city technologies from Chinese tech firms has been extensively discussed in Europe in recent years. A key concern is that the personal data of European citizens as well as company data could be accessed by Chinese party-state and military organizations. Such concerns are underlined by a 2019 report by Berlin-based think-tank MERICS which argued that "European

citizens' privacy, safety and rights need protection from Chinese government encroachment."

The assumption that sensitive data could be at risk is, in part, based on the adoption of Chinese legislation requiring domestic companies to cooperate with authorities in national security and intelligence work. The laws include the Intelligence Law (2017), the Cybersecurity Law (2016) and the National Security Law (2015). Through such legislation, Chinese companies could be forced to make decisions that compromise the integrity of their customers' data.

Indirectly, in a situation where Chinese tech firms could dominate future European and global markets for smart city technologies, Europeans would be dependent on China for critical infrastructure enabling their daily lives. Technologies used in Europe would also be shaped based on Chinese conceptions of smart cities, meaning that privacy and individual rights would be gradually eroded.