The China Quarterly (2026), 1–17
doi:10.1017/S0305741026103105

RESEARCH ARTICLE

Delegating Digital Policing: The Evolution of China's Security-Industrial Complex

Jingyang Huang

The Chinese University of Hong Kong - Shenzhen, China
Email: jyhuang@cuhk.edu.cn

Abstract

How did China build its formidable digital policing apparatus so rapidly? While prevailing narratives emphasize top-down state direction, this statist perspective obscures critical local dynamics. This article argues that China's security-industrial complex actually emerged from decentralized administrative pressures. Burdened by unfunded, time-sensitive central security mandates, resource-strapped local security agencies abandoned state-led technological development and outsourced to the private sector. Drawing on extensive field interviews (2017–2022) and policy analysis, this study traces the complex's evolution through three interrelated mechanisms: the decentralization of internal security politics, the formation of hybrid public–private partnerships, and the varied transactional behaviour exhibited by capitalists, as well as between government and business, in a multi-layered system. By demonstrating how localized security projects inadvertently catalysed technological innovation, this research reveals the hidden market-driven roots of China's security-industrial complex. It offers a novel framework for understanding how the party-state adaptively leverages capital for building a digital security state.

摘要

中国是如何迅速建立起其强大的数字警务体系的?虽然主流叙事强调自上而下的国家指导，但这种国家主义视角却掩盖了关键的地方动态。本文认为， 中国的"安全产业复合体"实际上源于去中心化的行政压力。面对中央下达的、缺乏资金且时间紧迫的指令， 资源匮乏的地方公安机关放弃了国家主导的技术开发， 转而开始依靠民营部门。本研究基于2017年至2022年广泛的实地访谈和政策文本分析，通过三个相互关联的机制追溯了该体系的演变:国内安全政治的去中心化、公私混合伙伴关系的形成， 以及企业之间、政企之间在多层级制度体系中的多样化交易行为。通过揭示地方性安全项目如何无意间催生了技术创新,本研究揭示了中国安全产业复合体的隐性市场驱动根源。它为理解政党-国家如何灵活运用市场力量实现安全目标提供了一个新的视角。

Keywords: digital police; security-industrial complex; surveillance; public security; government–business relationship

关键词: 数字警务; 安全产业复合体; 监控; 公共安全; 政商关系

Over the past two decades, China's security/surveillance industry has not only enabled the Chinese party-state to build a large and sophisticated surveillance apparatus[1] but has also expanded globally through the widespread exports of commercial digital control technology solutions and security equipment to foreign governments.[2] This raises the question of how China's digital surveillance

1 Xu, Xu 2021; Zhang 2025.
2 Mozur, Kessel and Chan 2019; Rolley 2019.

© The Author(s), 2026. Published by Cambridge University Press on behalf of SOAS University of London. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

capitalism emerged in such a short period of time. One common statist narrative attributes the dramatic rise of China's security/surveillance industry to strong party-state intervention and guidance.[3] Observers holding this perspective often point to Huawei president Ren Zhengfei's 任正非 former military service, the fact that a state-owned enterprise (SOE) holds a controlling stake in surveillance giant Hikvision, and the Party membership of other surveillance capitalists. While this argument on the state's activist role in China's political economy is well-founded, it is also one-sided. In reality, both Huawei and Hikvision experienced extremely difficult start-up histories due to the institutional bias of Chinese capitalism against small and medium enterprises (SMEs) and private firms more generally. Huawei had to undergo a phase of "marketing to rural areas before entering cities" during its business expansion.[4] Hikvision was forced to find its own way out of the wave of state-owned enterprise reform at the end of the last century, and its main technical backbone had to seek angel investment to set up a new company.[5] It is, therefore, more empirically nuanced to examine and trace the specific processes of how the entire surveillance industrial economy has evolved in response to changing national security objectives, rather than simply focusing on the party-state's intentions and capabilities to build a surveillance state.

This paper traces the rise of China's security-industrial complex through domestic security politics, expansive public security technology outsourcing and procurement, and the entrepreneurship invoked by specific temporal and spatial conditions. It employs the term "security-industrial complex" with a view towards reviving the agency approach in studies of Chinese political economy, which emphasizes the strategic behaviour of officials and capitalists in a changing institutional environment.[6] This term was inspired by the "military-industrial complex" and the "surveillance-industrial complex." In social science and historical studies, these terms describe a phenomenon where military forces, or surveillance corporations, and their advocates in the political system form an elite group that promotes political agendas that drive industrial growth to the detriment of state autonomy, welfare distribution and civil rights.[7] In this study, the term "security-industrial complex" does not imply that I view the combination of public security systems and security contractors as an interest group that threatens the party-state's autonomy. Undoubtedly, the advancement of China's surveillance agenda stems first and foremost from the party-state's autonomous security goals; however, under the politics of responsibility with Chinese characteristics, the central government's requirements for achieving these goals are usually general and abstract. In a project-oriented policy implementation, the central government often retains the right to set goals and appraisals in a contractual relationship between the top and bottom levels, while delegating the allocation of incentives for implementation tasks to the provincial government.[8] This incentive structure makes the relationship between lower levels of government and security firms much more flexible and complex than outsiders might think.

This study focuses on the political dynamics of local security responsibilities, particularly the diverse transactional behaviour of and interactions between local bureaucracies and commercial sectors under resource and technological constraints. This adaptive form of surveillance capitalism offers a complementary perspective on China's party-state capitalism.

In the following sections, I first analyse China's domestic security policies since the 1990s and the party-state's ongoing demand for information surveillance infrastructure. The empirical section draws on various data, textual analyses and original field interviews to illustrate how public–private interdependence operates within the security industry. From 2017 to 2022, I conducted 177 interviews across Guangzhou, Shenzhen, Dongguan, Hong Kong, Shanghai, Beijing,

3 Chin and Lin 2022; Beraja et al. 2023.
4 Harwit 2007.
5 Huang, Jingyang, and Tsai 2021.
6 Nee and Opper 2012; Xu, Yan 2024.
7 Mills 2000; Ball and Snider 2013; Wills 2017.
8 Zhou, Xueguang, and Lian 2020.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

Hangzhou, Changsha and Wuhan. Interviewees included the founders or executives of enterprises, mid-level managers of enterprises, leaders of industry associations, central and local serving and retired cadres, technical experts, academics, grassroots civil servants and clerks.[9] I also scrutinized numerous Chinese news reports, industry reports, industry yearbooks, company annual reports, brokerage reports, corporate publications and brochures to support and test the reliability of field materials.

The Security State Seeking Technology

Following the launch of the economic reform and opening up, the social control mechanisms exercised under Mao Zedong 毛泽东 were eroded to varying degrees.[10] This weakening led security bureaucrats to constantly seek technological support to compensate for institutional and coercive manpower deficiencies.[11] Initially, the deployment of security technology by the Ministry of Public Security (MPS) was restricted to crime prevention and property protection. In March 1979, the MPS held a national conference on crime-prevention technology. This meeting resulted in the adoption of the "Trial provisions on the use of science and technology to prevent criminal offences," which officially established "security technology for [crime] prevention" (*anquan jishu fangfan* 安全技术防范) as an integral part of public security operations.[12] The initial technological applications were based on various protection infrastructure and alarm equipment, including burglar-proof doors, locks, safes and special line alarm equipment.

Until the end of the 1990s, local public security bureaus (PSBs) used traditional human-tracking approaches to tackle various mass incidents and social unrest.[13] At this stage, the government lacked both the capability and the capacity to adopt electronic surveillance technology. The aspirations of China's "red engineer generation" leaders to construct a strong information state in the 1990s drove the MPS to explore the use of information technology. The deployment of various electronic surveillance technologies in developed countries after 9/11 further inspired public security technocrats to apply novel technologies to a wide range of so-called "digital" or "smart" policing.[14] As the concept of security continues to expand in China's political context, surveillance technology is increasingly viewed as an effective governance tool and is used extensively by other government departments. Finally, various electronic surveillance applications, combined with Internet of Things (IoT) and web-based technologies, have become a pivotal part of China's smart city-building agenda in this century. China's digital monitoring construction prior to the COVID-19 pandemic can be roughly divided into three periods: Golden Shield (*jindun gongcheng* 金盾工程) and Safe Cities (*ping'an chengshi* 平安城市) (2003–2007); Safe Construction and Safe China (*ping'an Zhongguo* 平安中国) (2007–2014); and Sharp Eyes (*xueliang gongcheng* 雪亮工程) and Smart Cities (2015–2019).

Golden Shield and Safe Cities (2003–2007)

In November 2003, Beijing launched a national strategy to strengthen China's public security through advanced science and technology.[15] One month later, the MPS requested that all regions accelerate the introduction and transformation of advanced and applicable scientific and

9 This research has been reviewed and approved by the Human Participants Research Panel of The Hong Kong University of Science and Technology, with an approved protocol number of 16601418.

10 Tanner and Green 2007; Wang, Yuhua, and Minzer 2015.

11 Scoggins and O'Brien 2016; Liu 2021.

12 "Anfang hangye qibu jieduan (1979–1992)" (The early stages of the security industry, 1979–1992). *China Security and Protection Industry Net*, 21 June 2011, http://www.21csp.com.cn/html/View_2011/06/20/191470.html. Accessed 11 January 2026.

13 Pei 2024.

14 Lyon 2003; Doyle, Lippert and Lyon 2013.

15 Central Committee of the CCP 2003.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

technological achievements to continuously improve the technological content of policing.[16] The MPS Science and Technology Bureau proposed to upgrade its video surveillance systems through research and the integrated application of perimeter alarms and access control technologies. These efforts aimed to improve the security of key infrastructure and establish specialized emergency alarm monitoring networks.

The MPS pilot project for urban alarm and monitoring technology systems (UAMS) was launched in 2004. The experiment introduced digital policing enhancements that focused on improving the incident response capabilities of Chinese cities' 110 command centres and traffic management hubs, while exploring the creation of a unified urban digital monitoring network. In March that year, an MPS research team was instructed to investigate and report back on integrated urban alarm and monitoring systems in Beijing, Jinan, Suzhou and Hangzhou.[17] The MPS then immediately instructed city governments to prepare for the implementation of UAMS.[18] Selection of the pilot localities was not random. Provincial, municipal and autonomous regional governments were required to submit a formal declaration of interest in serving as a pilot location. A panel of MPS experts surveyed the applications of 49 cities before selecting 22 cities in late 2004 to serve as pioneers in "strengthening the police through science and technology."[19]

From the end of 2005, the experimental project was known as Project 3111.[20] It was specifically designed to identify a city in each province, a county within a city, and a community or neighbourhood within a county with suitable conditions to pilot the UAMS. Concurrently, the central government ordered the Beijing Municipal Government to complete the hardware and software infrastructure for the "four networks" public security information system by the end of 2006 in preparation for the 2008 Beijing Olympics. The "four networks" referred to a prevention and control system composed of patrol, community, public security and internal government unit networks.[21] The Olympic security systems, including the Olympic security organization, the command centre and the early warning system, were all completed in 2007.[22] In addition to deploying information technology, Beijing also introduced a system of dividing urban communities into grid cells to enable more targeted information collection and coordinated management at the grassroots level. This was the prototype of "grid management," which would subsequently be fully implemented throughout urban China.[23]

Safe construction and safe China (2007–2014)

In mid-2007, the MPS conducted a preliminary survey of the 3111 Project in Yiwu city 义乌市, Zhejiang province.[24] A year later, the MPS and the MST conducted an on-site assessment of the second batch of 38 cities trialling the "strengthen policing through science and technology" pilot.[25] Following this initial phase, local governments began to implement Safe Cities according to their financial resources and security needs. Building on a wide range of electronic eyes as the foundation for monitoring, the project was also known as the Skynet Project in tender applications and official publicity. Under the Skynet Project, the locations and buildings of financial institutions, cultural monuments, sports venues, educational institutions, medical/healthcare facilities, energy supplies,

16 "Chengshi jianshe" (City construction). *China Security and Protection Industry Net*, 11 November 2010, https://www.21csp.com.cn/zhanti/08pandian/Article.asp?ID=7046. Accessed 20 September 2026.
17 CSPIA 2004, 120.
18 CSPIA 2006, 315.
19 Ibid.
20 Xu 2021.
21 CSPIA 2007, 70.
22 Ibid., 71.
23 Chen, Huirong, and Greitens 2022; Xu, Jianhua, and He 2022.
24 CSPIA 2007, 7.
25 CSPIA 2008, 69–70.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

catering and entertainment, commercial and service enterprises, mines and residential communities were all incorporated into the city's monitoring and alarm management platform.

At the same time, the MPS became concerned about the practical implications of collecting surveillance data. In 2010, the MPS stipulated that by the end of 2013, the construction of UAMS should be basically completed in urban areas nationwide to achieve full coverage of key areas.[26] The related document highlighted the tasks that provincial, municipal, county and district-level public security organs had to undertake to complete the construction of databases to achieve effective cross-regional, cross-sector and interdepartmental information sharing and the proper management of video resources. The central MPS required city governments to expand their coverage of UAMS, locate any blind spots in video monitoring and increase and adjust the number of UAMS points in key and complex areas such as those with high crime rates and a large floating (migrant) population.

Once the foundations of urban monitoring infrastructure were established, the state turned its attention to monitoring rural areas. In 2009, the MPS began deploying security technologies across rural regions. In 2011, it proposed installing video surveillance and network alarm systems in 80 per cent of rural regions in the east, 70 per cent in central regions and 60 per cent in the west by 2015. The systems would be primarily located in areas with township governments or high rates of urbanization and industrialization.[27]

It was also during this phase that surveillance and security technologies were applied beyond the bounds of public safety. As one technocrat from the MPS explained:

> Security and prevention are not just a public security technology concept; they refer to a comprehensive security and prevention (*da anfang* 大安防) concept, meaning that everyone, everything and everywhere is safe. All the objects to be protected – people, property, buildings – are to be included within the scope of security applications.[28]

In May 2013, at a conference on "Deepening the building of Safe China," Xi Jinping 习近平 issued the instruction that "the building of Safe China should be planned in the overall development of the socialist cause with Chinese characteristics."[29] In 2014, Xi further proposed a "holistic security" (*zongti anquanguan* 总体安全观) concept, also known as "comprehensive security." Such initiatives further expanded the deployment of surveillance and policing technologies beyond the maintenance of public order and social security into the realm of "comprehensive social governance."[30] In a meeting on 3 November 2014, Beijing announced that local governments would be expected to take on "clearly defined security responsibilities over public squares, stations, airports, schools, kindergartens, hospitals and other key places, to fully implement the grid patrol forces, internal security mechanisms … and other means of systematic governance, to achieve full coverage of all types of security areas and security elements [and] to improve the overall level of [crime] prevention."[31]

Smart Cities and Sharp Eyes (2015–2019)

Not long after the implementation of Safe Cities, China began to promote Smart City projects at the local level from 2012. Local governments combined many of the completed and planned video surveillance projects with the Smart City programme initiatives. Various information-collection,

26 Ministry of Public Security 2010.

27 "Gonganbu guanyu zai nongcun diqu kaizhan anquan jishu fangfan gongzuo de yijian" (MPS opinions on the development of security and protection technology in rural areas). *China Security and Protection Industry Net*, 15 March 2012, https://www.21csp.com.cn/zhanti/08pandian/Article.asp?ID=7046. Accessed 20 September 2026.

28 Interview with retired MPS official, Beijing, November 2021.

29 "Xi Jiping: ba renmin qunzong dui ping'an Zhongguo jianshe de yaoqiu zuowei nuli fangxiang" (Xi Jinping: We must take the people's expectations for building a safe China as our guiding principle). *People's Daily*, 1 June 2013, https://cpc.people.com.cn/n/2013/0601/c64094-21697870.html. Accessed 5 January 2026.

30 Chin and Lin 2022; Trevaskes and Lin 2024.

31 CSPIA 2014, 7.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

analysis and surveillance platform systems were created to address different political and administrative priorities. These systems were designed to digitally transform information access within the constraints of fragmented institutions and improve the efficiency of supervision or coordination. Consequently, these platforms vary in their design and application across departments.

In April 2015, the State Council issued a new policy urging local governments to further strengthen the construction of public security "prevention and control" networks in key industries, as well as in townships, streets and village communities. The policy called for enhanced interoperability and in-depth sharing of information resources, accelerated development of an integrated information technology platform to enable horizontal and vertical data sharing, and improved system interconnection and information interoperability. It also emphasized integrating crime-prevention and control technologies more fully into the overall planning of Smart City initiatives.[32] In the same year, the MPS and nine other ministries jointly issued "Opinions on strengthening the construction of public security video surveillance networking applications," which called for full coverage of public security video surveillance and full network sharing. This policy sought to integrate data from cameras installed by various departments during the Smart Cities phase.[33]

The central and provincial governments established a cross-departmental working group for the construction, networking and application of public security video surveillance and began organizing a number of trial sites across the country. In 2016, the central government selected 45 cities to receive central subsidies for the construction of dedicated video image networks.[34] The party-state also incorporated security and surveillance technologies into comprehensive governance standards and Smart City evaluation indicators.[35] Consequently, different levels of government sought to increase public-area video surveillance coverage rates, network coverage rates and the number of new HD cameras.

Then, in 2017, the so-called "mass-line public security prevention and control project" (*qunzhongxing zhi'an fangkong gongcheng* 群众性治安防控工程), also known as the "Brightness Project" or "Sharp Eyes Project," was fully extended to the street and village levels. The Sharp Eyes Project comprised three aspects: the installation of high-definition (HD) cameras at major road junctions and crowd-gathering areas; the integration of fixed video surveillance, mobile video collection and alarm systems, which were then connected to the monitoring platform at the county, township and village administrative levels; and the channelling of these video images through the TV network to the home digital TV terminal. It continues to provide officials with the ability to monitor the security situation within their jurisdictions in real time and to detect any mass gatherings. At the same time, it allows individuals to report any contentious issues to the administrators at any time.[36] Overall, the Chinese government's expanding interpretation of security continues to create new applications for security and surveillance technologies.

Digital Security State Makes Capitalists

The Chinese government's consistent demand for information infrastructure over the past three decades has undoubtedly created stable market expectations for China's business sector, encouraging some domestic companies to make ongoing strategic investments in related technology development.[37] Among these, investments in digital security projects carry significant indicative value for the entire industry.[38] Numerous analyses based on Chinese government procurement data consistently

32 CSPIA 2015, 2.
33 Ibid.
34 CSPIA 2016, 2.
35 Ibid., 13.
36 Batke and Ohlberg 2020; Mozur, Xiao and Liu 2022.
37 Song, Zhang and Meng 2025.
38 Contracts from local PSBs at various levels across China account for 65.8% of all surveillance-related contracts. See Batke and Ohlberg 2020.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

highlight that the expansion of government investment in security has created a large community of shared interests. Both higher-level administrative requirements for security infrastructure and local social instability motivate local governments to procure surveillance systems.[39] These procurement demands foster an environment of incentive compatibility, thereby stimulating the diffusion and innovation of surveillance technology within China's industrial sector.[40]

However, the establishment of public–private alliances between coercive agencies and the business sector (particularly the private sector) through large-scale government procurement did not occur until 2009. Following the tax-sharing reform, the central government did not provide sufficient financial support for local governments' early Safe City infrastructure installation and technological upgrades.[41] In China's decentralized institutional context, the central government ensures that local governments and administrative agencies are incentivized to carry out the centre's political objectives through a top-down system of personnel management.[42] Specifically, the central government is responsible for setting administrative goals and for monitoring and evaluating task completion, while the local government, which handles the tasks, has the power to allocate incentives.[43] The process of building digital surveillance capacity has followed in this vein. The central government, particularly the MPS, set the goals for each round of surveillance projects, and then lower-level governments were responsible for implementing the tasks. These tasks were always time sensitive, but the central government did not offer financial incentives for the construction of local Safe Cities. Instead, the power to allocate incentives for undertaking the projects was vested at the provincial and municipal levels, which is why each locality developed different implementation plans. Faced with increasingly frequent demands for security infrastructure in public institutions, local public security departments (PSDs) came to depend on technological outsourcing. This led the security industry to separate from the state-led internal management of technical departments, resulting in adaptive surveillance capitalism at the local level.

Early technology providers: red engineers and tech brokers

In the first decade after security and crime-prevention technology became a formal part of the PSD in 1979, MPS technocrats sought to retain control over technology development and production. At the ministry level, two research institutes were tasked with developing related technologies: the First Research Institute of the MPS in Beijing and the Third Research Institute of the MPS in Shanghai, both of which were reorganized in 1984. The First Institute mainly engaged in the research and development of police communications, security screening, access controls, alarm systems and protective gear; the Third Institute initially focused on developing various types of technical reconnaissance, electronic forensics and cryptography, before turning to network security and intelligent policing with the advent of the digital era. By 1986, MPS-developed products had expanded to cover tasks in security, firefighting, traffic control, forensics technology and policing. At that time, the Ministry of Machinery and Electronics Industry intended to reclassify categories within the machinery and electronics industry. Following active lobbying by the MPS, the "public security products industry" was created in 1991 as a subcategory of machinery and electronics and placed under the management of the MPS. This marked the first time the MPS was given a mandate to manage these products and the market.[44]

One entrepreneur, who originally worked for the government but then went into security entrepreneurship, explained that, "early on, security did not qualify as a 'business' or 'industry,' but

39 Beraja et al. 2023; Liang, Li and Guo 2025.
40 Beraja, Yang and Yuchtman 2023; Liang, Li and Guo 2025.
41 Greitens 2017.
42 Landry 2008; Heilmann 2018.
43 Zhou, Xueguang, and Lian 2020.
44 Interview with technocrat, Beijing, November 2021. See also Liu, Ping 2007.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

rather it was basically a state-sponsored administration."[45] In the 1980s, the government explicitly prohibited and cracked down on companies engaging in the production of security-related products. Another security entrepreneur with public sector experience reflected:

> If I have to say that a security industry existed in the 1980s and 1990s, it was limited to physical protection. It was probably closer to the property protection industry in developed countries, but at a much lower end. This is a very different situation from the current industry, which is dominated by digital video surveillance. The only industries that allowed the private sector to participate at that time were safe boxes, security doors, security locks, etc.[46]

At the provincial level, the PSDs also had specialized research offices and factories to develop and produce related security products, such as alarms, wired alarm networks, bullet- and explosion-proof equipment, and riot gear. Before the reform era, China's national innovation system was modelled on that of the Soviet Union and relied on state-funded research. This legacy did not align with the organizational form or the technological orientation of China's thirst for developing information technology.[47] During the demilitarization process that began in the 1980s,[48] many military personnel were sent to work in local PSDs and their affiliated enterprises and factories. On the surface, the transfer of some military personnel, especially junior technical personnel, to the public security system was beneficial for enriching the public security science and technology team. However, according to one official, the most valuable technical personnel either remained in the military or went to the MPS. The transferred military cadres and technicians were helpful in enhancing ICT capabilities at the central level, as they came with certain political and social networks and technical information; however, their contribution to enhancing the R&D capabilities and production efficiency of enterprises was ultimately limited.[49]

Public safety researchers faced significant hurdles transitioning to digital technologies, and securing financial support was just as challenging. The MPS science and technology department had long fought for the inclusion of public safety technology in the national five-year science and technology plan. This multi-year effort finally succeeded for the 11th Five-Year Plan. In 2006, feasibility reports for several joint projects between national research institutes, the MPS and some local PSBs were approved and included in the plan.[50] At the local level, however, technocrats could not wait for the national strategy to be implemented. Faced with the rapidly changing social and political security landscape at the turn of the century, they needed to find their own ways to upgrade.

During the "bringing in" (*yinjinlai* 引进来) era, public security technocrats in the provinces at the forefront of the opening-up policy sought access to technology from the West. Owing to their proximity to Hong Kong, technocrats in Guangdong were uniquely positioned to learn and introduce Western technology. In the 1980s and 1990s, technology transfer occurred both formally and informally. Alarm equipment was the first security technology to attract interest. By visiting factories and companies in Hong Kong, mainland technocrats gained vital technical inspiration, enabling them to significantly upgrade domestic alarm systems upon their return. Local PSB-affiliated companies and industry associations also procured Western security technology through commercial exchanges and foreign trade transactions. In addition, many technology brokers emerged in the early reform and opening-up period. These individuals usually had strong political backgrounds as well as the ability to connect with foreign industries. They provided PSBs in coastal areas with commercially proven

45 Interview with private entrepreneur, Guangzhou, October 2018.
46 Interview with the leader of an industrial association, Guangzhou, October 2017.
47 Cheung 2022.
48 Zhou, Taomo, and Weng 2024.
49 Interview with former technocrat, Guangzhou, May 2018.
50 Interview with technocrats and researchers, Beijing, November 2021. See also CSPIA 2006, 312.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

overseas security products through formal or informal import channels, facilitating mainland technical research and development. These technology brokers were particularly active in the wake of the Tiananmen crackdown when the West imposed technology sanctions on China.

The security industry is not restricted to political actors. Driven by grassroots entrepreneurialism, many business owners coincidentally saw a huge potential need to maintain public security in China. For example, Mr Ma, a Malaysian-born overseas Chinese businessman (*qiaoshang* 侨商), runs a company that manufactures security screening equipment. He started his business by renting out screening apparatus to PSBs and security companies managing concerts and sporting events. When asked how he expanded his business, Mr Ma admitted he "didn't know anyone" at the beginning:

> Our method was very stupid, that is, we looked up information about local shows and events in newspapers and on the TV and then called security agencies one by one to try our luck. Of course, there were always more bumps than successes, but once we were successful, some local PSBs or security companies would offer to refer us to other security agencies in the same city because the need is real for other managers.[51]

In the early stages of building security infrastructure, just a few agencies and sites, such as prisons, banks, museums and government offices, required alarm and surveillance systems. However, with the widespread urbanization of coastal areas in the late 20th century, government-owned enterprises struggled to meet the demand for surveillance projects. The rapid technological changes contrasted with the slow pace of work in public security technical departments, which remained constrained by economic incentives and limited human resources. Local bureaucrats, facing an urgent need for new technology and equipment, quickly looked to outsource public security procurement to private and foreign sectors.

Adaptative surveillance capitalism from below

The state's gradual step away from the independent development of security equipment and the building of infrastructure opened the door for the private sector. In the 1990s, private security contracts stemmed from small-scale outsourcing by certain SOEs, public institutions, utilities, key government departments and real estate development projects, rather than from large-scale public investments. In China, public facilities and buildings are legally required to install the appropriate security surveillance systems before they are permitted to open.

Such business opportunities were initially grabbed by division/section-level (*chu/ke* 处/科) officials and technical cadres already working in the security sector, in related companies or research institutions. One entrepreneur, who left the public security agency in 1998, launched his business because he believed he could find the right technology partner and that his background in government service would foster greater trust with government departments. This calculation was proved correct when, in the early days of UAMS construction, his joint venture won a large number of local contracts.[52]

China's accession to the WTO in 2001 inspired another wave of entrepreneurship among SME security and surveillance equipment manufacturers. A senior executive of a listed company recalled his company's entrepreneurial journey: "In the 1990s, not far from our office building were several very large specialized wholesale markets (*zhuangye shichang* 专业市场), which were managed by the government. The markets were very chaotic and the security was not good, so we started our business by installing alarm and monitoring systems there and then slowly expanded to other areas."[53] For at least a decade beginning in 1990, the business model adopted by these private security engineering firms was primarily to assemble foreign products acquired from various sources into

51 Interview with private entrepreneur, Shenzhen, October 2018.
52 Interview with private entrepreneur, Guangzhou, January 2018.
53 Interview with private entrepreneur, Guangzhou, March 2022.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

alarm and prevention systems that could easily be applied and operated by the agencies. Additionally, entrepreneurs with public-sector backgrounds gradually left inefficient state-owned agencies, using their accumulated expertise to enter the growing markets for surveillance equipment manufacturing and system integration.

During the late 1990s and early 2000s, foreign enterprises also played a major role. A typical example is the US company C&K, which became the main supplier of China's early urban alarm systems after it provided the security architecture for the 1990 Asian Games in Beijing. By 1993, the new alarm centres nationwide had almost universally adopted its products and services. The company worked with a domestic partner to develop alarm centre software specifically for China's public security agencies. The expansion of the city alarm centre and alarm networking business made C&K's China branch the most profitable affiliate in the mid-1990s.[54] Similarly, Honeywell contributed video surveillance systems, while joint ventures, such as that between Huawei and the US-based 3Com, facilitated the integration of advanced networking technologies.

Demand in the private security market, driven by policies mandating the installation of surveillance equipment, began to decline after the mid-2000s. As Safe City initiatives expanded nationwide, security firms increasingly focused on winning bids for large-scale government public projects.

Most entrepreneurs and officials noted that the four-trillion-yuan stimulus investment plan promoted by the central government in 2008–2009 had a significant impact on the overall prosperity of the security industry. One security entrepreneur observed:

> Before 2008, when Safe Cities was in its pilot phase, non-experimental cities or regions rarely invested in surveillance specifically, unless they were in a particularly good financial position or if the local governor really thought it was necessary. Financial support was less than adequate and governments rarely invested in security with borrowed funds, but after 2008, there was a big difference.[55]

During the Safe Cities phase, the construction of security systems generally followed two models. Under the first, the PSB built, operated and managed the systems, based on a self-built proprietary network and direct access to an internal network of public security information and communications. Under the second model, UAMS was outsourced, with the PSB instructing state-owned telecommunications operators to fund, construct, operate and manage the system. Unlike the first model, such systems were built on a non-public security proprietary network and local PSDs rented the monitoring systems from SOEs. Prior to 2008, local PSBS lacked the financial resources to cover the full cost of building the urban surveillance system, so most local governments adopted the second model. In Zhejiang, for example, 45,613 security video surveillance cameras were funded by the government ahead of the Olympic Games in 2008. Local PSBs installed 20,190 of these cameras using about 800 million yuan in construction funds, accounting for 64 per cent of the total public expenditure. The remaining 25,423 cameras were installed and operated by state-owned telecommunications operators, at a cost of about 450 million yuan (36 per cent of the total public expenditure).[56] Fewer cameras were installed by PSBs than by state-owned enterprises.

After 2008, local governments incorporated the building of monitoring systems into their local infrastructure investment plans. A provincial official described the shift in the government's financial spending strategy over several years:

> Electronic cameras are also considered an essential part of the information infrastructure, with a key security governance role. As long as there is enough financial backing, local governments

54 Interview with private entrepreneur, Guangzhou, September 2019.
55 Interview with private entrepreneur, Guangzhou, October 2018.
56 CSPIA 2008, 118.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

are willing to allocate more resources to develop surveillance systems. In the past, localities had less access to funding.[57]

Guangdong, for instance, included "comprehensive video surveillance" (*da shipin* 大视频) among its key financial support projects under its "Safe Guangdong" development plan. Companies are also acutely aware of the changes in the business sphere: "Before 2008, it was very impressive for a company to get contracts in the tens of millions of dollars; in the years after 2008, many of the contracts awarded were in the hundreds of millions."[58] Since completing the Safe Cities project, the Guangdong provincial PSD has successively implemented its "Three-year plan for the construction of the social security video surveillance system in Guangdong (2012–2014)," the "Plan for the construction of social security video surveillance system in Guangdong (2016–2017)" and the "13th Five-Year Plan for the construction of public security video surveillance" to expand the coverage of cameras in Guangdong. Between 2012 and 2014, 1,084,000 new video image collection points were constructed;[59] from 2015 to 2016, another 765,000 were built.[60] Under top-down political pressure trickling down from the provincial government down to the street level, different PSBs had to upgrade their various security needs, presenting opportunities for private companies. As one supplier reasoned: "Even if we could not get city-level projects like the big companies, we can still fight to get district (county) security projects."[61]

Transactional Behaviour in the Security-Industrial Complex

The growing number of security contracts has spurred capitalists to invest in the development of surveillance products that meet the increasingly sophisticated technological requirements of both the public and private sectors. However, in an institutional environment lacking stable and credible commitments,[62] transactions – whether within industries or between government and enterprises – are not always enforced or legally protected. Local governments might choose not to honour contracts with businesses based on their own considerations, and such breaches face no penalties. The weakness of the rule of law also means that cooperation among market entities lacks effective contractual constraints, instead being driven by various opportunistic impulses. For heuristic purposes, this section identifies four types of transactions in China's security-industrial complex. This classification distinguishes between networks of security capitalists and global stakeholders on the one hand, and networks between security capitalists and state agencies on the other. Transactions at the local level are sometimes irregular, clientelist and opportunistic,[63] but at other times, they can be long-term and regular, with positive incentives to stimulate sustained technological development.

Irregular forms: opportunistic engagement and ad hoc assignment

In the coastal regions with the earliest exposure to the global production chain in the security industry, the first generation of SMEs was mainly engaged in renting or selling foreign products. Then, some enterprises began searching for suitable overseas companies to partner with, looking to become their original equipment manufacturing (OEM) contractors. This shift was helped by the competitive dynamics of the Chinese internal market, which exacerbated cost pressures on foreign firms, forcing them to localize their activities. The evolving business practices of domestic private firms coupled

57 Interview with official, Guangzhou, October 2018.
58 Interview with private entrepreneur, Guangzhou, October 2017.
59 CSPIA 2015, 133.
60 Field notes, Guangzhou, October 2020.
61 Interview with private entrepreneur, Guangzhou, June 2018.
62 Hou 2019; Xu, Chenggang 2025.
63 Wedeman 2012; Hou 2019; Leng 2025.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

with foreign firms' desire for domestic suppliers constituted the backdrop for the security capitalists' opportunistic engagement, which was found mainly in transactions among SMEs. Foreign SMEs tended to be more opportunistic in knowledge transfer, given their eagerness to expand their markets. They formed joint ventures with local producers and also granted their domestic production partners more operational autonomy, allowing them to adapt their products to the Chinese market.[64] Their domestic partners exploited this opportunity to build up their own technological capabilities. An institutional environment with weak intellectual property rights protection allowed these local companies to "borrow" designs from foreign SMEs to start up their own business.[65]

Another type of opportunistic engagement bypassed the establishment of linkages between local and foreign firms. Instead, by taking advantage of the low costs and supply chain efficiencies created by the massive shift of the global electronics production chain to China, local firms networked directly with local suppliers of components to replicate goods produced for multinational corporations (MNCs). These copycats even formed a unique industrial cluster in the Pearl River Delta region, known as the "Shanzhai 山寨 economy." Not only were the goods produced by copycat manufacturers superficially authentic, but some security products had incremental features added to them. In the early 2000s, security engineers would knowingly, or unknowingly, purchase these products for small surveillance projects run by local PSBs – in some cases, without the knowledge of the grassroots public security officials.[66]

This illustrates the volatility of dealings between Chinese security capitalists and state agents. In differentiating between "assignment" (*chengbao* 承包) and "contracting" government–business relations in China,[67] Philip C.C. Huang argues that an imperfect rule of law and unrestrained state power allow public agencies to infringe on market players to promote their own interests.[68] As a result, instead of reciprocal contracting, where both parties honour their responsibilities, market players find themselves subject to unilateral government demands. This ad hoc assignment phenomenon occurs frequently at the grassroots level of politics. Many interviewed entrepreneurs indicated that in the early stages of digital surveillance construction (2001–2006), their business model relied on purchasing foreign products for Safe Cities networks. Some simply sold products to engineers who had ties with the local authorities, while others acted as both product agents and engineers, directly securing contracts from local PSBs. Because security projects were outsourced in a very fragmented and decentralized manner, SMEs could easily secure contracts at the district level through either formal public bidding or informal favours and social connections.[69]

This fragmented procurement procedure offered SMEs both advantages and drawbacks. The upside was that start-ups did not have to build political relationships with higher authorities to develop their businesses. Instead, it was much easier to grow by meeting the security infrastructure demands of the different grassroots public agencies. The disadvantage, however, was that payments from many agencies were unreliable, and enterprises were often forced to finish government-assigned projects within short timeframes and for very low returns. For instance, several security entrepreneurs recounted occasions when local governments had demanded subcontractors complete projects ahead of deadlines, even when funding had not been secured; many payments went unpaid for up to three years, or even longer, by which time some companies had gone bankrupt.[70]

It should be noted that ad hoc assignment is harmful to both public agencies and the market. Rather than competing on the quality of the products offered or the engineering, security capitalists secure short-term benefits through rent-seeking access to government contracts. For example,

64 Chen, Ling 2020.
65 Dimitrov 2009.
66 Interview with local official in Shenzhen, November 2019.
67 Zhou, Li'An 2016.
68 Huang, Philip C.C. 2019.
69 Wank 2001.
70 Field notes, Guangzhou, January 2017.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

one police officer complained about an electronic system used for assigning tasks within the local PSB. Instead of improving efficiency, the system added more stress to front-line work. The company that developed this system did not have a good reputation in the industry, and it was impossible to find someone to maintain and upgrade the system. Relatedly, poor electronic surveillance engineering installations at the grassroots level often plague higher-level policing. Corruption in security projects was common during the 2000s. It was an unspoken norm that enterprises gave kickbacks (*huikou* 回扣) to officials on projects in some small cities. In one exposed corruption case, it was revealed that a local public security official had tailored the bidding criteria to suit a specific enterprise.[71]

Regular forms: strategic coupling and subcontracting

Increasing globalization allowed Chinese security manufacturers to enter the market as OEM producers or as component suppliers in specialized areas, helping them gradually move up to the middle of global value chains.[72] Local manufacturing firms with ambitions to develop their own products engaged in "strategic coupling" with global intellectual property networks and supply chains.[73] In the case of electronic surveillance, the localization of multinational firms helped domestic firms with some R&D capabilities to trade with local foreign OEMs for what used to be expensive digital technology components at much lower prices. China's accession to the WTO in 2001 lifted barriers to accessing foreign high-end technology components. This allowed domestic firms to strategically couple with important front-end chip, sensor and camera suppliers to form relatively stable supply alliances. To improve their technical capabilities, these local enterprises began to purchase patents and hire overseas returnees with technical expertise, as well as engineers formerly employed by MNCs. With broadened and diverse access to technical support, certain ambitious domestic enterprises not only recombined technologies but also introduced technological innovations in digital surveillance hardware and software to meet the party-state's increasingly demanding surveillance requirements. Due to their cutting-edge technology and technical indispensability, a handful of domestic surveillance tech giants gradually established stable contracting arrangements with provincial and municipal departments.

The concept of asset specificity is a key mechanism in explaining the emergence of more regular subcontracting relations between security capitalists and state agents during the large-scale technology outsourcing after the 2010s. For example, when a provincial PSD or city PSB invests in a networked electronic surveillance system, it not only has to purchase high-quality surveillance cameras but must also rely on security companies to provide technicians stationed in the control centre to maintain, sustain and continuously improve the operation of the system. In such a scenario, the leverage granted by the surveillance system's asset specificity counterbalances the potential threat of arbitrary governmental behaviour. Government departments with an ongoing need for effective, stable and advanced surveillance technology tend to establish long-term, regular subcontracting relationships with companies with a strong technical capacity. As the government grows increasingly reliant on tech companies, these firms can persuade administrative departments to procure technological products that are not always necessary. Corporate interests are not the key drivers of this lobbying – it often stems from the competition for survival among different technical teams within the tech companies themselves. According to a former product manager at a leading company:

> To meet government technical requirements, there can be different technical approaches or system integration methods. Our various engineering teams will strive to incorporate their

71 Lu and Wang 2023.
72 Chen, Ling 2020.
73 Yeung 2016.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

team's technical elements into the surveillance system to ensure their own survival and development within the company. It must be acknowledged that some of these technologies may not be appropriate.[74]

As China's security-industrial complex has expanded to encompass a vast network of SOEs, SMEs, tech giants and global stakeholders,[75] and as public security projects have grown in technological complexity, the patterns of transactional behaviour within the industry and between government and enterprises have progressively shifted from irregular to more regularized practices. Ad hoc assignments plagued by unreliable payments and corruption in grassroots projects have increasingly been supplanted by long-term subcontracting arrangements, where asset-specific investments in advanced technologies foster mutual dependence, reduce volatility and incentivize reliable contractual commitments to support the party-state's sophisticated surveillance needs. Despite government defaults, companies still found profit margins owing to the massive expansion and volume of digital policing projects (2008–2016). As several entrepreneurs noted, while some local projects were unprofitable, others in more economically developed regions did prove profitable, providing them with the incentive to re-invest.[76]

Conclusion

This paper has traced the evolution of China's security-industrial complex as a dynamic interplay between the party-state's expansive security imperatives and the adaptive strategies of local officials and capitalists within a decentralized institutional framework. The findings offer contributions to the study of party-state capitalism.[77] They refine the models that portray the state as an engineer directing industries through interventions.[78] Instead, the evidence counters this narrative by demonstrating how local security agencies, under the duress of performance evaluations, abandoned cumbersome in-house development due to fiscal and temporal constraints, outsourcing instead to the agile private sector and fostering a form of adaptive surveillance capitalism. This resonates with recent research in Chinese politics on the outsourcing of state mandates to the private sector.[79] Security here is not merely a tool of control but a force for innovation, where the party-state's autonomy is preserved through flexible delegation, yet is subtly reshaped by the entrepreneurial logics it unleashes.

In summary, the security-industrial complex illustrates how China's political economy thrives on controlled improvisation,[80] yielding a security state with unexpectedly capitalist traits. However, this adaptive model raises pressing questions for both scholarship and policy. As China's surveillance and digital policing exports proliferate amid geopolitical tensions, how might increasing international sanctions disrupt these global couplings? Domestically, the tension between expansive security spending and fiscal strains at lower levels exacerbates contract defaults by state agencies,[81] thereby undermining the fragile incentive structures that sustain the digital industry's growth.

Acknowledgements. This project was supported by the Hong Kong Research Grants Council's General Research Fund (#16601219) and the Hong Kong Research Grants Council's Postdoctoral Fellowship Schemes. The article was made Open Access thanks to the support of the University Development Fund (UDF01004117) at The Chinese University of Hong Kong, Shenzhen. The author gratefully acknowledges feedback from Yongshun Cai, Martin Dimitrov, Wenkai He, Yue Hou, Siqin Kang, Pinghan Liang, Yi-min Lin, Yuchen Liu, Huihua Nie, Kevin O'Brien, Lynette Ong, Ben Read, Ran Tao, Kellee Tsai, Andrew Walder, Ge Xin, Jack Xing, Jianhua Xu, Dong Zhang, Han Zhang and Wenjuan Zheng, as well as the participants

74 Interview with former manager, Hangzhou, November 2022.
75 Huang, Jingyang, and Tsai 2022; Bernot 2026.
76 According to feedback from some entrepreneurs, this transaction pattern continued at least until the end of COVID-19.
77 Pearson, Rithmire and Tsai 2023.
78 Wang, Dan 2025.
79 Liu, Lizhi 2024; Chen, Huirong, and Bian 2025; Leng 2025; Ong, Nie and Lee 2026.
80 Ang 2025.
81 Greitens 2026.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

in the conferences and workshops held by The Chinese University of Hong Kong (Shenzhen), Shanghai Jiaotong University, Sun Yat-sen University and Zhejiang University.

Competing interests. None.

References

Ang, Yuen Yuen. 2025. "Adaptive political economy: toward a new paradigm." *World Politics* **77**(1), 51–67.

Ball, Kirstie, and Laureen Snider (eds.). 2013. *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. Abingdon: Routledge.

Batke, Jessica, and Mareike Ohlberg. 2020. "State of surveillance: government documents reveal new evidence on China's efforts to monitor its people." *ChinaFile*, 30 October, https://www.chinafile.com/state-surveillance-china. Accessed 20 October 2025.

Beraja, Martin, Andrew Kao, David Y. Yang and Noam Yuchtman. 2023. "AI-tocracy." *The Quarterly Journal of Economics* **138**, 1349–1402.

Beraja, Martin, David Y. Yang and Noam Yuchtman. 2023. "Data-intensive innovation and the state: evidence from AI firms in China." *The Review of Economic Studies* **90**(4), 1701–23.

Bernot, Ausma. 2026. "Police cloud: functional modularity in China's cloud public security infrastructure." *Regulation and Governance* **20**(1), 90–104.

Central Committee of the CCP. 2003. "Zhonggong zhongyang guanyu jinyibu jiaqiang he gaijin gong'an gongzuo de jueding" (Further strengthening and improving public security work), 18 November, http://www.reformdata.org/2003/1118/4921.shtml. Accessed 20 September 2026.

Chen, Huirong, and Yangxin Bian. 2025. "Policy experimentation within bureaucratic power networks: the 'police–business cooperation' scheme in urban China." *The China Quarterly* **264**, 938–956.

Chen, Huirong, and Sheena Chestnut Greitens. 2022. "Information capacity and social order: the local politics of information integration in China." *Governance* **35**(2), 497–523.

Chen, Ling. 2020. *Manipulating Globalization: The Influence of Bureaucrats on Business in China*. Stanford, CA: Stanford University Press.

Cheung, Tai Ming. 2022. *Innovate to Dominate: The Rise of the Chinese Techno-security State*. Ithaca, NY: Cornell University Press.

Chin, Josh, and Liza Lin. 2022. *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. London: St. Martin's Press.

CSPIA (China Security and Protection Industry Association). 2004; 2006; 2007; 2008. *China Security and Protection Industry Yearbook*. Beijing: People's Liberation Army Press.

CSPIA. 2014; 2015; 2016. *China Security and Protection Industry Yearbook*. Beijing: People's Public Security University of China Press.

Dimitrov, Martin K. 2009. *Piracy and the State: The Politics of Intellectual Property Rights in China*. New York: Cambridge University Press.

Doyle, Aaron, Randy Lippert and David Lyon (eds.). 2013. *Eyes Everywhere: The Global Growth of Camera Surveillance*. New York: Routledge.

Greitens, Sheena Chestnut. 2017. "Rethinking China's coercive capacity: an examination of PRC domestic security spending, 1992–2012." *The China Quarterly* **232**, 1002–25.

Greitens, Sheena Chestnut. 2026. "China's internal security spending: an assessment of new data." *The China Quarterly* **266**, 470–480.

Harwit, Eric. 2007. "Building China's telecommunications network: industrial policy and the role of Chinese state-owned, foreign and private domestic enterprises." *The China Quarterly* **190**, 311–332.

Heilmann, Sebastian. 2018. *Red Swan: How Unorthodox Policy-making Facilitated China's Rise*. Hong Kong: The Chinese University of Hong Kong Press.

Hou, Yue. 2019. *The Private Sector in Public Office: Selective Property Rights in China*. New York: Cambridge University Press.

Huang, Jingyang, and Kellee S. Tsai. 2021. "Upgrading Big Brother: local strategic adaptation in China's security industry." *Studies in Comparative International Development* **56**, 560–587.

Huang, Jingyang, and Kellee S. Tsai. 2022. "Securing authoritarian capitalism in the digital age: the political economy of surveillance in China." *The China Journal* **88**, 2–28.

Huang, Philip C.C. 2019. "In search of a long-term development path for China: starting from differences between assigning responsibility and contracting." *Rural China* **16**(2), 157–183.

Landry, Pierre. 2008. *Decentralized Authoritarianism: The Communist Party's Control of Local Elites in the Post–Mao Era*. New York: Cambridge University Press.

Leng, Ning. 2025. *Politicizing Business: How Firms Are Made to Serve the Party-state in China*. New York: Cambridge University Press.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

Liang, Pinghan, Xijie Li and Yuchen Guo. 2025. "Local governments and the diffusion of video surveillance in China: evidence from the public procurement contracts." *Journal of Chinese Political Science* **30**(3), 421–447.
Liu, Lizhi. 2024. *From Click to Boom: The Political Economy of E-commerce in China*. Princeton, NJ: Princeton University Press.
Liu, Ping. 2007. "Jianzheng Zhongguo anfang zhuanfang: gong'anbu zhuangbei caiwuju fujuzhang Tao Junsheng" (Interview about witnessing China's security and protection industry: Tao Junsheng, deputy director of the equipment and finance bureau of the MPS), 21 June, http://www.21csp.com.cn/jzzgaf/article.asp-ArticleID=265.htm. Accessed 2 March 2026.
Liu, Yuchen. 2021. "The art of criminal investigation in China." *China Review* **21**, 21–54.
Lu, Shenghua, and Hui Wang. 2023. "How political connections exploit loopholes in procurement institutions for government contracts: evidence from China." *Governance* **36**(4), 1205–24.
Lyon, David. 2003. *Surveillance After September 11*. Cambridge: Polity Press.
Mills, C. Wright. 2000. *The Power Elite* (New Edition). New York: Oxford University Press.
Ministry of Public Security. 2010. "Guanyu shenru kaizhan chengshi baojing yu jiankong xitong yingyong gongzuo de yijian" (Opinions on the further development of the application of urban alarm and monitoring systems), 6 April, https://www.21csp.com.cn/njcd/2012/Article/108.html. Accessed 19 September 2026.
Mozur, Paul, Jonah M. Kessel and Melissa Chan. 2019. "Made in China, exported to the world: the surveillance state." *The New York Times*, 24 April, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html. Accessed 20 October 2025.
Mozur, Paul, Muyi Xiao and John Liu. 2022. "An 'invisible cage': how China is policing the future." *The New York Times*, 25 June, https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html. Accessed 20 October 2025.
Nee, Victor, and Sonja Opper. 2012. *Capitalism from Below: Market and Institutional Change in China*. Cambridge, MA: Harvard University Press.
Ong, Lynette H., Huihua Nie and Jesslene Lee. 2026. *Outsourcing Surveillance: Online Opinion Management in China*. Cambridge: Cambridge University Press.
Pearson, Margaret M., Meg Rithmire and Kellee Tsai. 2023. *The State and Capitalism in China*. Cambridge: Cambridge University Press.
Pei, Minxin. 2024. *The Sentinel State: Surveillance and the Survival of Dictatorship in China*. Cambridge, MA: Harvard University Press.
Rolley, Chip. 2019. "Is Chinese-style surveillance coming to the West?" *The Guardian*, 7 May, https://www.theguardian.com/commentisfree/2019/may/07/chinese-style-surveillance-exported-west. Accessed 21 October 2025.
Scoggins, Suzanne E., and Kevin J. O'Brien. 2016. "China's unhappy police." *Asian Survey* **56**(2), 225–242.
Song, Wenjia, Jingxian Zhang and Tianguang Meng. 2025. "Digital corporatism: state–business dynamics of digital state capacity building in China." *Journal of Chinese Political Science* **30**(3), 323–357.
Tanner, Murray Scot, and Eric Green. 2007. "Principals and secret agents: central versus local control over policing and obstacles to 'rule of law' in China." *The China Quarterly* **191**, 644–670.
Trevaskes, Susan, and Delia Lin. 2024. "Integrating stability maintenance into comprehensive governance: the burgeoning 'safe China' behemoth." *Modern China* **50**(6), 671–701.
Wang, Dan. 2025. *Breakneck: China's Quest to Engineer the Future*. New York: W.W. Norton and Company.
Wang, Yuhua, and Carl Minzer. 2015. "The rise of the Chinese security state." *The China Quarterly* **222**, 339–359.
Wank, David L. 2001. *Commodifying Communism: Business, Trust, and Politics in a Chinese City*. New York: Cambridge University Press.
Wedeman, Andrew. 2012. *Double Paradox: Rapid Growth and Rising Corruption in China*. Ithaca, NY: Cornell University Press.
Wills, Jocelyn. 2017. *Tug of War: Surveillance Capitalism, Military Contracting, and the Rise of the Security State*. Montreal: McGill-Queen's Press.
Xu, Chenggang. 2025. *Institutional Genes: Origins of China's Institutions and Totalitarianism*. New York: Cambridge University Press.
Xu, Jianhua, and Siying He. 2022. "Can grid governance fix the party-state's broken windows? A study of stability maintenance in grassroots China." *The China Quarterly* **251**, 843–865.
Xu, Xu. 2021. "To repress or to co-opt? Authoritarian control in the age of digital surveillance." *American Journal of Political Science* **65**(2), 309–325.
Xu, Yan. 2024. "Harnessing venture capital in China." *Socio-Economic Review* **22**(1), 349–371.
Yeung, Henry Wai-chung. 2016. *Strategic Coupling: East Asian Industrial Transformation in the New Global Economy*. Ithaca, NY: Cornell University Press.
Zhang, Han. 2025. "Two-layer panopticon: how the Chinese government uses digital surveillance to prevent collective action." *Social Forces* **105**(1), 340–362.
Zhou, Li-An. 2016. "The administrative subcontract: significance, relevance and implications for intergovernmental relations in China." *Chinese Journal of Sociology* **2**(1), 34–74.

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press

Zhou, Taomo, and Cuifen Weng. 2024. "Soldiering in the special zone: the People's Liberation Army Engineering Corps in Shenzhen." *The China Quarterly* **260**, 906–924.
Zhou, Xueguang, and Hong Lian. 2020. "Modes of governance in the Chinese bureaucracy: a 'control rights' theory." *The China Journal* **84**, 51–75.

Jingyang HUANG is an assistant professor at the School of Public Policy, The Chinese University of Hong Kong, Shenzhen. He holds a PhD in social science from The Hong Kong University of Science and Technology (HKUST). His research interests span comparative political economy, political sociology and public policy, with a focus on government–business relations and state–society dynamics in the digital era. He has published articles in *The China Journal* and *Studies in Comparative and International Development*. He is currently working on a book project about the political economy of digital social control in China.

Cite this article: Jingyang Huang. 2026. "Delegating digital policing: the evolution of China's security-industrial complex." *The China Quarterly*, 1–17. https://doi.org/10.1017/S0305741026103105

https://doi.org/10.1017/S0305741026103105 Published online by Cambridge University Press