

Geopolitical Challenges of Chinese Smart Cities

Kazuki Ichida

(Visiting Researcher, Cyber Security Research Institute, Meiji University)

October 31, 2023

Abstract

Smart cities are geopolitical battlegrounds composed of technologies in which the U.S. and China are competing for supremacy. Chinese smart cities are governance systems that prioritize safety, whereas those of American companies are business systems that advocate improving quality of life, optimizing urban functions, and reducing operating costs. Chinese smart city projects are often integrated with economic and informatization support, and are deeply tied to China economically and politically. Authoritarian countries and weakened democracies are seeking Chinese smart cities as political instability increases, and the number of these cities is growing as a result of this increase. There are 144 such projects underway worldwide, and the vast amount of data and networks accumulated could give China a strategic advantage. Smart cities have become geopolitical battlegrounds for supremacy, but the West has been outnumbered.

Mark Leonard, a British political scientist and board member of the European Council on Foreign Relations, says that while most Western leaders and policymakers try to preserve the existing rules-based international order, Chinese strategists increasingly define their goal as survival in a world without order.¹ Furthermore, the "international order" that the West uses is not necessarily fair in the eyes of the rest of the world. It is believed that they are willing to change and sometimes disregard the rules for their own interests, and in short, are not trusted. Leonard concludes that Beijing's understanding may well be more accurate than Washington's.²

These basic differences in worldview appear everywhere. The smart city is one such example. While Chinese smart cities are governance systems that prioritize security, those of American companies are business systems that advocate improving quality of life, optimizing urban functions, and reducing operating costs.³ The former can be described as a tool for authoritarian governance, while the latter can be described as a tool for a surveillance capitalism community.

The technologies, products, etc. that make up the Chinese and American company-style smart cities will differ in many cases due to decoupling. China and the U.S. have been vying for supremacy in the technologies used in smart cities, including networks, AI, and big data. In a sense, smart cities are a geopolitical battle field of worldviews and technologies. This paper introduces the current status of Chinese smart cities based on existing papers and reports. Both the smart city as a package and the elemental technology of monitoring are treated in this paper.

China's Smart Cities and the Proliferation of Surveillance Technologies

China's smart city and surveillance technology is spreading around the world: since 2009, 144 smart city contracts involving Chinese companies have been signed, mostly in countries with restricted freedoms, and in the regions of Southeast Asia and the Middle East.⁴

¹ Mark Leonard, "China Is Ready for a World of Disorder America Is Not," *Foreign Affairs*, July/August 2023. <<https://www.foreignaffairs.com/united-states/china-ready-world-disorder>>

² *Ibid.*

³ Hubert Beroche, Ana Chubinidze, and Lina Goelzer, "Geopolitics of Smart Cities: Expression of Soft Power and New Order," March 2023, <<https://urbanai.fr/wp-content/uploads/2023/03/Geopolitics-of-Smart-Cities.pdf>>

⁴ James Kynge et al., "Exporting Chinese Surveillance: The Security Risks of 'Smart Cities'," *Financial Times*, June 8, 2021, <<https://www-ft-com.ezp.lib.cam.ac.uk/content/76fdac7c->

In addition, among the surveillance technologies that are at the core of smart cities, China is particularly prominent in facial recognition AI. Looking at its exports, from 2008 to 2021, China exported to roughly twice as many countries as the United States (China 83 and U.S. 48), with 10% more transactions (China 238 and U.S. 211).⁵ Most exports are to countries in the Global South, including countries participating in One Belt One Road, BRICS (Brazil, Russia, India, China, and South Africa), and members of the China-Africa Cooperation Forum, but some countries in the Global North have also adopted the system.

However, the actual numbers of Chinese smart city exports is not exactly known. This is because Chinese government agencies and Chinese companies require non-disclosure of details in contracts, sometimes even requiring that the existence of the contract be kept secret.⁶

Ties between China and other countries often start with economics and extend to relationships that include security, which in turn has led to the introduction of smart cities. The recent proximity to Middle Eastern monarchies is one such example. Saudi Arabia's largest trading partner is China, which has strategic partnership agreements with both Saudi Arabia and the United Arab Emirates. In March 2023, Saudi Arabia decided to join the Shanghai Cooperation Organization as a dialogue partner. Bahrain, Kuwait, and the United Arab Emirates are also expected to join as dialogue members. China has provided Saudi Arabia and the United Arab Emirates with information and communications infrastructure, including 5G networks, and smart cities have adopted surveillance cameras and other equipment from Chinese companies.⁷

In Africa, economic assistance and informatization support have triggered the implementation of smart cities. China has provided approximately 70% of Africa's digital infrastructure, and 22 countries have installed Huawei surveillance systems. In Kenya, ZTE and Huawei have laid optical fiber and will cooperate on surveillance systems and e-government.

In addition, surveillance systems from Dahua and Hikvision and an

[7076-47a4-bcb0-7e75af0aadab>](#)

⁵ Martin Beraja et al., "Exporting the Surveillance State via Trade in AI," The Brookings Institution, January 12, 2023. <<https://www.brookings.edu/articles/exporting-the-surveillance-state-via-trade-in-ai/>>

⁶ Christopher Walker, "How China Exports Secrecy," *Foreign Affairs*, July 11, 2023. <<https://www.foreignaffairs.com/china/how-china-exports-secrecy>>

⁷ Andrew Chack, "Analyzing the Entrenchment of Beijing's Digital Influence in Saudi Arabia and the United Arab Emirates," *Georgetown Security Studies Review*, April 14, 2023. <<https://georgetownsecuritystudiesreview.org/2023/04/14/analyzing-the-entrenchment-of-beijings-digital-influence-in-saudi-arabia-and-the-united-arab-emirates/>>

urban traffic management system from Nanjing Les Information Technology were installed. Huawei received an order for a smart city that installs surveillance cameras and manages police and traffic in an integrated manner. Huawei's surveillance and other systems have been installed in Uganda, and smart cities are being introduced in South Africa.⁸

Zimbabwe's smart cities have been the focus of much attention in recent years. The Zimbabwe African National Union, the political party that came to power after two political upheavals due to political instability, has consistently stepped up surveillance of opposition parties and forces critical of the government. Currently, China, Russia, and Iran are the main countries providing surveillance technology to Zimbabwe. Chinese companies have been particularly active in Zimbabwe, and a military-industrial complex of Chinese companies such as Huawei and the Zimbabwe Defense Forces has been created there.⁹

Through smart cities, Chinese authorities will have access to more accurate information about the country which introduces the system, and may be able to control information and facilities as needed.

Smart cities are often discussed with a focus on monitoring technologies, but as described in this paper, they are about integrated management. Conceptually, it looks like Figure 1.¹⁰ Those who operate this

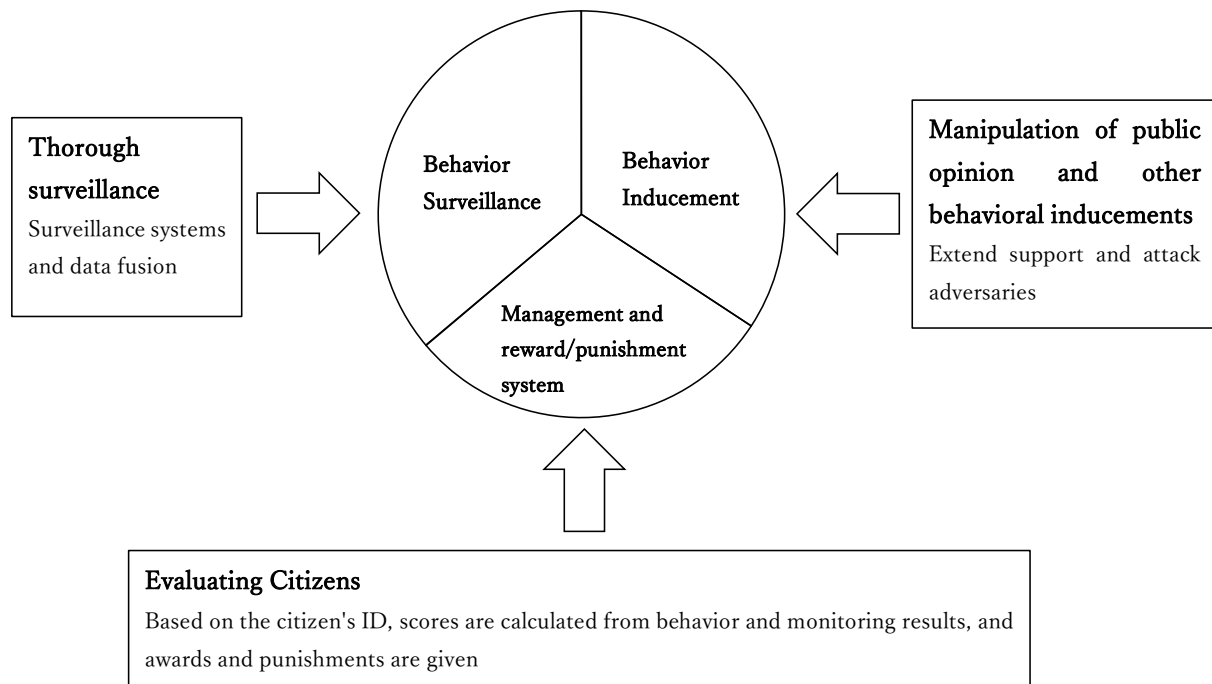
⁸ Bulelani Jili, "China's Surveillance Ecosystem & The Global Spread of Its Tools," Atlantic Council, October 17, 2022. <<https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/>>; Bulelani Jili, "What Is Driving the Adoption of Chinese Surveillance Technology in Africa?" Atlantic Council, May 15, 2023. <<https://dfrlab.org/2023/05/15/africas-demand-for-and-adoption-of-chinese-surveillance-technology/>>

⁹ Farai Shawn Matiashe, "Zimbabwe's Cyber City: Urban Utopia or Surveillance Menace?" *Context*, February 20, 2023. <<https://www.context.news/surveillance/zimbabwes-cyber-city-urban-utopia-or-surveillance-menace>>; Civic Media Observatory, "Undertones: Zimbabwe's Cyberpunk Cities Fueled by China. Interrogating the Narratives Behind Zimbabwe's Smart Cities," *Global Voices*, February 28, 2023. <<https://globalvoices.org/2023/02/28/undertones-zimbabwes-cyberpunk-cities-fueled-by-china/>>; Privacy International, "Huawei and Surveillance in Zimbabwe: We Explore Zimbabwe's Embrace of Surveillance Technologies, and the Zimbabwean Government's Increasingly Close Relationship with Huawei," November 18, 2021. <<https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe>>; ADF staff, "Zimbabwe Turns to Chinese Technology to Expand Surveillance of Citizens," *Africa Defense Forum DAILY NEWS*, January 17, 2023. <<https://adf-magazine.com/2023/01/zimbabwe-turns-to-chinese-technology-to-expand-surveillance-of-citizens/>>; Advox, "How Zimbabwe Is Building a Big Brother Surveillance State: Chinese Tech Companies Enable This Expensive and Advanced Surveillance Machine," *Global Voices*, January 10, 2023. <<https://globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/>>

¹⁰ Kazuki Ichida et al., *Nettoyoron'sōsato dejitaruēkyōkōsaku "miezaru te" o kashikasuru* (Net Public Opinion Manipulation and Digital Influence Work - Visualizing the "Invisible Hand") Hara Shobo, 2023.

system can control everything from the city’s infrastructure to the consciousness and behavior of its residents. In Kenya, the system is operated by staff dispatched from a Chinese company, and local officials do not understand how to operate the system (the manual is only available in Chinese).¹¹

Figure 1. Integrated Smart City Management



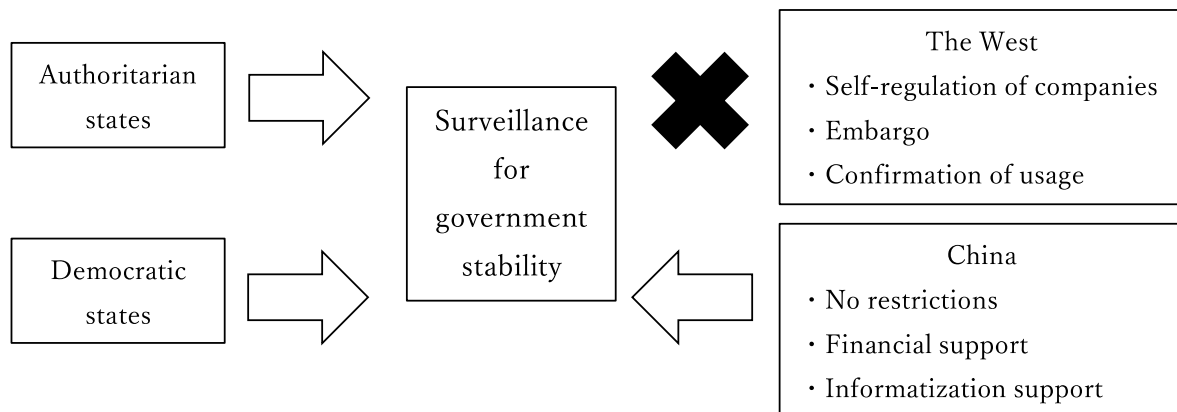
Source: Prepared by the author.

Demand Drives China’s Smart City Exports

China is expanding smart cities with strategic intent, but it is a one-sided understanding to say that China is trying to spread Chinese smart cities around the world to further its own ambitions, and this is against the backdrop that many countries need Chinese smart cities.

¹¹ Jili, *op. cit.*, 2022; Jili, *op. cit.*, 2023.

Figure 2: Smart City Demand and Supply



Source: Prepared by the author.

Democracies are already no longer the majority in the world, and democracy continues to recede today.¹² In authoritarian states or states where democracy has been weakened, it is crucial to maintain domestic security and control public opinion.

However, some Western companies, such as IBM and Microsoft, have self-imposed restrictions that prevent them from providing surveillance technology to authoritarian states, and Western governments have embargoes or require confirmation on applications. In contrast, China has no self-imposed regulations, no embargoes, and no restrictions on applications. As a result, China (other options include Russia and Iran) is the country that can meet the current demand.

In fact, it has been observed that states with weakened democracies and authoritarian states are deploying Chinese facial recognition AI systems at times of political instability.¹³ China’s smart cities and surveillance technologies are expected to be instrumental in resolving domestic instability.

Data Fusion and Closed Nets

There are two more developments in the Chinese smart city. One is

¹² Kazuki Ichida, “Sekaide mottomo ōi tōchikētaiwa min’shushugino rinen’o kakageru dokusaikokkadatta” (The Most Common Form of Governance in the World Was a Dictatorship with Democratic Principles), *Newsweek Japan*, March 23, 2021. <<https://www.newsweekjapan.jp/ichida/2021/03/post-22.php>>

¹³ Beraja et al., *op. cit.*

integrated management and behavior prediction through data fusion, and the other is the realization of asymmetry at the regional level through closed networks.

China has been working on a project to integrate and utilize the vast amount of data it has collected. The program, called data fusion, is underway in a variety of areas, integrating and utilizing everything from surveillance cameras, license plate recognition cameras, social media accounts, phone numbers, location data, facial features, blood types, and heights. In Xinjiang Uyghur Autonomous Region, the Integrated Joint Operations Platform (IJOP) is in operation, tracking detailed personal information and behavioral history. In addition to IJOP, the Tianshan Anti-terrorism Cloud is a forecasting system that predicts terrorist and dangerous activities.¹⁴

The use of data fusion may expand in the future because of the potential to achieve higher security by incorporating data fusion.

In addition, by networking and sharing information across multiple cities rather than a single city, integrated surveillance over a wider area will be possible. Terrorism and riots across multiple regions can also be predicted. The approach can predict and curb the behavior of believers of conspiracy theories and other theories that have spread around the world.

A closed net is, in plain terms, the same as a closed network of a state as a single unit, making it impossible for another entity to access the inside of the network from the outside. Authoritarian states like China and Russia are aiming for closed nets, and if they achieve this, they can have unrestricted access to other countries while creating an asymmetric environment where other countries do not have reciprocal access.

Smart cities can achieve closed nets on a city-by-city basis. Closed nets can create a more secure cyberspace. On the other hand, it is difficult to see what is happening inside the closed net from the outside. If a problem occurs within a closed net, it will not be possible for individuals in the closed net to report and spread the information via the Internet.

The networking of multiple cities also makes it easier to detect international cyber attacks. China is improving its cybersecurity information dissemination capabilities and is now disseminating threat information in the same way as Western cybersecurity firms.¹⁵ However, it has also become a

¹⁴ Dahlia Peterson, "How China Harnesses Data Fusion to Make Sense of Surveillance Data," The Brookings Institution, September 23, 2021. <<https://www.brookings.edu/articles/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/>>

¹⁵ Eileen Yu, "China Says NSA Used Multiple Cybersecurity Tools in Attacks Against Chinese University," *ZD NET*, September 13, 2022. <<https://www.zdnet.com/article/china-says-nsa-used-multiple-cybersecurity-tools-in-attacks-against-chinese-university/>>; AFP, "U.S.

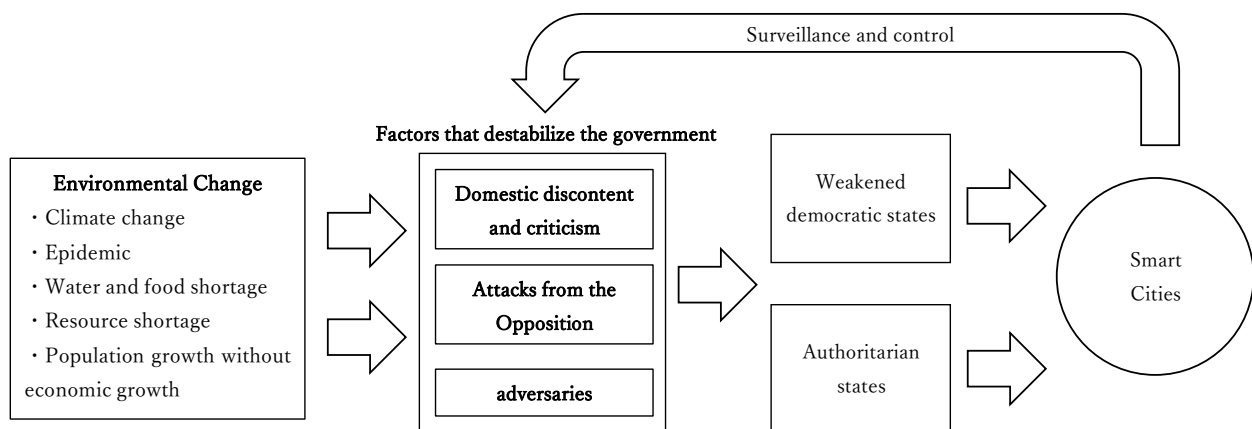
propaganda tool to push the West to take the lead in cyberattacks in an operation called Honey Badger.¹⁶

Spread of Demand Suggests Winners and Losers in Geopolitical Campaigns

Smart cities with data fusion and even closed nets are attractive to those who want to maintain a stable government. As noted above, the number of such rulers is increasing around the world today.

Also, as time goes on, more countries will be destabilized by climate change, epidemics, water and food shortages, resource shortages, population growth without economic growth (primarily in some African countries), and increased migration.

Figure 3: Growing Demand for Smart Cities



Source: Prepared by the author.

In the battle for the smart city, it is unlikely that the West, without a vision adapted to the world to come, will win, but this does not necessarily mean that China will be the winner either. China is not aiming to be a superpower of the sort that existed during the Cold War, but rather a major player in a multipolar world, so it does not need to be a winner like the United States once was. In any case, those who come up with ideas adapted to

CIA’s Investigative Report on Cyber Attacks on Other Countries Released by Joint Chinese Public-Private Investigation Team,” May 8, 2023. <<https://www.afpbb.com/articles/-/3463067>>

¹⁶ Albert Zhang, Tilla Hoja, and Jasmine Latimore, "Gaming Public Opinion," Australian Strategic Policy Institute, April 26, 2023. <<https://www.aspi.org.au/report/gaming-public-opinion>>

reality and who implement them will surely have the upper hand. At the moment, this is not the West, and of course not Japan.

【translated by】

Tomohito Nakano (Master's student, School of International and Public Policy, Hitotsubashi University)

Kazuki Ichida Profile

After managing several IT companies, Kazuki Ichida became a permanent resident of Canada in 2011 and moved to Vancouver. At the same time, he made his debut as a novelist. He has published many novels about cyber crimes that could happen in real life, as well as books and reviews about the manipulation of public opinion on the Internet. In recent years, he has written extensively on digital influence operations.