Surveillance State Rhymes with Digital Fate

31 MAY 2026

Tommaso Colonetti and Chiara Dinarello



Surveillance State Rhymes With Digital State

Surveillance State Rhymes with Digital Fate: An Overview of Chinese Tech Exports

From Theory to Infrastructure: Surveillance Capitalism in China

Based on the review of existing literature, this study primarily draws on the work of Zuboff (2019), whose analysis represents a central reference for understanding the economic dimension of technological development, particularly in the field of information technology. From this perspective, technological innovation is examined through a socio-economic lens: the

structural conditions in which it unfolds are conceptualised as 'surveillance capitalism', a regime of accumulation grounded in the systematic extraction and exploitation of data for profit. The recording and analysis of human behaviour operate through the pervasive integration of monitoring technologies into everyday life – such as video surveillance, network monitoring, and phone tapping – which can be implemented with varying degrees of visibility and concealment. While initially framed as a market-driven dynamic, Kilic (2025) argues that surveillance capitalism has rapidly demonstrated its potential to be leveraged by governments for broader political and institutional goals. As a result, it can be understood as a geopolitical regime capable of advancing specific state interests where the same tools designed for commercial purposes can be repurposed for governance, control, and strategic influence.

Although the People's Republic of China (PRC) remains formally governed by the Chinese Communist Party (CCP), characterising its system as capitalism is not oxymoronic, given the central role played by market logic, profit-driven incentives, and private capital accumulation within what is often described as party-state capitalism. The CCP prioritises political survival and risk management over purely economic objectives, maintaining control over key industries through state-owned enterprises while also exerting influence over private firms via mechanisms such as special management shares, which grant board representation and veto power over content. Within this framework, although market dynamics are present, they remain subordinated to political imperatives. The state actively directs private capital through instruments such as industrial guidance funds, aligning economic activity with national security and stability priorities (Pearson et al., 2023).

Historically, the CCP has predominantly relied on large state-owned enterprises to pursue its national ambitions. However, wanting China to become a global leader in Artificial Intelligence (AI), it has increasingly had to support smaller firms that operate with greater autonomy and are therefore not fully state-controlled. This transition has produced a mutually reinforcing relationship between political authorities and private technology companies, proving highly effective in accelerating innovation and technological expansion. At the same time, Chinese AI and surveillance firms operate within a highly permissive environment in which concerns regarding the impact of invasive surveillance systems on civil liberties are largely marginalised by design (Ryan et al., 2019).

Building on Balkin's (2008) assessment of the conditions underpinning the emergence of the surveillance state, it can be argued that governance practices based on the systematic collection and analysis of population data have developed significantly. This has enabled governments to anticipate potential risks and threats more effectively. In doing so, political actors have gained enhanced capacity not only to manage individuals more effectively but also to reinforce their own stability and preserve the status quo.

Accordingly, in the Chinese context, technologies are explicitly designed to meet the political requirements of social control (Peterson & Hoffman, 2022), thereby instrumentalising the operational logic of surveillance capitalism in support of political hegemony. More specifically, the commercial incentive to extract and process behavioural data functions as the technological engine underpinning a system of digital authoritarianism (Polyakova & Meserole, 2019). In contrast, while Western surveillance capitalism is primarily driven by profit and therefore produces comparatively limited dystopian effects – despite the role of intentionality – China's model is deliberately oriented toward the use of digital technologies to advance authoritarian rule (Zuboff, 2022).

This process has been further reinforced by the rapid expansion of the platform economy and the increasing integration of digital infrastructures into governance practices, as the functions enabled by the urban applications of AI (see Barns, 2021) closely align with the systemic digitalisation of Chinese society. Platforms such as WeChat and Alibaba have become central not only to economic activity and everyday social interaction but also to the large-scale collection, aggregation, and processing of behavioural data (Marvin et al., 2022). As Ding (2018) argues, the extensive deployment of AI technologies within an already highly developed surveillance system has provided China with vast quantities of readily usable information that can be exploited to train and refine algorithms. In turn, the application of such technologies enhances the state's capacity to monitor and manage populations, creating a self-reinforcing cycle of investment in surveillance infrastructure and data extraction technologies.

At the same time, the latter notes that this potential advantage is not always fully realised due to organisational fragmentation among major tech firms. Nevertheless, while economic incentives remain the primary driver behind both public and private investment in AI, social and political control significantly shape the application of these technologies in China. Taken together, these dynamics fit within the broader theoretical framework of surveillance capitalism previously outlined, stressing the importance of state-level agendas in constructing, consolidating, and ultimately exporting the apparatus of the Chinese surveillance state.

An illustrative example of the application of authoritarian rule through digital technologies is the Sky-Net project, China's primary national surveillance network. Although the initiative was conceived with the objective of achieving comprehensive nationwide CCTV coverage, Luo et al. (2026) note that Sky-Net operates less as a unified system than as a fragmented assemblage of local surveillance subnetworks. Such unevenness is evident not only in the limited integration between surveillance feeds but also in the differing levels of technological maturity. While major urban centres such as Shanghai, Beijing, and Hong Kong employ advanced facial recognition directly linked to the Chinese national biometric database, other

areas continue to rely predominantly on older surveillance devices and infrastructure.

Despite this fragmentation, Sky-Net's surveillance capacity is not necessarily diminished. As Liu (2019) contends, China compensates for the disparities in infrastructural development through the integration of commercial digital platforms into state monitoring practices. In this sense, the effectiveness of surveillance systems increasingly depends on the convergence of physical monitoring systems and privately operated digital ecosystems. This indicates that Chinese surveillance capacity is not constrained by infrastructural fragmentation but is instead structurally enabled by the interaction between state and commercial infrastructures, producing a flexible and scalable surveillance model with significant potential for replication and export.

Exporting the Surveillance State: China's Digital Silk Road

Having analysed the economic dimension of technological development, this section turns to the growing global significance of China's export of surveillance technologies, drawing upon the existing scholarly literature on the subject. As noted by Bernot (2021), since the early 1970s, well before its accession to the World Trade Organisation in 2001 and the state-led economic reforms that accelerated the country's modernisation, China had already become a considerable importer of internationally traded surveillance technology. Major surveillance technology firms from the Global North, including companies such as Cisco and Nortel, took advantage of a regulatory environment marked by indifference and corporate neutrality to export their products to the PRC.

Within the economic framework outlined above, technological development has progressed to the point where Chinese technology firms have emerged among the world's largest corporations, enabling the State to deploy simultaneous, invasive, and highly targeted forms of large-scale surveillance (Feldstein, 2019). Tibet and Xinjiang, two of China's most remote regions, effectively became testing grounds for the Sharp Eyes initiative, named after the communist slogan asserting that 'the masses have sharp eyes' (Gravett, 2022). These regions have played a central role in the expansion of China's surveillance apparatus, contributing to the emergence of one of the world's largest markets for security and surveillance technology (Russon Gilman & Benaim, 2018).

As outlined by Hicks (2022), China′s rise in this market was upheld by the Digital Silk Road (DSR), first introduced in 2015, representing a core backbone of the Belt and Road Initiative (BRI). The assistance provided through the DSR seeks to enhance recipient countries' telecommunications infrastructure, artificial intelligence capabilities, cloud computing systems, surveillance technologies, and other high-tech sectors. Kurlantzick (2020) reports that nearly one-third of the then 138 countries participating in the BRI have actively joined the DSR, with particularly strong engagement from African states.

The DSR places significant emphasis on the export of biometric technologies, entailing two major initiatives: Huawei's Safe City and ZTE's Smart City programmes. According to Atha et al. (2020), the first initiative is framed as a public security solution: through the use of advanced information and communication technologies, the company collaborates with governments and local partners to develop automated and data-driven policing systems. Officially, these projects are presented as tools to support the digital transformation of public security, strengthen urban safety, and improve administrative and economic efficiency. The latter involves the transfer of a wide range of digital infrastructures and technologies designed to collect, process, and integrate previously inaccessible datasets. Both of these projects include the use of CCTV cameras, 5G infrastructure, data centres, mobile payment systems, smart energy meters, parking and traffic management, and integrated control platforms such as emergency response systems and call centres.

Chinese AI-powered smart city and surveillance components have already spread extensively, with smart city platforms deployed in 56 countries and AI surveillance technologies supplied to at least 47 countries (Feldstein, 2019); simultaneously, Chinese data integration security platforms are estimated to operate in at least 80 countries (Hicks, 2022). Following this trend, Chinese policy documents further portray Beijing as a major provider of smart city technologies across regions such as the Maghreb and sub-Saharan Africa.

In this context, Huawei's Safe City initiative – financed through loans provided by China Exim Bank – has been implemented in more than 16 African countries (Passalacqua & Polito, 2024). China's technological footprint on the continent has a wide reach, as Chinese companies have become deeply intertwined in Africa's digital and surveillance infrastructure, to the point where many African states increasingly rely on Chinese providers for core communication services. Indeed, Huawei has constructed around 70 per cent of the continent's 4G networks, outperforming its European competitors; in Ethiopia, ZTE supplied telecommunications infrastructure reportedly enabling state monitoring of opposition activism and journalists, while the company HC3 secured contracts related to Nigeria's airport telecommunications network (Gravett, 2022). Comparable trends have been identified in several African countries – among them Algeria, Botswana, Tanzania, South Africa, and Zimbabwe – where authorities have increasingly partnered with Chinese firms to deploy facial recognition and broader surveillance infrastructures, as part of larger Chinese-backed investments and security agreements (Russon Gilman & Benaim, 2018).

Although some experts worry that Beijing is exporting so-called authoritarian technology to like-minded regimes in an effort to spread an alternative governance model, the reality appears more complex. Chinese surveillance systems have indeed been adopted in several illiberal states, where governments may view such technologies as useful tools for preserv-

ing political control and social stability. However, Chinese firms also supply surveillance and smart-city technologies to democratic countries, demonstrating that exports are not limited to authoritarian markets alone. At the same time, companies based in liberal democracies – including the United States, the United Kingdom, Germany, France, Japan, and South Korea – have likewise exported surveillance equipment to governments with problematic human rights records (Feldstein, 2019).

What's next?

China's unrivalled expansion in the technological realm represents one of the defining geopolitical developments of the contemporary era. The growing integration of surveillance technologies into state practices raises important questions not only about security, but especially about the future balance between state authority, individual freedoms, and democratic accountability. As the number of illiberal regimes rises every year, experts fear that their acquisition of Chinese surveillance systems will enhance their ability to identify and challenge political opponents, dissidents, and protesters, undermining the backbone of civil society and weakening the underpinning principles of the rule of law worldwide. In this context, the debate surrounding Chinese surveillance exports highlights a broader global challenge: striking a balance between fostering innovation and ensuring security while safeguarding fundamental rights.

References

Atha, K., Callahan, J., Chen, J., Drun, J., Francis, E., Green, K., Lafferty, B., Mcreynolds, J., Mulvenon, J., Rosen, B., & Walz, E. (2020). *China's Smart Cities Development* (Report prepared for the U.S.-China Economic and Security Review Commission). SOS International LLC.

Balkin, J. M. (2008). The constitution in the national surveillance state. *Minn. L. Rev.*, *93*(1), 1–25.

Barns, S. (2021). Out of the loop? On the radical and the routine in urban big data. *Urban Studies*, *58*(15), 3203–3210.

Bernot, A. (2021). Transnational State-Corporate Symbiosis of Public Security: China's Exports of Surveillance Technologies. *International Journal for Crime Justice and Social Democracy, 10*(2), 159–173.

Ding, J. (2018). *Deciphering China's AI Dream: The context, components, capabilities, and consequences of China's strategy to lead the world in AI* [Report]. Future of Humanity Institute, University of Oxford.

Feldstein, S. (2019, September). *The Global Expansion of AI Surveillance* [Working paper]. Carnegie Endowment for International Peace.

Gravett, W. H. (2022). Digital neocolonialism: The Chinese surveillance state in Africa. *African Journal of International and Comparative Law*, *30*(1), 39–58.

Hicks, J. (2022, August 1). *Export of digital surveillance technologies from China to developing countries* (Report no. 1190 in K4D Helpdesk series). Institute of Development Studies. 10.19088/K4D.2022.123

Kilic, B. (2025, October 27). *The geopolitics of surveillance capitalism* (Working paper no. 2025-07). Carr-Ryan Center for Human Rights. https://dash.harvard.edu/handle/1/42724133

Kurlantzick, J. (2020). *Assessing China's Digital Silk Road Initiative*. Council on Foreign Relations. https://www.cfr.org/china-digital-silk-road/

Liu, K. Z. (2019). Commercial-state empire: A political economy perspective on social surveillance in contemporary China. *The Political Economy of Communication*, *7*(1), 3–29.

Luo, T., Xing, W., & Xiao, J. (2026). Digital Sensing, Infrastructure of Sovereignty, and the Unmaking of the Chinese Surveillance State. *Theory, Culture & Society*, *43*(2), 37–57.

Marvin, S., While, A., Chen, B., & Kovacic, M. (2022). Urban AI in China: Social control or hyper-capitalist development in the post-smart city? *Frontiers in Sustainable Cities*, *4*.

Passalacqua, C., & Polito, C. (2024). *The Chinese Supply of Surveillance Technology to Africa Going Beyond the Authoritarian Bias* (Working paper no. SOG-WP7/2024). Luiss School of Government.

Pearson, M. M., Rithmire, M., & Tsai, K. (2023). *The state and capitalism in China*. Cambridge University Press.

Peterson, D., & Hoffman, S. (2022, June). *Geopolitical implications of AI and digital surveillance adoption* [Policy brief]. Brookings Institution.

Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models* [Policy brief]. Brookings Institution.

Russon Gilman, H., & Benaim, D. (2018). *China's Aggressive Surveillance Technology Will Spread Beyond Its Borders*. New America. https://www.newamerica.org/insights/chinas-aggressive-surveillance-technology-will-spread-beyond-its-borders/

Ryan, F., Cave, D., & Xu, V. X. (2019, November). M*apping more of China's technology giants: AI and surveillance* (Issue brief, report no. 24/2019). Australian Strategic Policy Institute.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory*, *3*(3), 1–79.