

C4ADS
innovation for peace



MONITORING THE FRONTIER

Chinese Digital Surveillance Projects in
Tibet, the Uyghur Region, Inner
Mongolia, and Hong Kong

Acknowledgments

About C4ADS

C4ADS (www.c4ads.org) is a 501(c)(3) nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide. Our approach leverages nontraditional investigative techniques and emerging analytical technologies. We recognize the value of working on the ground, capturing local knowledge, and collecting original data to inform our analysis. At the same time, we employ cutting-edge technology to manage and analyze that data. The result is an innovative analytical approach to conflict prevention and mitigation.

© C4ADS 2026

About the Author

Mishel Kondi is a Senior Analyst at C4ADS, specializing in global supply chain connections to illicit activity intersecting with the People's Republic of China (PRC). Kondi leads our work on PRC-linked activities and developments related to emerging and surveillance technologies, circumvention of export controls on advanced/AI semiconductors, and U.S. supply chain vulnerabilities. A master's candidate at Georgetown University, Kondi received a bachelor's degree in history from Middlebury College and pursued advanced coursework in Chinese at Beijing Normal University, Yunnan Normal University, National Taiwan University, and National Cheng Kung University in Taiwan.

Acknowledgments

The author would like to thank all those who provided guidance, time, and support during this project, including current and former C4ADS staff, as well as Eli Miller for the design and layout. Special thanks to Laura T. Murphy, Professor of Human Rights and Contemporary Slavery at the Helena Kennedy Centre for International Justice at Sheffield Hallam University (UK), and Conor Healy, Director of Research at IPVM.

C4ADS is also grateful to its technology partners, whose software and systems were integral to the project's success.



Legal Disclaimer

The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed to so imply.

Powered By





Table of Contents

Executive Summary4

Introduction.....6

 Contextual Note8

Methodology9

Cross-Regional Analysis10

Tibet12

 Background12

 Key Findings.....12

 Case Study14

The Uyghur Region16

 Background16

 Key Findings16

 Case Study 119

 Case Study 221

Inner Mongolia.....22

 Background22

 Key Findings.....22

 Case Study24

Hong Kong27

 Background27

 Key Findings.....27

 Case Study28

Conclusion30

Recommendations31

Appendix: Methodology Comment33

 Consolidated List of Surveillance Search Terms.....35

Executive Summary

Using an original dataset built from government and corporate records, this report maps digital surveillance supply chains across four regions governed by China: the Tibet Autonomous Region (Tibet/TAR)¹, the Xinjiang Uyghur Autonomous Region (XUAR/ the Uyghur region),² Inner Mongolia Autonomous Region (Inner Mongolia), and Hong Kong. This data offers a novel lens on China's surveillance apparatus because, unlike secondary reporting or victim testimony, government records document the state's own purchasing decisions and reveal which companies and technologies underpin its infrastructure.

Analysis limited to a single region misses the pervasiveness of China's digital surveillance architecture. While these four regions are not the only ones affected by China's repressive surveillance system, this report focuses on them due to the acute impact that surveillance has had on those populations. Tibet is often recognized as the prototype and the Uyghur region as the scale-up for China's repression of ethnic minorities and mass surveillance.³ These tools and tactics extended into Hong Kong under a nominally distinct legal system, and have also spread into Inner Mongolia, which has garnered significantly less attention.⁴

China's digital surveillance apparatus has evolved from Maoist-era grassroots social control to a high-tech infrastructure enabled by artificial intelligence (AI), consisting of high-resolution cameras, biometric data collection, and predictive policing platforms.⁵ The Chinese Communist Party's (CCP) "Five Poisons" (五毒) framework designates ethnic and religious minority populations as well as pro-democracy activists as existential threats and provides the ideological foundation for targeted surveillance in China.⁶ State-led initiatives like "Sharp Eyes" (雪亮工程) enhance the reach and scale of targeted digital surveillance. Notably, the extent of Chinese state surveillance in Inner Mongolia documented by C4ADS shows that the CCP's surveillance and repression patterns are not confined to the populations named in the Five Poisons framework. However, the Five Poisons designation still identifies the populations Beijing views as posing the greatest threat to its national security.⁷

Chinese government records show four recurring elements in the state's repressive surveillance apparatus: (1) public security bureaus (PSBs) are the primary procurers of surveillance equipment, (2) PSBs are acquiring AI-enabled biometric technology, (3) projects rely largely on domestic distributors (especially the three largest telecommunications companies), and (4) U.S.-sanctioned manufacturers such as Uniview and Hikvision remain major manufacturers of surveillance equipment supplied to China.

China's surveillance technology capacity was built by leveraging Western technology and partnerships, but a large domestic industry now exists comprising the world's largest surveillance manufacturers and exporters. This report's findings show that as domestic capacity grows, it increasingly limits the reach of sanctions and export controls that target only named foreign manufacturers,⁸ creating a need to leverage additional tools aimed at distributors and end users, discussed further in the Recommendations. However, foreign companies remain embedded in the supply chain.

Through government acquisition systems, global supply chains may still be more widely complicit in the repression of ethnic minority groups and political dissidents. Mapping these supply chains and understanding the patterns of how China continues to power its repressive surveillance apparatus is a precondition for financial, legal, and reputational accountability. Disruption requires knowing which actors to target, how they are connected, and the ways they operate. This report identifies the leading domestic suppliers of surveillance hardware named in relevant contracts across the four regions, offering an initial snapshot of the companies most central to this market. Because the U.S.-sanctioned manufacturers discussed in this report operate on a global scale, corporate due diligence and know-your-customer (KYC) standards are essential tools for preventing further complicity in state-sponsored repression.

Introduction

Digital surveillance acquisition networks across TAR,⁹ XUAR,¹⁰ Inner Mongolia, and Hong Kong exhibit commonalities that highlight critical components of China's digital surveillance architecture as well as gaps in international enforcement mechanisms intended to curtail China's targeting of ethnic, religious, and pro-democracy groups.

China's repressive state surveillance raises human rights concerns and carries direct legal and strategic implications. By enabling authorities to identify, track, and flag individuals, this surveillance infrastructure functions as a direct input into the mass detention, forced labor, and arbitrary prosecution that human rights organizations and United Nations (UN) bodies have documented across these regions. The supply chain relationships discussed in this report show People's Republic of China (PRC) public security end users accessing sensitive technologies. This exposes implicated U.S. and global companies, distributors, and investors to sanctions and export-control violations. Strategically, a documented record of how Beijing builds and sustains its digital surveillance apparatus gives U.S. policymakers an evidentiary basis for sanctions designations, export-controls, and coordinated enforcement action with like-minded governments. It also undercuts the CCP's narrative of "stability" and "harmonious" governance in these regions, a point of leverage in broader U.S.-China strategic competition.

This report adds detailed evidence of China's contemporary technology-enabled surveillance apparatus, the origins of which are rooted in the CCP's preoccupation with territorial integrity and ethnic separatism – a preoccupation that long predates the modern era. Its anxieties about border regions are rooted in decades of political and military history. Historically, the CCP maintained a surveillance and social control system through work units (单位), neighborhood committees, and informant networks.¹¹ This system was partially inherited from Soviet models and partially organized from CCP doctrine. The modern system continues to rely on a labor-intensive organizational structure; China's extensive human surveillance infrastructure is still essential to maximizing the effectiveness of its high-tech tools.¹²

C4ADS' analysis illuminates four recurring elements observed in China's surveillance-related government records: (1) public security bureaus (PSBs) are the primary procurers of surveillance equipment, (2) PSBs are acquiring AI-enabled biometric technology, (3) projects rely largely on domestic distributors (especially the three largest telecommunications companies), and (4) U.S.-sanctioned manufacturers such as Uniview and Hikvision remain major manufacturers of surveillance equipment supplied to China.

China's investment in cutting-edge technologies – including biometric data collection and other advanced surveillance tactics – intensifies threats to ethnic and religious minorities, political dissidents, and other repressed groups. U.S.-sanctioned Chinese manufacturers such as Uniview and Hikvision continue to operate on a global scale, while supplying PSBs in China through domestic distributors, activity beyond the reach of U.S. enforcement. These companies not only supply the surveillance state, they have also helped define the PRC's national and provincial surveillance standards with police forces, giving them direct influence over functions and specifications even in cases when they are not the vendor.¹³ As evidenced in this report, domestic companies now dominate China's digital surveillance supply chain; however, foreign companies continue to play a role in the supply chain and are at risk of enabling state-sponsored repression.

This investigation examines case studies from each region to highlight these phenomena. Analysis limited to a single region cannot capture the pervasive and strategic nature of the surveillance system China is building, nor can it adequately illuminate how interconnected supply chains underpin surveillance efforts and feed them with new technologies. This report addresses that gap by mapping the shared structures, common procurement patterns, and replicated technologies that have enabled surveillance across these regions. While the CCP's repressive surveillance tactics extend beyond the regions covered by this report, those regions face surveillance that differs in intensity and type, with ethnic minority groups and political dissidents in Tibet, the Uyghur region, Inner Mongolia, and Hong Kong experiencing heightened repression.

Contextual Note



After the 1989 Tiananmen Square protests and massacre, the CCP prioritized public security investments to prevent ideological cracks from widening and creating a domino effect of disobedience and protest. Post-1989, the party focused on monitoring activists, journalists, and intellectuals across the entire country. However, while the CCP viewed any dissent as posing a risk, individuals of specific ethnic and religious backgrounds were regarded as belonging to a higher-risk category. This distinction was formalized in the 1990s and 2000s, when the CCP codified a label that had been used for decades: the “Five Poisons” (五毒). According to the CCP, the Five Poisons represent Tibetan independence activists, Uyghur independence activists (referred to as separatists), Taiwan independence advocates, Falun Gong practitioners, and pro-democracy activists.¹⁴

The Five Poisons framework underpins China’s surveillance priorities, domestically and abroad. Surveillance of groups that fall within the Five Poisons framework has been used as the basis for targeting ethnic minorities in Tibet, the Uyghur region, Inner Mongolia, and Hong Kong, including mass detention, torture and abuse in custody, forced labor, reproductive coercion, and cultural erasure.¹⁵

The advent of the internet in the mid-1990s led the CCP to develop the “Great Firewall,” a nationwide system of internet filtering and censorship.¹⁶ Subsequently, the CCP pivoted to leverage the internet and other technological innovations as part of modernized surveillance and monitoring mechanisms that have been institutionalized according to various state-led initiatives. The “Sharp Eyes” project (雪亮工程), for example, is a government surveillance program designed to achieve comprehensive coverage of public spaces, with a focus on rural communities.¹⁷ China’s central government named the Sharp Eyes project as part of its strategy for “constructing peaceful rural communities” (建设平安乡村) in a policy directive that also emphasizes combating “illegal religious activities and foreign infiltration.”¹⁸ In practice, Sharp Eyes cameras and household sensor networks feed real-time footage and movement data directly to local PSBs, extending state monitoring into rural homes and community life rather than merely deterring petty crime.¹⁹ The CCP’s implementation of advanced technology for state-led surveillance initiatives, such as the integration of biometric data collection and AI-enabled tools, is accelerating.²⁰

Methodology

This report is based on analysis of TAR, XUAR, Inner Mongolia, and Hong Kong government records, as well as Chinese and Hong Kong corporate records. Government records offer a novel lens on China's surveillance apparatus because, unlike secondary public reporting or victim testimony, they document the state's purchasing decisions and reveal which companies and technologies underpin its surveillance infrastructure.

C4ADS curated a list of 165 Chinese-language terms that were used as filters to identify Chinese digital surveillance contracts within the government records. In addition to the 165 baseline terms, C4ADS also gathered terms that are directly related to digital surveillance practices in specific regions (e.g., "pastoral area" for Inner Mongolia contracts). These terms were chosen based on their relevance to China's digital surveillance apparatus and related monitoring policies and initiatives (e.g., "Sharp Eyes"). C4ADS reviewed government documents for these keywords and flagged records containing two or more terms affiliated with digital surveillance, on the basis that a single term may appear in non-surveillance contexts, while a co-occurrence of two or more terms increases the likelihood that a contract was specifically oriented toward digital surveillance infrastructure. Case studies were chosen to illustrate patterns we had already identified in the data, and were further narrowed to those meeting two criteria: at least two keywords present in the contract, and involvement of a government actor, sanctioned entity, or foreign company. These terms were run through the Hong Kong records in English, as the Hong Kong source data is in English. Additionally, top suppliers in each region are ranked by the number of flagged contracts in which the supplier appears, as opposed to contract value.

This research has several limitations. Some of the most sensitive business contracts may not be publicized on Chinese government websites and therefore may not be publicly available. The records used for this analysis were collected in multiple formats and do not represent all relevant Chinese databases. Data availability and coverage vary substantially across regional datasets. C4ADS' holdings of XUAR and Inner Mongolia records date back to 2013, TAR to 2019, and Hong Kong records only to 2019. This variation reflects data collection priorities and different levels of censorship and publication restrictions, not necessarily differences in actual activity. Cross-regional comparisons should therefore be treated as indicative rather than definitive, a caveat that applies to all the comparisons drawn in the cross-regional analysis section below.

Cross-Regional Analysis

This analysis illuminates four recurring elements observed in China's surveillance-related government records: (1) PSBs are the primary procurers of surveillance equipment, (2) PSBs are acquiring AI-enabled biometric technology, (3) projects rely largely on domestic distributors (especially the three largest telecommunications companies), and (4) U.S.-sanctioned manufacturers such as Uniview and Hikvision remain major manufacturers of surveillance equipment supplied to China.

China's Ministry of Public Security (MPS) is the primary police and internal security apparatus responsible for law enforcement and social order. Beyond this domestic mandate, MPS also runs a significant transnational repression apparatus abroad, including overseas police stations and fugitive-recovery campaigns like Fox Hunt and Skynet. While foreign intelligence and influence operations are more properly associated with the Ministry of State Security (MSS) and the Party's United Front Work Department (UFWD), the lines between these institutions are not always sharp, with the MPS itself retaining some intelligence and influence functions. MPS has localized offices via local-level PSBs throughout China. MPS has been implicated in numerous human rights abuses, including mass surveillance, arbitrary detention, torture, and the suppression of groups belonging to the Five Poisons.²¹ PSBs are charged with law enforcement, fire prevention, traffic control, immigration control and registration and other matters affecting public security, and are under the national-level authority of the MPS. While it is unsurprising that they are the primary procurers of surveillance equipment, this finding provides concrete evidence for that dynamic. The fact that the types of surveillance technology procured vary from region to region suggests that while some coordination may occur, each region is pursuing its own surveillance needs relatively independently.

Despite this variation, C4ADS identified notable patterns. PSBs across the four selected regions are acquiring biometric data collection technologies. In Tibet, this takes shape via a dedicated DNA database construction contract; in Hong Kong, it appears in the form of palmprint, fingerprint, and Live Scan identification systems. In the Uyghur region and Inner Mongolia, it is embedded within broader video-surveillance contracts that include biometric sample collection. While China is not alone in adopting biometric procurement as part of national monitoring and policing, China's history of using surveillance as the basis for systematic targeting of ethnic minority populations makes China's acquisition of these technologies particularly concerning. For instance, China previously established automated ethnicity-detection built into camera systems that specifically identify and flag Uyghur individuals and other ethnic groups. Against that record, China's modernization of its policing system raises red flags about expanded population control and human rights abuses.²²

The projects analyzed for this report also highlight that the projects in Tibet, the Uyghur region, Inner Mongolia, and Hong Kong are predominantly supplied by domestic entities. This is significant and indicates that international actors interested in curbing China's human rights abuses against minority populations will have to consider new ways to curtail the growth of China's surveillance state, in addition to preventing China from procuring foreign equipment. Chinese telecommunications companies – China Mobile, China Telecom, and China Unicom – are key and repeat suppliers of surveillance-related projects across Tibet, the Uyghur region, and Inner Mongolia. In these frontier and ethnic minority provinces, Chinese telecom companies have been

consistently present as suppliers on surveillance-related contracts in nearly every year since 2020, though the number of such contracts has varied considerably from year to year. Hong Kong data reveals different concerns. There were fewer surveillance-related projects in general, and C4ADS did not identify telecommunication companies as playing the same prominent role.

While the role of Chinese companies is significant, foreign companies are not free from complicity, as seen in the Hong Kong case study. These findings demonstrate that the PRC's surveillance technology market is dominated by a diversified domestic industry – yet foreign companies continue to supply China with products that support the CCP's repressive surveillance practices. Much of this domestic capacity was originally built through early-stage adaptation of foreign technology, and dual-use components remain part of the supply chain today; restricting China's access to dual-use foreign technology remains a necessary complement to sanctioning individual surveillance companies. At the same time, sanctions and export controls that target a small number of already-blacklisted foreign manufacturers may miss a considerable component of this activity; disrupting it will likely require tools aimed at end users and end uses, such as procurement-side due diligence and distributor-level designations. As China's domestic industry continues to mature, policymakers should begin considering what additional tools will be needed in the future if China's surveillance industry no longer depends on foreign inputs.



Background

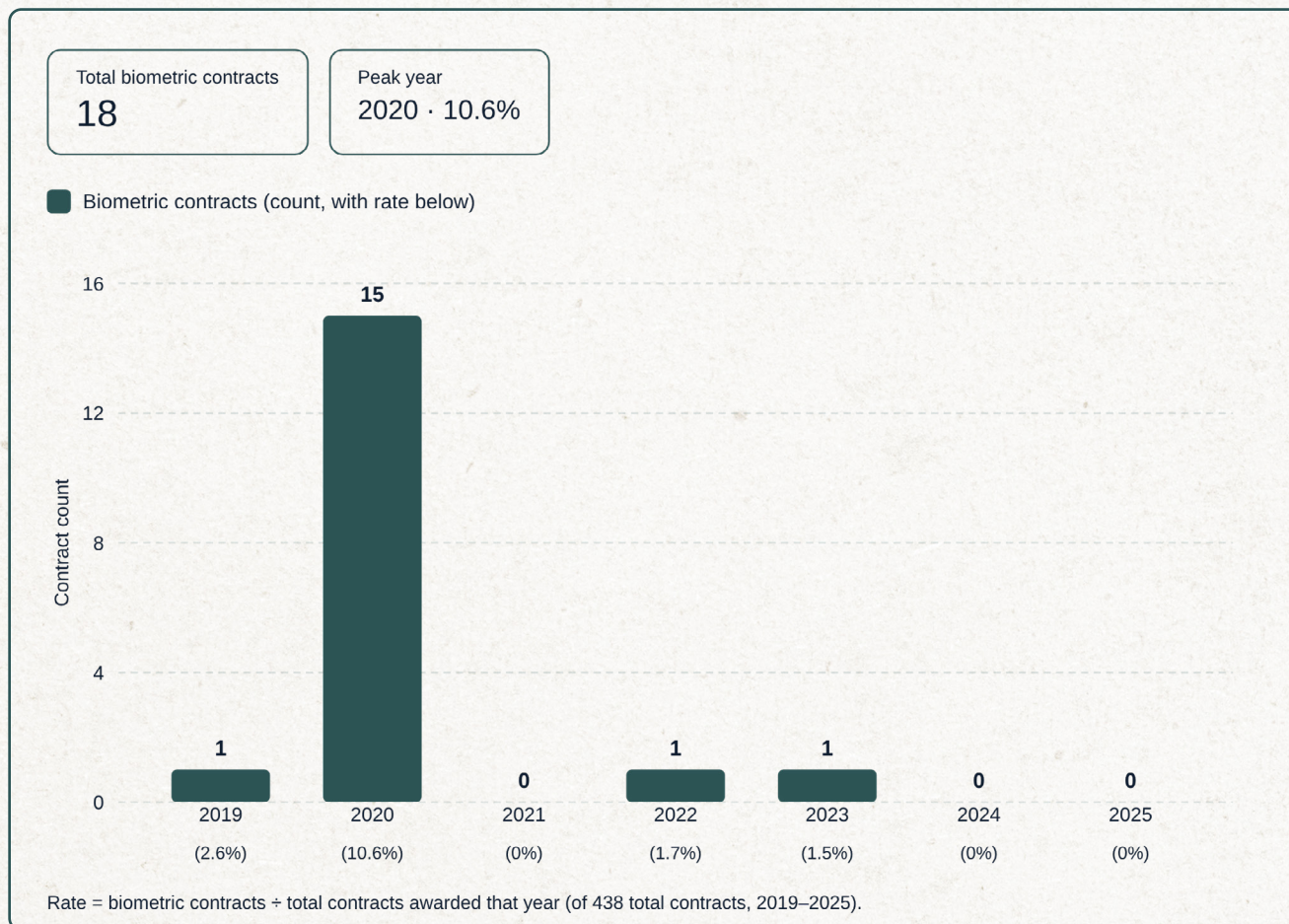
The CCP has used Tibet as a foundational laboratory for its surveillance apparatus, with the methods developed there later exported to the Uyghur region and beyond.²³ Following the CCP's military occupation of Tibet in 1950, much of which was later organized into the Tibetan Autonomous Region (TAR) and other Tibetan autonomous prefectures, control there evolved from a conventional military presence into a sophisticated system of high-tech repression.²⁴ During Party Secretary Chen Quanguo's tenure (2011–2016), there was significant escalation of surveillance and monitoring. He introduced a “grid management” system dividing urban areas into surveillance cells, establishing over 600 high-tech “convenience police stations” throughout Tibet and deploying “Red Armband Patrol” volunteer security units to monitor daily life.²⁵ These measures were complemented by mandatory DNA collection, biometric data gathering, Wi-Fi network monitoring, and the deployment of closed-circuit television (CCTV) networks with facial recognition technology across Lhasa and other population centers.²⁶ The International Campaign for Tibet has noted that security spending in Tibet has been among the highest per capita of any Chinese province or region, reflecting the CCP's prioritization of Tibetan suppression.²⁷ Critically, when Chen Quanguo was transferred to serve as CCP Party Secretary of Xinjiang in 2016, he replicated and amplified this blueprint at scale, underscoring Tibet's role not merely as a target of repression but also as the testing ground where China's infrastructure of surveillance was first systematically refined.²⁸

Researchers and Tibetan advocates say that the human consequence of such a system has been a “complete breakdown” in ordinary digital contact. People self-censor in calls and messages, avoid discussing sensitive topics even with family in diaspora communities, and describe a persistent fear of being flagged as “politically unreliable,” which can lead to detention.²⁹ Human Rights Watch has framed this as part of a deliberate effort to build a “totalitarian social control state” in which surveillance systems help sort and vet the population, with those deemed unreliable funneled into reeducation programs or prison.³⁰

Key Findings

C4ADS collected 41,729 contracts of TAR government data with date coverage from July 2019 to June 2025. The top surveillance-related keywords found in TAR contracts were: “peace and security” (安保, 586 contracts), “social credit” (社会信用, 425 contracts), “prevention and control” (防控, 369 contracts), “urban management” (城市管理, 334 contracts), and “surveillance” (监控, 291 contracts). The analysis identified 438 TAR contracts that contain two or more surveillance keywords. Of the 438 contracts, 18 contain at least one biometric data collection technology term. Of the 18 biometric contracts, 15 were published in 2020, suggesting an increased policy focus on biometric data collection. None of the 18 contracts took place in 2024 or 2025. This may suggest increased self-censorship of publicly available TAR contracts involving biometrics in recent years – as in, the government may be procuring at the same or a higher rate as in the past, but is no longer making that information publicly available – or that the significant investment that took place in 2020 may have already established the main infrastructure for China's biometric needs in TAR.

Figure 1. Rate of biometric contracts across 438 flagged records, showing a spike in 2020.³¹



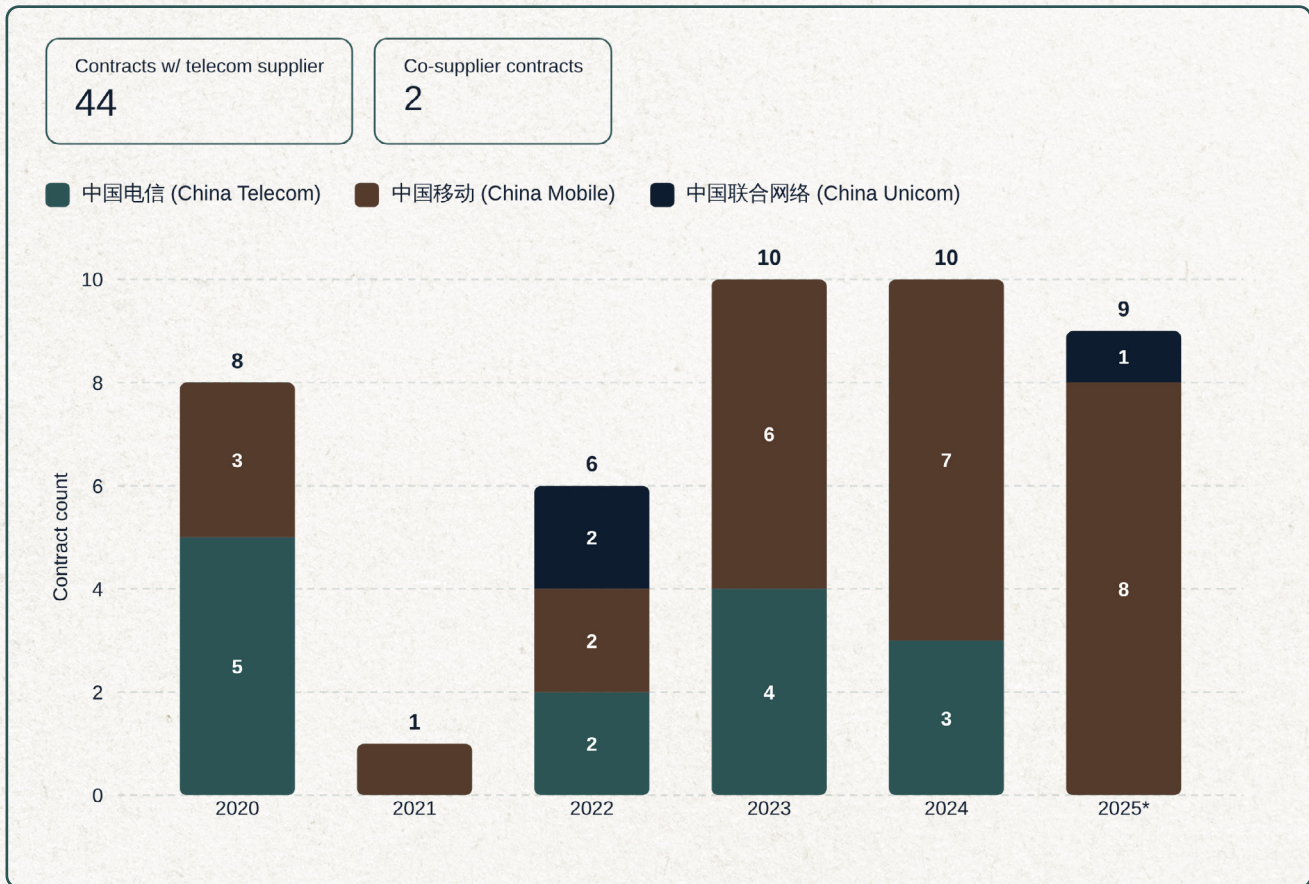
The top suppliers on these 438 flagged contracts are:

1. China Mobile Group Tibet Co., Ltd. (中国移动通信集团西藏有限公司, 25 contracts)
2. China Telecom Digital Intelligence Technology Co., Ltd. (中电信数智科技有限公司, 24 contracts, merged with former name 中国电信集团系统集成有限责任公司)
3. China Mobile System Integration Co., Ltd. (中移系统集成有限公司, 13 contracts)
4. Tibet Xi'an Information Technology Co., Ltd. (西藏熙安信息技术有限公司, four contracts, formerly 西藏熙安信息技术有限责任公司)
5. China Unicom Digital Technology Co., Ltd. (联通数字科技有限公司, four contracts)
6. Tibet Yuanrui Network Technology Co., Ltd. (西藏缘瑞网络科技有限公司, four contracts)

Of the 438 contracts, 42 contracts involve one of China's three largest state-owned telecommunications companies: China Unicom, China Telecom, or China Mobile as a direct supplier.

According to the data, China Mobile is listed as the direct supplier for the majority of these flagged telecommunication contracts. As the bar graph below also demonstrates, Chinese telecommunication companies have been consistently present as suppliers on surveillance-related TAR contracts in nearly every year since 2020,³² though the number of such contracts has varied considerably year to year.

Figure 2: Number of Surveillance Contracts in TAR Held by Three Major Chinese Telecommunications Companies (2020-2025)³³

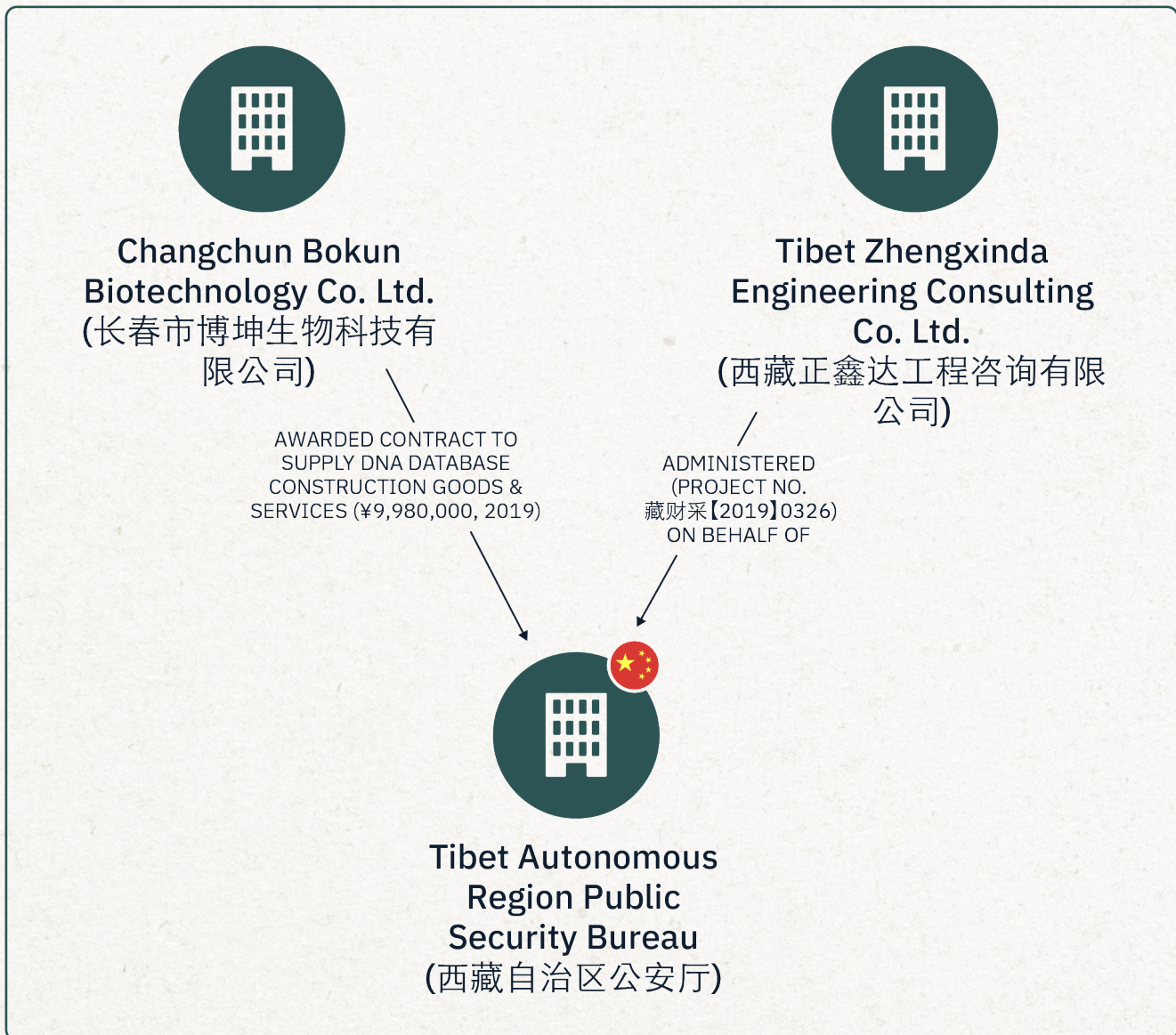


Case Study

The case study of Changchun Bokun Biotechnology Co., Ltd. (长春市博坤生物科技有限公司, hereafter Changchun Bokun) demonstrates two of the recurring elements identified through government contracts in the region: public security bureaus (PSBs) as a major actor through which surveillance contracts are executed and the heavy investment of PSBs in biometric data collection projects. This case also represents a direct, population-scale DNA database acquisition rather than an incidental biometric feature of a larger contract.³⁴ This contract was selected for containing three surveillance-related keywords: “stability maintenance,” “social governance,” and “DNA.”

In 2019, Changchun Bokun won a bid to supply the Tibet Autonomous Region Public Security Bureau (西藏自治区公安厅, hereafter TAR PSB) with goods and services for a DNA database construction project (DNA数据库建设). The contract, assigned project number 藏财采 (2019) 0326 and announced on July 30, 2019, carries a total value of US\$1,487,000 (¥9,980,000). The procurement was administered by Tibet Zhengxinda Engineering Consulting Co., Ltd. (西藏正鑫达工程咨询有限公司, hereafter Tibet Zhengxinda), a Lhasa-based agency acting on behalf of the Tibet Public Security Bureau.

Figure 3: Supplier and procurement agent for the TAR Public Security Bureau's 2019 DNA database contract³⁵



This contract is notable in the context of broader Chinese government efforts to construct compulsory population-wide DNA databases in ethnic minority regions. Researchers and human rights organizations have documented that PSBs across Tibet and the Uyghur region have conducted mandatory DNA collection campaigns targeting residents, including children, with no requirement of criminal suspicion, as part of what authorities frame as “social governance” and “stability maintenance” (维稳) infrastructure.³⁶ The TAR PSB’s contracting of a dedicated DNA database sample testing project valued at nearly ¥10-million in 2019 is consistent with this documented pattern of biometric data infrastructure investment in minority regions. Changchun Bokun’s role as the sole awarded vendor for the full scope of sample testing services indicates it may serve as a foundation for building and populating the database.



The Uyghur Region



Background

Mass surveillance in the Uyghur region has developed into one of the most extensive systems of population control in the world.³⁷ As early as 2014, the CCP installed thousands of high-definition cameras throughout the region, in villages, mosques, and at critical intersections, connected to centralized command facilities.³⁸ Between 2016 and 2018, city administrations spent up to US\$1 billion expanding high-tech surveillance infrastructure, including the installation of facial recognition technology across nearly 1,000 mosques in a single county.³⁹ By 2018, the U.S. Department of State characterized the region as having “unprecedented levels of surveillance.”⁴⁰ The pervasiveness of these measures, which encompass CCTV networks, artificial intelligence, facial recognition, biometric data collection, and cell phone monitoring, has been documented by many civil society organizations, governments, UN officials, and individuals.⁴¹

Mass surveillance in the Uyghur region has transformed it into what has often been described as a “virtual cage” and an “open air prison,” with the surveillance systems built with functionalities specifically designed to flag Uyghurs and other Turkic Muslims for arbitrary detention.⁴² The mass detention reflects a systemic approach and exposes people to sexual violence, torture, forced sterilization, forced organ harvesting, other killings, and forced labor, with evidence that some detainees have died as a result of their treatment in the camps.⁴³ In effect, the surveillance apparatus does not merely monitor the population, but functions as the operational trigger that prompts the state to physically target Uyghurs and other groups identified as threats by the PRC.

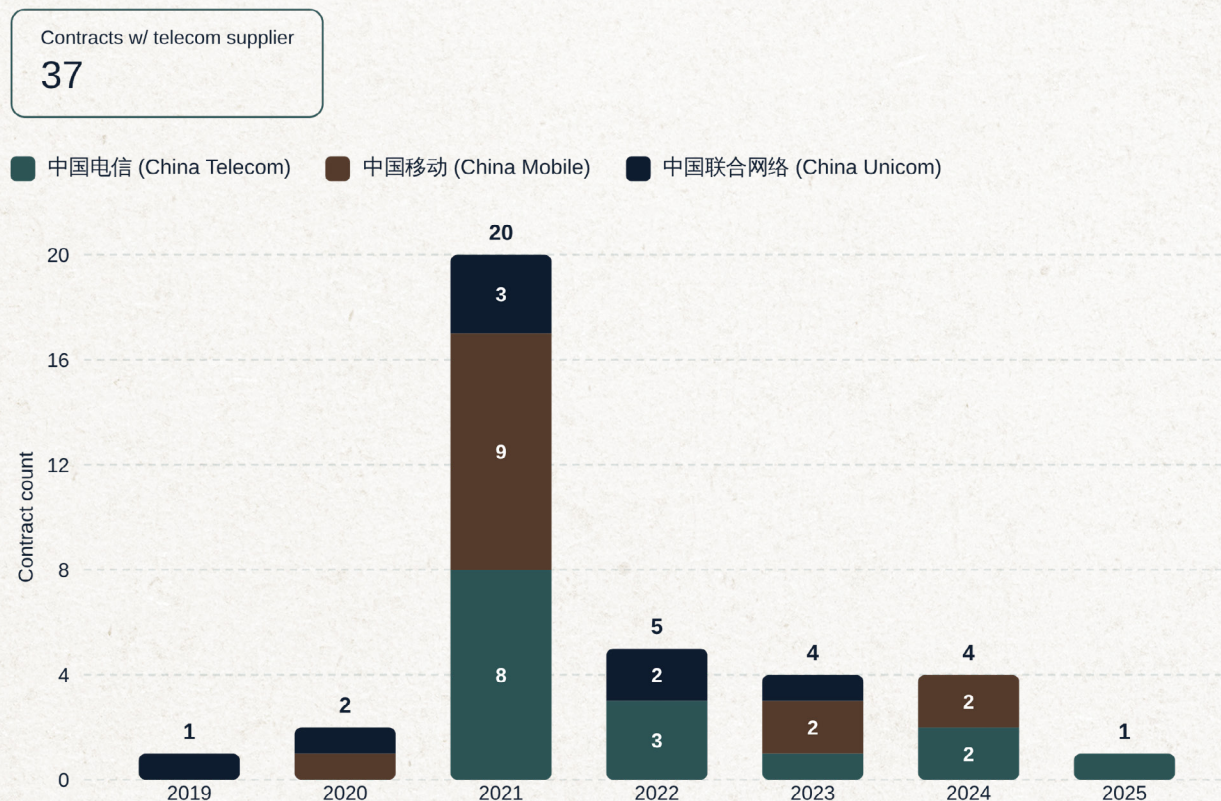
Key Findings

For the Uyghur region, C4ADS had to separately analyze records from the regional government (“XUAR dataset”), as well as the Xinjiang Production and Construction Corps (“XPCC dataset”) – a distinct governing body in the region with its own records system. XPCC is a paramilitary organization that operates as a quasi-state entity and controls significant portions of the region’s economy. C4ADS analyzed 112,077 rows of XUAR government data, spanning a date range from September 2020 to April 2025. Within this dataset, the top surveillance-related keywords appearing across XUAR contracts were: “prevention and control” (防控, 1,841 contracts), “surveillance” (监控, 708 contracts), “peace and security” (安保, 518 contracts), “comprehensive management” (综合治理, 470 contracts), and “network security” (网络安全, 314 contracts). C4ADS also analyzed 21,572 rows of XPCC data, spanning a date range from June 2022 to April 2025. Within this dataset, the top surveillance-related keywords appearing across XPCC contracts were: “surveillance” (监控, 409 contracts), “prevention and control” (防控, 292 contracts), “peace and security” (安保, 246 contracts), “early warning” (预警, 183 contracts), and “network security” (网络安全, 140 contracts).

In the XUAR dataset, C4ADS flagged 368 contracts containing two or more of these keywords. Public security bureaus (公安局) appear as the listed buyer in 55 of these flagged contracts. The top suppliers among the 368 flagged contracts are:

1. Xinjiang Zhixiang Technology Co., Ltd. (新疆智翔科技有限公司, 14 contracts)
2. China Mobile Communications Group Xinjiang Company Limited Urumqi Branch (中国移动通信集团新疆有限公司乌鲁木齐市分公司, 10 contracts)
3. CCS Public Information Industry Co., Ltd. (中通服公众信息产业股份有限公司, seven contracts)
4. China Telecom Urumqi Branch (中国电信股份有限公司乌鲁木齐分公司, six contracts)
5. Xinjiang Dachen News Co., LTD (新疆大晨报股份公司, six contracts)

Figure 4: Date distribution of the 38 XUAR contracts with a telecom supplier⁴⁴



Of 38 contracts with a telecom company as direct supplier, 1 is excluded above for lacking date information.

In the XPCC data, C4ADS found 305 contracts meeting the same two-keyword threshold; PSBs are the listed buyer in 60 of them. The top suppliers among these 305 contracts are:

1. Tower Zhilian Technology Co., LTD (铁塔智联技术有限公司, 21 contracts)
2. Neusoft Corporation (东软集团股份有限公司, 19 contracts)
3. China Mobile Communications Group Xinjiang Company Limited Urumqi Branch (中国移动通信集团新疆有限公司乌鲁木齐市分公司, eight contracts)
4. XPCC Communications Technology Center Company Limited (新疆生产建设兵团通信科技中心有限公司, six contracts)
5. China Telecom Digital Intelligence Technology Co., Ltd. (中电信数智科技有限公司, five contracts)

As with TAR contracts, large telecommunications companies were often suppliers of surveillance-related equipment.⁴⁵ Thirty-eight of the 368 flagged contracts in the XUAR data list one of China's three largest telecommunications companies – China Mobile, China Unicom, or China Telecom – or one of their subsidiaries, as a direct supplier. This category saw a significant spike in 2021, with China Telecom and China Mobile tied at 15 contracts each across the XUAR dataset. In terms of telecommunications-related contracts in the XPCC dataset, 35 of the 305 contracts were directly supplied by one of China's three largest telecommunications companies – China Mobile, China Unicom, or China Telecom – or one of their subsidiaries.

Looking more closely at the XUAR and XPCC records to identify the presence of biometric technologies, C4ADS found 135 contracts containing at least one mention of a biometric data collection technology term drawn from the biometric term subset.

Government records from XUAR and the XPCC also reflect the involvement of U.S.-sanctioned companies in digital surveillance contracts with public security agencies, a phenomenon similarly found in Inner Mongolia records. No XUAR contracts list Zhejiang Uniview Technologies Co., Ltd. (浙江宇视科技有限公司, hereafter Uniview), a U.S.-sanctioned surveillance equipment manufacturer, or its wholly-owned subsidiaries as a direct supplier. However, Uniview is mentioned in other capacities, such as product-level specifics, in 54 XUAR contracts related to surveillance collected for this analysis, which suggests that Uniview products are maintained or provisioned via third parties in XUAR for projects that overtly mention surveillance. Domestic distributors, their subsidiaries, and other intermediaries can obscure the role of U.S.-sanctioned companies in these supply chains. Of the 54 contracts that mention Uniview (浙江宇视), four involve public security bureaus (公安局), and five mention the XPCC (兵团), indicating that Uniview products are operationalized for public security and XPCC projects in the region.

Uniview was added to the U.S. Department of Commerce's Bureau of Industry and Security (BIS) Entity List in 2024 because "it develops and sells products and services that enable China's public security establishment to carry out human rights violations."⁴⁶ Uniview maintains global operations through its 21 branches in Japan, South Korea, Australia, the United Kingdom, France, the Netherlands, and the United States.⁴⁷

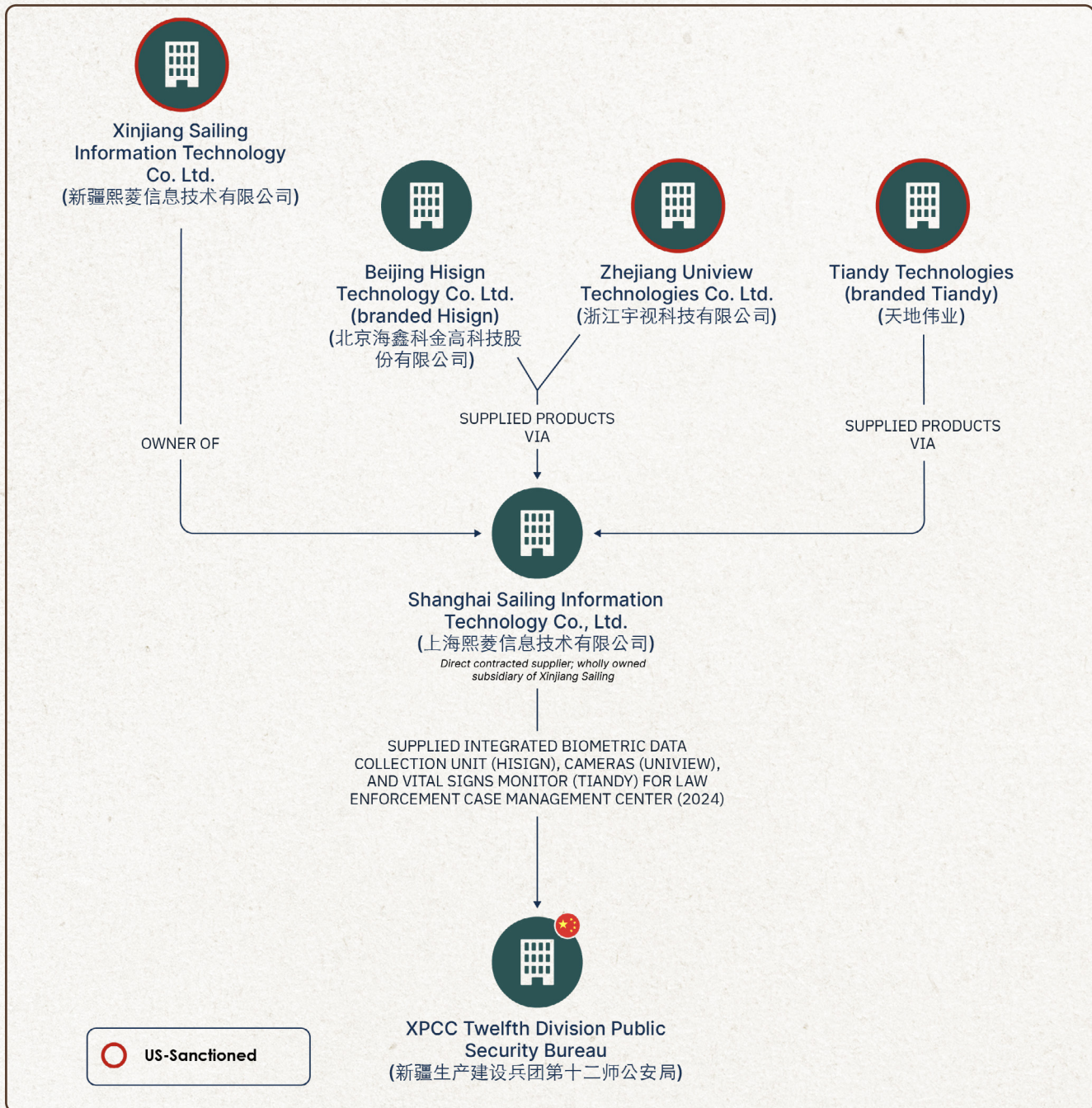
C4ADS more deeply examined two PSB contracts that demonstrate different aspects of China's growing surveillance capabilities. The first case study demonstrates three of the four recurring elements identified in the contracts: the role of a PSB as the party acquiring surveillance technology; equipment

provided through the contract was manufactured by a U.S. Office of Foreign Assets Control (OFAC) designated entity but not directly supplied by this sanctioned entity; and the contract has a biometric component. This first contract contains four surveillance-related keywords: “biometrics,”⁴⁸ “visualization” (可视化), “video surveillance” (监控), and “big data” (大数据). The second case study discussed below involves a PSB purchasing AI technologies for predictive policing purposes from a leading Chinese software development company. The contract included two keywords: “visualization” (可视化) and “big data” (大数据).⁴⁹

Case Study 1

In 2024, the XPCC Twelfth Division Public Security Bureau (新疆生产建设兵团第十二师公安局, hereafter the XPCC 12th Division PSB) contracted Shanghai Sailing Information Technology (上海熙菱信息技术有限公司, hereafter Shanghai Sailing) to equip a law enforcement case management center with a total contract value of US\$158,700 (¥1,065,000). Shanghai Sailing is 100% owned by a U.S. Department of Commerce BIS-listed entity, Xinjiang Sailing Information Technology Co., LTD (新疆熙菱信息技术有限公司).⁵⁰ Shanghai Sailing supplied the XPCC 12th Division PSB with an integrated biometric data collection unit (branded Hisign 海鑫科金) and Uniview cameras, which integrate deep learning algorithms. Shanghai Sailing also equipped the case management center with video data and visualization servers, a storage system, a fully equipped interrogation room with cameras and audio equipment, a biometric sample collection machine (branded Hisign 海鑫科金), footprint capture devices, and a vital signs monitor (branded Tiandy weiye 天地伟业).

Both Tiandy and Uniview are sanctioned in the United States due to their involvement in human rights violations, high-tech surveillance, and mass arbitrary detention of Uyghurs and other ethnic minorities in the PRC.⁵¹ The manufacturer of the branded equipment used in this project, Hisign 海鑫科金, does not face any restrictions.

Figure 5: Supply relationships in a 2024 XPCC Twelfth Division Public Security Bureau biometric procurement⁵²

Beijing Hisign Technology Co., Ltd. (北京海鑫科金高科技股份有限公司), the manufacturer of Hisign products, is a state-owned high-tech company focused on AI biometric recognition tools, including fingerprint, palmprint, facial, iris, footprint, voiceprint, DNA recognition machines, and big data tech.⁵³ The company supplies PSBs throughout the PRC, including three of the regions with a documented history of human rights abuses discussed in this report, the Uyghur region, Inner Mongolia, and Hong Kong. According to publicly available information, this company does not seem to have active or recent projects in TAR. The services Hisign provides include digital and data forensics, biological and laboratory forensics, investigation and identification systems, audio forensics, and field and mobile

data collection.⁵⁴ According to a report by the Australian Strategic Policy Institute focusing on China's pioneering of more sophisticated genomic surveillance, the company has also boasted about its ability to connect with the "DNA national library," and "provide intelligent family tree mapping."⁵⁵

Finally, Beijing Hisign holds overseas investments in the United States, Germany, Singapore, the Netherlands, and Canada, and it remains unsanctioned.⁵⁶ These jurisdictions overlap with several of the markets where this report's recommended enhanced KYC and due-diligence standards would apply. Regulators and companies in these jurisdictions should more closely scrutinize Hisign's operations. Hisign itself is not designated by BIS, despite manufacturing the biometric collection equipment supplied directly to the XPCC 12th Division PSB alongside sanctioned Uniview and Tiandy hardware in this same contract.

Case Study 2

In 2023, the Eighth Division Public Security Bureau (第八师公安局) contracted Beijing Xinyu Industrial Technology Co., Ltd. (北京鑫宇兴业科技有限公司; hereafter Beijing Xinyu) to supply a "big data visualization cognitive analysis system" (大数据可视化认知分析系统) for an internal unnamed PSB unit referred to as "A unit" ("某单位"). According to WireScreen, "A unit" is a Chinese government designation generally used for military or intelligence agencies.⁵⁷ The contract is worth US\$47,400 (¥318,200). Line item details explicitly refer to "智器云" (Zhiqiyun or Zhiqi Cloud)-branded software, specifying "Huoyanjinjing AI Visualization Analysis Software V2.0."⁵⁸

Past research into predictive policing in the Uyghur region has shown that these systems work by ingesting disparate data streams, including checkpoint logs, financial records, communications data, and travel data to identify patterns and flag behaviors that stray from those patterns.⁵⁹ According to its publications, Zhiqi Cloud markets Huoyanjinjing for structurally identical work to past predictive policing systems in the Uyghur region. The company describes itself as a leader in "law enforcement investigations and intelligence analysis" (执法调查和情报分析). Its product materials describe the software's core function as importing heterogeneous data of any type, auto-generating relationship graphs and timelines, and applying nearly "a hundred built-in analysis models" for one-click case analysis.⁶⁰ According to an article published by a Beijing Public Security Bureau-affiliated website, Zhiqi Cloud has over 10,000 users within PSBs and law enforcement bodies, covering 99% of prefecture-level cities, including Hong Kong and Macau.⁶¹

While the supplier, Beijing Xinyu, is not directly sanctioned by OFAC, according to WireScreen, it is a direct supplier to a number of entities sanctioned by the United States and Canada, and restricted by Japan.⁶² The company is a direct supplier to companies that are on Canada's National Research Organizations List (which includes entities that pose a risk to Canada's national security), and on the U.S. Department of Commerce's Entity List, namely Beihang University and Harbin Institute of Technology.⁶³



Inner Mongolia



Background

Although not as well documented as those in the Uyghur region and Tibet, human rights abuses in Inner Mongolia are a growing concern.⁶⁴ According to a 2026 PEN America report, Mongolians comprise 20% of Inner Mongolia's population, and yet their language, culture, and digital spaces have faced sustained repression by Chinese authorities.⁶⁵ The aforementioned PEN America report found that 89% of known Mongolian cultural websites have been censored or banned, which shows how the Chinese government has weaponized digital monitoring against ethnic minorities in the region.⁶⁶ In addition to censorship and the shutdown of Mongolian digital platforms, Chinese authorities have used surveillance as the basis for mass detention, reeducation campaigns, removal of bilingual education, online harassment, state-sponsored migration, and coerced statements.⁶⁷ According to the Minority Rights Group, Mongol communities have also been forcibly removed from pastoral areas by Chinese authorities, constituting a major threat to their culture and livelihood.⁶⁸ Data from Inner Mongolia's government publications demonstrates the significant scale at which public security agencies in the region are acquiring digital surveillance technology for state-led surveillance initiatives like the Sharp Eyes project and provide insights into the main organizations involved in supplying this technology.⁶⁹

Key Findings

C4ADS collected 165,940 contracts of Inner Mongolia government data, with date coverage spanning from December 2013 to January 2026. Within this dataset, the most prevalent surveillance-related keywords identified in the contracts were: “prevention and control” (防控), appearing in 2,165 contracts; “urban management” (城市管理), appearing in 1,595 contracts; “surveillance” (监控), appearing in 1,345 contracts; “pastoral area” (牧区), appearing in 700 contracts; and “big data” (大数据), appearing in 602 contracts. By cross-referencing these terms, C4ADS identified 692 Inner Mongolia contracts containing two or more of these keywords. Among these 692 flagged contracts, public security bureaus (公安局) were listed as the buyer in 67 instances. Twenty-three flagged contracts mention Sharp Eyes (雪亮工程), further showing that a significant number of Inner Mongolia contracts are in service of state-led surveillance projects.

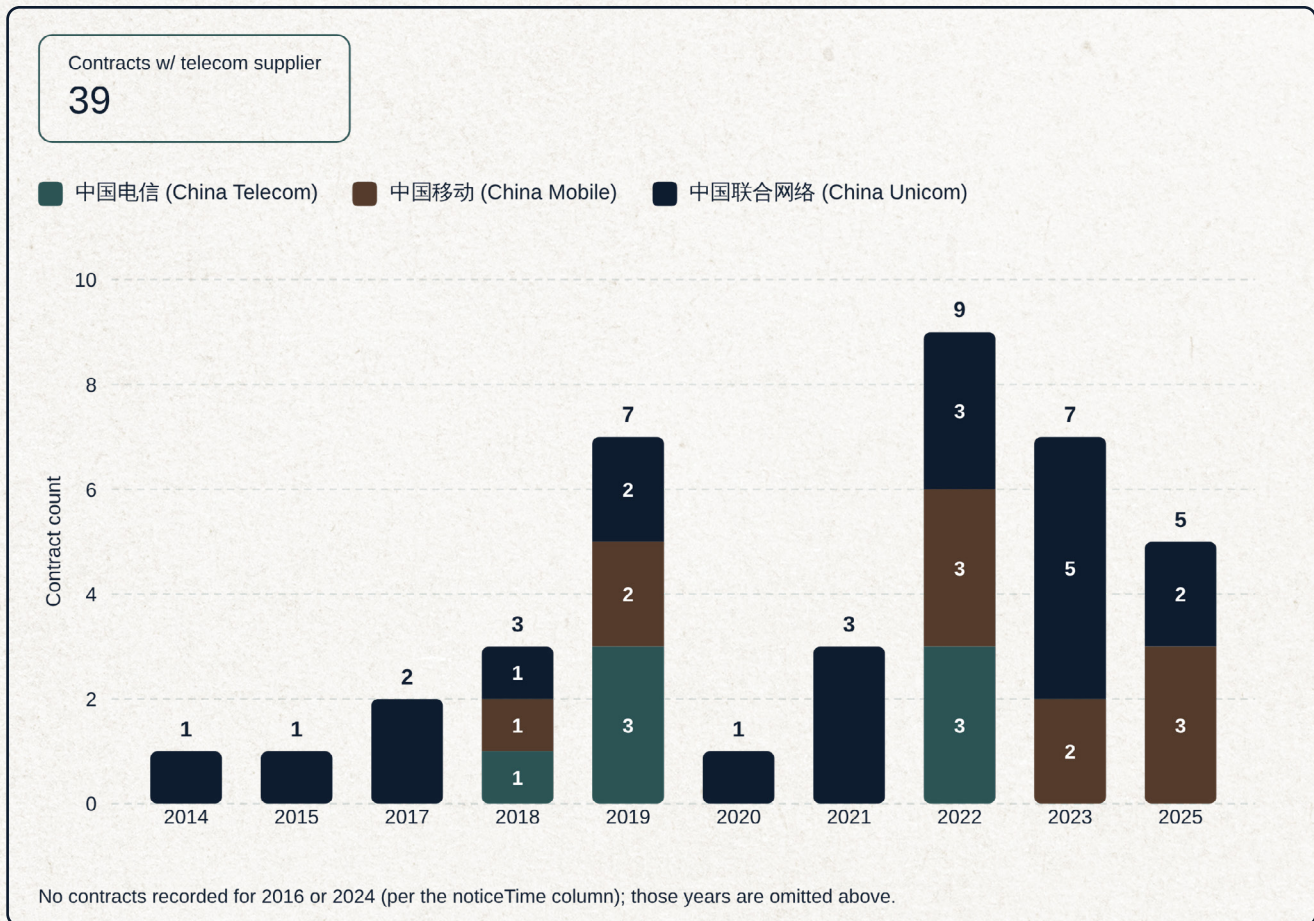
The suppliers most frequently associated with these flagged contracts are:

1. Xinyuan Network Technology Co., Ltd. (信元网络技术股份有限公司, seven contracts)
2. China Unicom Co., Ltd. Ordos Branch (中国联通网络通信有限公司鄂尔多斯市分公司, seven contracts)
3. Inner Mongolia Mintong Electronic Engineering Supervision Consulting Co., Ltd. (内蒙古敏通电子工程监理咨询有限公司, seven contracts)
4. Unicom Digital Technology Company Limited Inner Mongolia Branch (联通数字科技有限公司内蒙古自治区分公司, seven contracts)
5. Inner Mongolia Zili Technology Co., Ltd. (内蒙古自立科技有限责任公司, six contracts)

Considering specifically biometric-related purchases, 213 contracts in the Inner Mongolia dataset contained at least one mention of a biometric data collection technology term drawn from the relevant subset of biometric terms.

Analyzing the involvement of telecommunications companies, C4ADS found that 39 of the 692 flagged contracts listed one of China's three largest telecommunications companies, China Mobile, China Unicom, or China Telecom, or one of their subsidiaries as a direct supplier. Among the "big three," China Unicom and its subsidiaries stood out as the most common direct suppliers across these flagged surveillance-related contracts, appearing as the listed supplier on 21 of them.

As was the case for the XUAR records, Inner Mongolia government records reflect the obscured involvement of U.S.-sanctioned companies in digital surveillance contracts with public security agencies. Hangzhou Hikvision Digital Technology Co. Ltd. (杭州海康威视数字技术股份有限公司, hereafter Hikvision), a U.S.-sanctioned surveillance equipment manufacturer, is mentioned in 1,094 of the Inner Mongolia contracts collected for this analysis. Only seven Inner Mongolia contracts list Hikvision or its wholly-owned subsidiaries as a direct supplier, which may suggest that Hikvision products are maintained or provisioned via third parties in Inner Mongolia. Domestic distributors and other third parties can obscure the role of U.S.-sanctioned companies in these supply chains. Of the 1,094 contracts that mention Hikvision (海康威视), 185 mention public security bureaus (公安局) and five mention Sharp Eyes (雪亮工程) projects, which also indicates that Hikvision products may be operationalized for public security projects and state-led surveillance projects in the region.

Figure 6: Date distribution of the 39 Inner Mongolia contracts with a telecom supplier⁷⁰

Hikvision was added to the BIS Entity List in 2019 for “human rights violations and abuses in the implementation of China’s campaign of repression, mass arbitrary detention, and high-technology surveillance against Uyghurs, Kazakhs, and other members of Muslim minority groups in the XUAR.”⁷¹ Hikvision maintains global operations through its subsidiaries in Canada, Australia, the Netherlands, the United Kingdom, Brazil, South Africa, Singapore, South Korea, and the United States.⁷²

This report selects the following Hebei Brilliance contracts as case studies for demonstrating the obscured involvement of U.S.-sanctioned companies in digital surveillance contracts with public security agencies, and for containing three surveillance-related keywords each: “video surveillance” (视频监控), “Sharp Eyes” (雪亮工程), and “pastoral area” (牧区). The obscured nature of U.S.-sanctioned companies simply reflects a larger supply chain risk for companies that want access to the U.S. market. The case study also illustrates the role of domestic distributors and large, state-owned telecom companies in such contracts.

Case Study

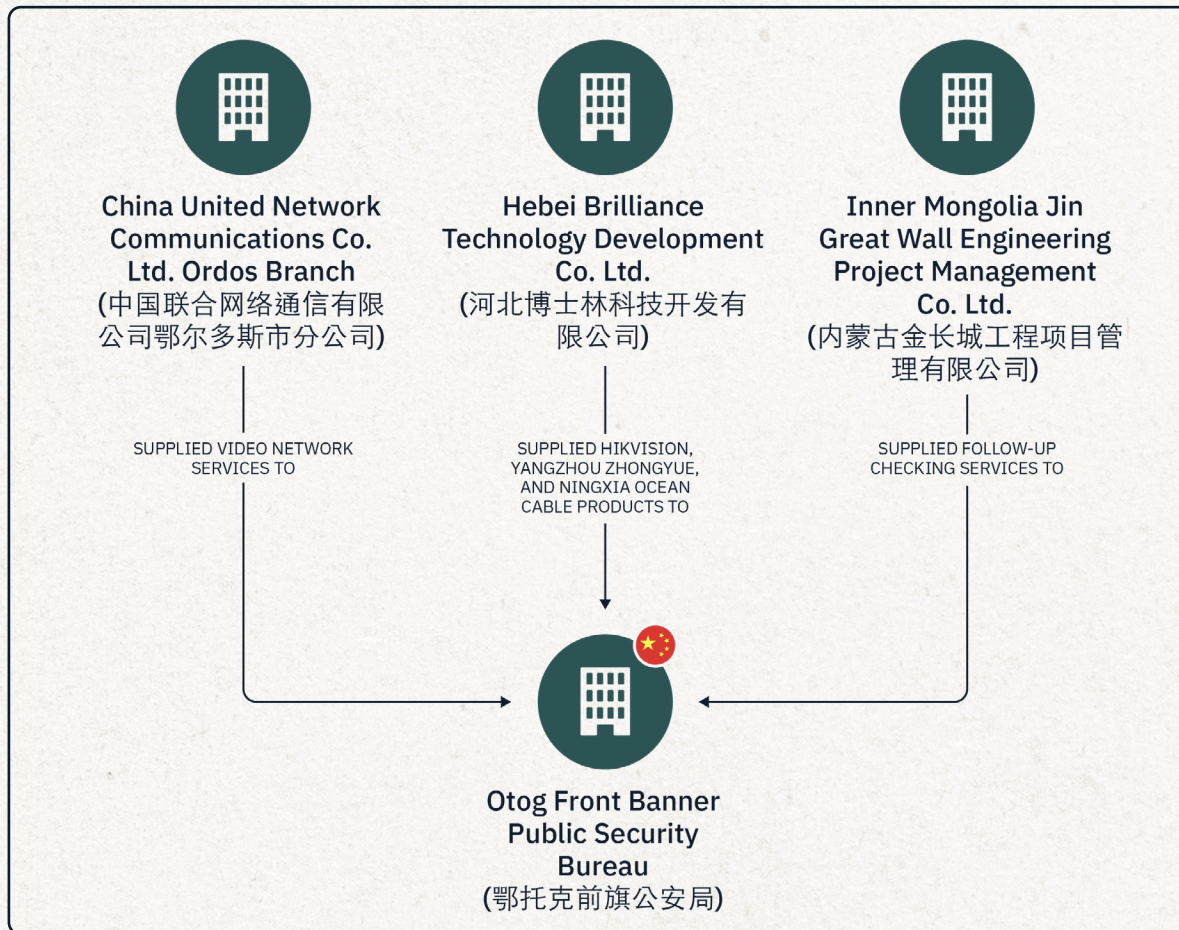
In 2022, Hebei Brilliance Technology Development Co., Ltd. (河北博士林科技开发有限公司, hereafter Hebei Brilliance); China United Network Communications Co., Ltd. Ordos Branch (中国联合网络通信有限公司鄂尔多斯市分公司, hereafter China Unicom Ordos); and Inner Mongolia Jin Great Wall

Engineering Project Management Co., Ltd. (内蒙古金长城工程项目管理有限公司, hereafter Inner Mongolia Jin Great Wall); won bids to supply Otog Front Banner Public Security Bureau (鄂托克前旗公安局, hereafter Otog Front Banner PSB), with goods and services for a rural and pastoral areas (农村牧区) video surveillance network under the Sharp Eyes (雪亮工程) project.⁷³ China Unicom Ordos is the second most frequent supplier on Inner Mongolia contracts flagged for this report.

Hebei Brilliance is an artificial intelligence technology company that develops software and big data solutions for law enforcement agencies to analyze video footage and process large amounts of public safety data.⁷⁴ According to WireScreen, Hebei Brilliance has also supplied the Shijiazhuang Municipal Public Security Bureau (石家庄市公安局) and the Traffic Management Bureau of the Hebei Public Security Department (河北省公安厅交通管理局) with maintenance and operations services, respectively.⁷⁵

According to the contract details, Hebei Brilliance supplied Otog Front Banner PSB with multiple Hikvision products: 33 terminal servers, 33 outdoor industrial switches, 94 smart bullet cameras, 94 bullet camera brackets, 94 supplemental lights, six smart pan-tilt-zoom (PTZ) cameras, six PTZ camera brackets, and 100 units of “camera power supply,” all of which were manufactured by Hikvision.⁷⁶ For this 2022 Sharp Eyes project, Hebei Brilliance supplied a total of US\$188,900 (¥1,268,000) worth of video surveillance equipment and installation. Hikvision products make up 58.26% (US\$110,000/¥738,770) of Hebei Brilliance’s total contributions to the project in 2022.⁷⁷ Other manufacturers of the products supplied by Hebei Brilliance include Yangzhou Zhongyue Lighting Technology Co., Ltd. (扬州中越照明科技有限公司, hereafter Yangzhou Zhongyue) and Ningxia Ocean Cable Co., Ltd. (宁夏海洋线缆有限公司, hereafter Ningxia Ocean Cable).⁷⁸ Yangzhou Zhongyue’s products, which account for 7.63% (US\$14,400/¥96,784) of the contract, include surveillance poles and other video surveillance equipment.⁷⁹ Ningxia Ocean Cable’s products, which account for 4.72% (US\$8,900/¥59,900) of the contract, include power cables.

Figure 7: Supplier relationships in the 2022 Otog Front Banner Public Security Bureau Sharp Eyes procurement⁸⁰



For the same Sharp Eyes project, China Unicom Ordos and Inner Mongolia Jin Great Wall supplied Otog Front Banner PSB with US\$25,300/¥169,900 worth of “specialized video network” (视频专网) services and US\$4,400/¥29,500 worth of “follow-up checking” (跟踪审核) services, respectively.⁸¹ China Unicom Ordos’s involvement in this contract is reflective of the significant role China Unicom and other large, state-owned telecom companies play in Inner Mongolia surveillance projects.

Hebei Brilliance, China Unicom Ordos, and Inner Mongolia Jin Great Wall are listed as suppliers on a 2023 contract of the same name, which indicates an ongoing Sharp Eyes project in Otog Front Banner.⁸² In 2023, Hebei Brilliance was commissioned for US\$286,970/ ¥1,925,994 worth of “equipment and installation” on the same Sharp Eyes project for a rural and pastoral areas video surveillance network.⁸³ The 2023 contract indicates that Hebei Brilliance supplied another batch of similar Hikvision products: terminal servers, smart bullet cameras, smart PTZ cameras, camera brackets, and camera power supplies.⁸⁴ According to Chinese government records, Hikvision products make up 53.47% (US\$153,400/¥1,029,750) of Hebei Brilliance’s total contributions to the project in 2023.⁸⁵ Yangzhou Zhongyue and Ningxia Ocean Cable also contributed 7.68% (US\$22,030/¥147,824) and 4.43% (US\$12,710/¥85,314) to the 2023 contract, respectively. Taken together, these figures demonstrate that Hikvision, a sanctioned manufacturer, supplied the majority of this contract’s value, not directly, but through an unsanctioned distributor, Hebei Brilliance. This exemplifies the type of intermediary relationship that the recommendations urge regulators to scrutinize more closely.

Hong Kong

Background



Since the 2019 Hong Kong pro-democracy protests and the passage of the 2020 National Security Law (NSL), the Chinese government's involvement in and oversight of Hong Kong's internal security matters has increased.⁸⁶ The NSL broadly criminalizes secession, subversion, terrorism, and "collusion with a foreign country," with persons convicted sentenced to up to life in prison, and China's central government able to prosecute and adjudicate cases in mainland China.⁸⁷ This law has been used to prosecute Hong Kong residents for peaceful political expression, participation in pro-democracy electoral activities, and journalism.⁸⁸ For example, 47 politicians and activists were charged with subversion under the NSL for their involvement in the 2020 unofficial pan-democratic primary election.⁸⁹ For nearly a decade, the Hong Kong Police Force (HKPF) has used excessive force against pro-democracy protesters, employing repressive tactics such as beatings, arbitrary arrests, and other instances of police misconduct.⁹⁰ According to the Hong Kong Democracy Council, 1,944 political prisoners have been detained by the HKPF since the 2019 mass protests began, among them journalists, students, activists, and lawyers.⁹¹ Public reporting in and outside of Hong Kong suggests that the HKPF is enhancing digital surveillance practices and increasingly digitizing the collection of biometric data with the implementation of advanced technology like AI-enabled facial recognition.⁹²

Key Findings

C4ADS collected 5,880 contracts of Hong Kong government data spanning December 2019 to April 2025. Within this dataset, C4ADS identified 15 Hong Kong contracts containing two or more surveillance-related keywords. The most frequently occurring keywords across the Hong Kong contracts were "police" (233 contracts), "surveillance" (78 contracts), "camera" (33 contracts), "risk assessment" (eight contracts), and "fingerprint" (three contracts).

The flagged records most frequently identify the following five suppliers:

1. Creaxon Technologies Inc. Limited
2. Hong Kong Telecommunication (HKT) Limited
3. OT Systems Limited
4. Parking Systems Limited
5. Thales DIS Hong Kong Limited

Taken together, this data from the Hong Kong Government Gazette illustrates how local authorities are acquiring biometric data collection technology and services, a trend consistent with the broader expansion of China's surveillance economy and one that mirrors patterns already documented in the regions discussed above. This report highlights the Thales HK contracts as a case study because it demonstrates the HKPF's acquisition of biometric data collection technology or services and reflects the notable involvement of a foreign manufacturer supplying such technology to the HKPF. Additionally, these contracts were selected

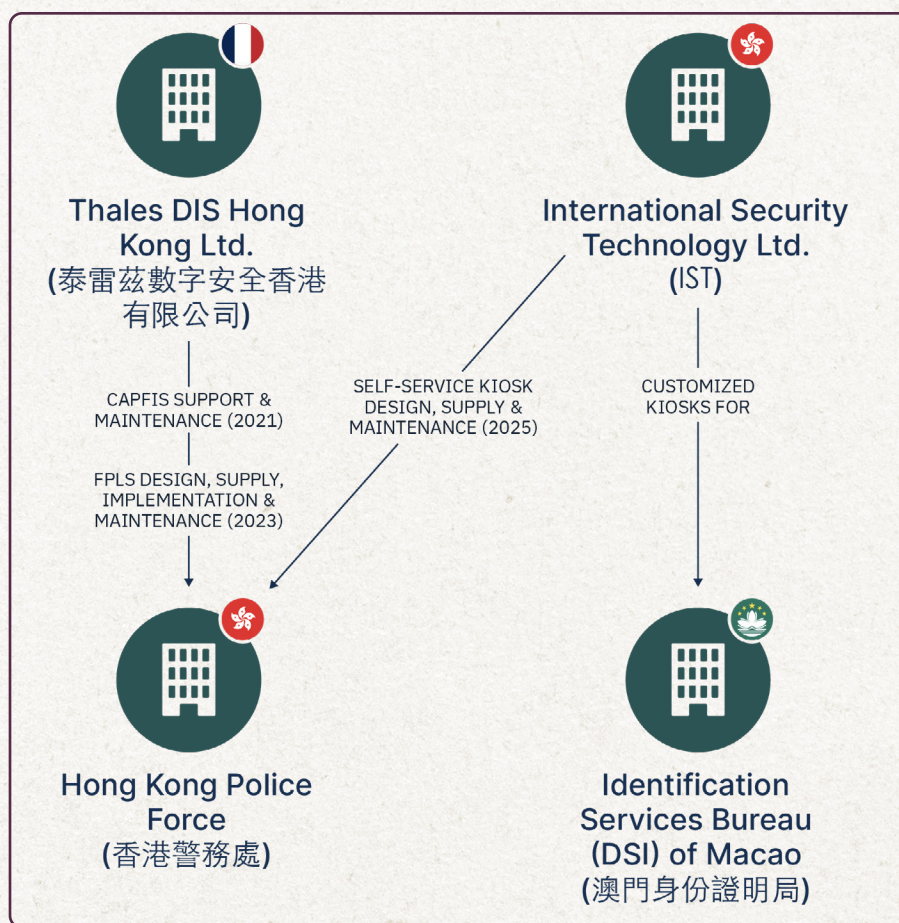
because each contains three surveillance-related keywords: “police,” “palmprint,” and “fingerprint.” Finally, the case study shows HKPF’s continued investment in biometric data collection technology that carries a high potential for use in heavy-handed and potentially abusive policing.

Case Study

On June 15, 2021, the HKPF awarded Thales DIS Hong Kong Limited (泰雷茲數字安全香港有限公司, hereafter Thales HK) a contract for the “provision of system support and maintenance services” for the HKPF’s Computer Assisted Palmprint and Fingerprint Identification System.⁹³ The contract, which was published in the Hong Kong Government Gazette, is valued at US\$3,640,000 or HKD 28,539,845 and covers a period of five years.⁹⁴ Thales HK is a wholly owned, Hong Kong-registered subsidiary of Thales Group, a French multinational technology corporation.⁹⁵ Thales Group provides digital identity and security solutions, including identity and biometrics solutions for law enforcement and financial institutions.⁹⁶

On December 12, 2023, the HKPF awarded Thales HK another contract for the design, supply, implementation, maintenance, and replacement of the HKPF’s Fingerprint and Palmprint Live Scan System.⁹⁷ The contract was published in the Hong Kong Government Gazette in January 2024 and is valued at US\$7,190,000 or HKD 56,389,159.⁹⁸

Figure 8: Supplier relationships in Hong Kong Police Force biometric purchases (2021–2025)⁹⁹



On March 13, 2025, the HKPF awarded International Security Technology Limited (IST) a contract for the design, supply, implementation, and maintenance of the “Self-Services Kiosk with Fingerprint-Taking Service” for the HKPF.¹⁰⁰ The contract is valued at US\$127,300 or approximately HKD 998,385 and covers a maintenance service period of five years.¹⁰¹ IST is based in Hong Kong and describes itself as a “global provider of identity security systems and products” on its official website.¹⁰² IST’s self-service kiosks, which it has customized for government agencies like the Identification Services Bureau of Macau, are designed for the “application and collection of identity cards and travel documents,” with features like “infrared height measurement, ten-finger fingerprint collection, and rolled fingerprint collection [to] ensure the accuracy and compliance of biometric data capture.”¹⁰³ Unlike the sanctioned manufacturers examined in the other regional case studies, neither Thales nor IST is currently subject to U.S. or EU sanctions. Because these arrangements involve direct government-service contracts rather than equipment shipments, they also fall outside existing export-control frameworks. This enforcement gap is also addressed via the recommendations below.

Conclusion

China's surveillance apparatus constitutes a deliberate architecture of repression. Analyzing Tibet, the Uyghur region, Inner Mongolia, and Hong Kong together demonstrates that the CCP's surveillance efforts are not isolated but part of a system of control that represses ethnic minorities and political dissidents at scale. Targeted populations in three of the four regions (Tibet, the Uyghur Region, and Hong Kong) are identified in the CCP's Five Poisons framework. The pervasiveness of surveillance projects in Inner Mongolia and the commonalities between government surveillance acquisitions in Inner Mongolia and other regions demonstrates that the CCP views other populations as potential threats and has extended the reach of its repressive surveillance efforts well beyond the Five Poisons groups. Nevertheless, the Five Poisons designation remains the clearest indicator of which populations Beijing regards as the greatest threats to national security.

In all four regions covered by this report, PSBs appear as buyers of biometric and video surveillance technology capable of identifying and monitoring individuals at scale. In Tibet, the Uyghur region, and Inner Mongolia, PSBs are relying heavily on domestic distributors and telecommunications subsidiaries as suppliers. In the Uyghur region and Inner Mongolia, sanctioned manufacturers' equipment appears in contracts in which these manufacturers are rarely the direct supplier. Hong Kong is a distinct case: the buyer is the police force, while the major suppliers are unsanctioned, and one identified supplier is a foreign entity – placing the enforcement gap in government-services contracts rather than in layered distribution channels.

The Chinese government data from these regions also exposes gaps in existing accountability mechanisms and highlights key players in digital surveillance procurement networks in China. Despite intermittent public attention to China's surveillance apparatus, international efforts to disrupt the CCP's repression campaigns remain insufficient and will need to grapple with the growing domestication of China's surveillance supply chain. As that domestic industry continues to mature, the foreign-technology dependencies that current sanctions and export controls rely on as points of leverage will weaken over time. Policymakers should begin identifying tools – financial designations, corporate disclosure requirements, multilateral coordination, or other mechanisms – that will remain effective in a future where China's surveillance apparatus may no longer depend on foreign inputs at all.

The supply chains revealed through data explored in this report offer a model to help identify the companies, contracts, and purchase patterns where accountability efforts can focus now, even as the broader policy toolkit continues to evolve.

Recommendations

- **Extend sanctions to intermediary and distributor relationships. Current sanctions lose effect once a manufacturer's products pass through a distributor.** None of the flagged Uyghur region contracts in this report list Uniview as a direct supplier, yet Uniview is named in 54 surveillance-related contracts, including one where intermediary Shanghai Sailing Information Technology supplied Uniview equipment directly to a PSB. Inner Mongolia shows the same pattern: Hikvision equipment delivered through distributor Hebei Brilliance made up over half the value of a 2023 Sharp Eyes contract. Regulators should treat repeat distributors of sanctioned hardware as designation candidates in their own right, closing the gap between the sanctioned manufacturer and its government end user.
- **Broaden export controls on dual-use technology inputs, not just finished surveillance products.** Much of China's domestic surveillance industry was built through early-stage adaptation of foreign technology, and dual-use components (i.e., semiconductors, sensors, etc.) continue to enter the supply chain today. Restricting China's access to dual-use foreign inputs is a necessary complement to sanctioning individual surveillance manufacturers. Regulators should evaluate whether current dual-use export control lists adequately capture the inputs feeding this supply chain.
- **Raise due diligence and know-your-customer standards for suppliers of biometric technology to abusive security services.** Thales DIS Hong Kong Limited, a subsidiary of the French Thales Group, won two direct HKPF contracts to build and maintain biometric identification systems in the years following the HKPF's documented use of excessive force against pro-democracy protesters. Because these are government-services contracts rather than equipment shipments, they fall outside existing export-control frameworks. U.S. and EU regulators should require companies to disclose and justify subsidiary contracts that supply biometric or surveillance technology to security services with documented abuse records, and private firms should apply the same scrutiny before signing.
- **Require export licenses for dual-use surveillance technology, including biometric collection hardware and video analytics platforms** – destined for public security agencies in Tibet, the Uyghur region, Inner Mongolia, Hong Kong, or other high-risk regions with documented human rights abuses. Existing end-use certification requirements should extend to sales made through domestic distributors and system integrators, not just direct exports.
- **Open Treasury and Commerce investigations into the companies named in this report.** Firms such as Shanghai Sailing, Beijing Xinyu, Hebei Brilliance, and Hisign play central roles in supplying China's surveillance apparatus without themselves being sanctioned. They warrant closer scrutiny and should be evaluated for designation.
- **Coordinate sanctions and export-control lists with European and other partner governments.** Without harmonization, companies flagged in this report can route around U.S.-specific restrictions through non-U.S. markets and corporate structures.

- **Require European technology firms to conduct enhanced human rights due diligence.** Firms should verify end users and end uses to ensure their components, capital, and technology are not incorporated into systems deployed against marginalized populations.
- **Treat routine telecom-subsidary contracts as a distinct enforcement gap.** China Telecom, China Mobile, and China Unicom subsidiaries were among the top suppliers for surveillance-related projects across the regions discussed in this report. These companies have continued signing low-cost surveillance-infrastructure contracts with sanctioned entities such as the XPCC, years after U.S. restrictions were enacted on investment in their parent companies. This shows that restricting investment in the parent companies has not stopped subsidiaries from supplying equipment and services at the operational level. Complementary tools are needed, such as Entity List additions targeting specific subsidiaries or import restrictions that place the burden on companies to show their supply chains are clean.
- **Strengthen export controls on biotechnology and related intellectual property shared with Chinese government partners.** Multinational companies should audit their forensic DNA products and processes to ensure they are not being used, or are not likely to be used, in ways that violate human and civil rights.

Appendix: Methodology

Comment

During the literature review, search terms were aggregated from the following sources:

- ChinaFile¹⁰⁴
- Center for Security and Emerging Technology (CSET Georgetown)¹⁰⁵
- Brookings¹⁰⁶
- Human Rights Watch¹⁰⁷
- Journal of Chinese Political Science article: Liang, Li, and Guo on video surveillance diffusion in China¹⁰⁸
- Remote Ethnography XUAR¹⁰⁹
- Australian Strategic Policy Institute (ASPI)¹¹⁰

Consolidated List of Surveillance Search Terms

No.	Chinese Term	English Translation	Type of Term
1	语音识别	SPEECH RECOGNITION	General, Biometric term
2	人脸识别	FACIAL RECOGNITION	General, Biometric term
3	面部识别	FACIAL RECOGNITION	General, Biometric term
4	声纹	VOICEPRINT	General, Biometric term
5	虹膜扫描	IRIS SCANNING	General, Biometric term
6	步态识别	GAIT RECOGNITION	General, Biometric term
7	步态分析	GAIT ANALYSIS	General, Biometric term
8	多模态生物识别	MULTI-MODE BIOMETRICS	General, Biometric term
9	身份验证	AUTHENTICATION	General, Biometric term
10	生物识别	BIOMETRIC RECOGNITION	General, Biometric term
11	生物数据	BIOMETRIC DATA	General, Biometric term
12	生物特征识别	BIOMETRIC DATA	General, Biometric term
13	三维人像综合数据门	THREE-DIMENSIONAL PORTRAIT / DATA DOOR	General, Biometric term

No.	Chinese Term	English Translation	Type of Term
14	人证核验	PERSON-ID VERIFICATION TERMINAL	General, Biometric term
15	人脸比对	FACE COMPARISON / MATCHING	General, Biometric term
16	民族分类	ETHNIC CLASSIFICATION	General, Biometric term
17	维族高危人员库	HIGH-RISK UYGHUR DATABASE	General, Biometric term
18	种族属性	RACIAL ATTRIBUTES	General, Biometric term
19	DNA采集	DNA COLLECTION	General, Biometric term
20	DNA数据库	DNA DATABASE	General, Biometric term
21	指纹识别	FINGERPRINT RECOGNITION	General, Biometric term
22	多模态生物特征	MULTIMODAL BIOMETRIC FEATURES	General, Biometric term
23	虹膜识别	IRIS RECOGNITION	General, Biometric term
24	身份核验	IDENTITY VERIFICATION	General, Biometric term
25	虹膜采集	IRIS COLLECTION	General, Biometric term
26	人像感知网络	PORTRAIT PERCEPTION NETWORK	General, Biometric term
27	监控	SURVEILLANCE	General
28	监视	SURVEILLANCE	General
29	情感分析	SENTIMENT ANALYSIS	General
30	行为预测	BEHAVIOR PREDICTION	General
31	机器学习	MACHINE LEARNING	General
32	深度学习	DEEP LEARNING	General
33	大语言模型	LARGE LANGUAGE MODEL	General
34	大型语言模型	LARGE LANGUAGE MODEL	General
35	神经网络	NEURAL NETWORK	General
36	自然语言处理	NATURAL LANGUAGE PROCESSING	General
37	音频定位	AUDIO LOCALIZATION	General
38	声源定位	AUDIO LOCALIZATION	General
39	不可见光谱成像	NON-VISIBLE SPECTRUM IMAGING	General
40	红外成像	INFRARED IMAGING	General
41	数据追踪	DATA TRACKING	General
42	实时位置追踪	REAL-TIME LOCATION TRACKING	General
43	加密绕过	ENCRYPTION BYPASS	General
44	综合安全平台	INTEGRATED SECURITY PLATFORM	General
45	集成安全平台	INTEGRATED SECURITY PLATFORM	General
46	智能安全	SMART SECURITY	General

No.	Chinese Term	English Translation	Type of Term
47	智能安防	SMART SECURITY	General
48	公共安全解决方案	PUBLIC SAFETY SOLUTION	General
49	摄像头	CAMERA	General
50	联合作战平台	IJOP	General
51	一体化平台	IJOP	General
52	警戒摄像机	ALERT CAMERAS	General
53	智慧磐石	BOULDER OF WISDOM	General
54	中央维护稳定工作领导小组	CENTRAL LEADING SMALL GROUP FOR STABILITY MAINTENANCE	General
55	政法委员会	CENTRAL POLITICAL AND LEGAL AFFAIRS COMMISSION	General
56	中央社会治安综合治理委员会	CENTRAL PUBLIC SECURITY COMPREHENSIVE MANAGEMENT COMMISSION	General
57	综合管理平台	COMPREHENSIVE MANAGEMENT PLATFORM	General
58	天眼工程	EYE IN THE SKY	General
59	流动人口信息系统	FLOATING POPULATION INFORMATION SYSTEM	General
60	在逃人员系统	FUGITIVE SYSTEM	General
61	资金分析模块	FUND ANALYSIS MODULE	General
62	智能跟踪一体机	INTEGRATED INTELLIGENT TRACKING CAMERAS	General
63	一体化联合作战平台	INTEGRATED JOINT OPERATIONS PLATFORM (IJOP)	General
64	重点人员	KEY PERSONS	General
65	重点人管控模块	KEY PERSON CONTROL MODULE	General
66	重点人口	KEY POPULATIONS	General
67	公安部	MINISTRY OF PUBLIC SECURITY	General
68	多元分析模块	MULTIVARIATE ANALYSIS MODULE	General
69	全景一体化摄像机	PANORAMIC CAMERAS	General
70	人员密度摄像机	POPULATION DENSITY CAMERA	General
71	人口信息系统	POPULATION INFORMATION SYSTEM	General
72	雪亮工程	SHARP EYES PROJECT	General
73	天网工程	SKYNET PROJECT	General
74	安全边界平台	SAFE BORDERS PLATFORM	General
75	平安城市	SAFE CITIES	General
76	智慧城市	SMART CITIES	General
77	智慧警务	SMART POLICING	General
78	社会资源整合平台	SOCIETAL RESOURCE INTEGRATION PLATFORM	General
79	涉恐涉暴人员预测模块	TERRORIST AND VIOLENT PERSON PREDICTION MODULE	General
80	高空瞭望热成像监控	THERMAL IMAGING MONITORING POINTS	General
81	轨迹分析模块	TRAJECTORY ANALYSIS MODULE	General
82	城市管理	URBAN MANAGEMENT (CHENGGUAN)	General
83	平安乡镇	SAFE TOWNSHIP	General
84	平安校园	SAFE CAMPUS	General
85	平安景区	SAFE SCENIC AREA	General
86	平安建设	SAFE/PEACE CONSTRUCTION	General
87	视频监控	VIDEO SURVEILLANCE	General

No.	Chinese Term	English Translation	Type of Term
88	预测性警务	PREDICTIVE POLICING	General
89	便民警务站	CONVENIENCE POLICE STATION	General
90	舆情	PUBLIC OPINION (YUQING)	General
91	舆论	PUBLIC OPINION / PUBLIC DISCOURSE	General
92	网评	ONLINE COMMENTARY / COMMENTING	General
93	民意	PUBLIC SENTIMENT	General
94	金盾工程	GOLDEN SHIELD PROJECT	General
95	警务云	POLICE CLOUD	General
96	网格化管理	GRID-BASED MANAGEMENT	General
97	去极端化	DE-EXTREMIFICATION	General
98	反恐	COUNTER-TERRORISM	General
99	防控	PREVENTION AND CONTROL	General
100	维稳	STABILITY MAINTENANCE	General
101	数据融合	DATA FUSION	General
102	国防动员	NATIONAL DEFENSE MOBILIZATION	General
103	可视化	VISUALIZATION (POLICE)	General
104	警务信息化	POLICE INFORMATIZATION	General
105	政府信息孤岛	GOVERNMENT INFORMATION ISLANDS	General
106	卡口	CHECKPOINT / ACCESS CONTROL POINT	General
107	WiFi探针	WIFI SNIFFER / PROBE	General
108	电子围栏	ELECTRONIC FENCE / GEOFENCE	General
109	安防	SECURITY / SECURITY PREVENTION	General
110	数字城市	DIGITAL CITY	General
111	电子警察	ELECTRONIC POLICE	General
112	法治	RULE OF LAW	General
113	安保	PEACE AND SECURITY	General
114	抓拍	SNAPSHOT / CAPTURE	General
115	智能分析	INTELLIGENT ANALYSIS	General
116	维族	UYGHUR (IN FACE DATABASES)	General
117	平安新疆	SAFE XINJIANG	General
118	大数据	BIG DATA	General
119	综合治理	COMPREHENSIVE MANAGEMENT / COMPREHENSIVE GOVERNANCE	General
120	综治	COMPREHENSIVE MANAGEMENT (ABBREV)	General
121	网格化	GRID-BASED MANAGEMENT (SHORT)	General
122	社会信用	SOCIAL CREDIT	General
123	预警	EARLY WARNING	General
124	车牌识别	LICENSE PLATE RECOGNITION	General
125	车辆识别	VEHICLE RECOGNITION	General
126	无人机	DRONE / UAV	General
127	热成像	THERMAL IMAGING	General
128	执法记录仪	BODY-WORN CAMERA / BODY CAM	General
129	网络安全	CYBERSECURITY / NETWORK SECURITY	General
130	内容审查	CONTENT REVIEW / CENSORSHIP	General
131	内容过滤	CONTENT FILTERING	General

No.	Chinese Term	English Translation	Type of Term
132	深度包检测	DEEP PACKET INSPECTION	General
133	净网	CLEAN NET	General
134	电子取证	DIGITAL FORENSICS	General
135	手机检查	MOBILE PHONE INSPECTION	General
136	信息拦截	INFORMATION INTERCEPTION	General
137	访客管理	VISITOR MANAGEMENT SYSTEM	General
138	双语教育	BILINGUAL EDUCATION	General
139	风险评估	RISK ASSESSMENT	General
140	轨迹分析	TRAJECTORY ANALYSIS	General
141	IMSI捕获器	IMSI CATCHER	General
142	蜂采	BXAQ APP	General
143	民族团结进步	ETHNIC UNITY AND PROGRESS	General
144	一人一档	ONE PERSON, ONE FILE	General
145	百万警进千万家	ONE MILLION POLICE ENTERING TEN MILLION HOMES	General
146	综治中心	COMPREHENSIVE MANAGEMENT CENTER	General
147	社会治安防控	PUBLIC-SECURITY PREVENTION AND CONTROL	General
148	立体化社会治安防控体系	THREE-DIMENSIONAL PUBLIC-SECURITY PREVENTION AND CONTROL SYSTEM	General
149	长治久安	LONG-TERM STABILITY	General
150	动态管控	DYNAMIC CONTROL	General
151	一标三实	"ONE PROPER, THREE REALS"	General
152	群体性事件	MASS INCIDENTS	General
153	社会稳定(维稳)	SOCIAL STABILITY	General
154	社会管理	SOCIAL MANAGEMENT	General
155	智慧边防综合应用平台	SMART BORDER DEFENSE COMPREHENSIVE APPLICATION PLATFORM	General
156	无感数据门	SENSELESS DATA GATES	General
157	行人特帧识别	PEDESTRIAN SPECIAL FRAME RECOGNITION	General
158	车辆特侦识别	VEHICLE SPECIAL RECONNAISSANCE RECOGNITION	General
159	动态视频行为	DYNAMIC VIDEO BEHAVIOR	General
160	智服惠民	WISDOM SERVING THE PEOPLE	General
161	人员管控系统	PERSONNEL CONTROL SYSTEM	General
162	国安局 / 国家安全局	STATE SECURITY	General
163	武警	ARMED POLICE/PAP	General
164	边防	BORDER DEFENSE	General
165	民委 / 民族事务委员会	ETHNIC AFFAIRS COMMISSION	General
166	寺庙监控	MONASTERY SURVEILLANCE	TAR-specific
167	寺院管理	MONASTERY MANAGEMENT	TAR-specific
168	平安西藏	SAFE TIBET	TAR-specific
169	僧尼	MONKS AND NUNS	TAR-specific
170	藏族	TIBETAN ETHNICITY	TAR-specific
171	爱国主义教育	PATRIOTIC EDUCATION	TAR-specific
172	僧尼管理	MONK AND NUN MANAGEMENT	TAR-specific
173	双联户	DOUBLE-LINKED HOUSEHOLDS	TAR-specific

No.	Chinese Term	English Translation	Type of Term
174	驻村工作队	VILLAGE-BASED CADRE TEAMS	TAR-specific
175	强基础惠民生	STRENGTHEN FOUNDATIONS, BENEFIT LIVELIHOODS	TAR-specific
176	感党恩	"FEEL THE PARTY'S KINDNESS"	TAR-specific
177	无缝隙、无漏洞、无空白	NO SEAMS, NO LOOPHOLES, NO BLANKS	TAR-specific
178	维稳双联户	DOUBLE-LINKED HOUSEHOLDS FOR STABILITY MAINTENANCE	TAR-specific
179	村村成堡垒，人人做守望	EVERY VILLAGE A FORTRESS, EVERYONE A WATCHMAN	TAR-specific
180	战斗堡垒	FIGHTING FORTRESS / FORTRESS STRONGHOLD	TAR-specific
181	基层维稳	GRASSROOTS STABILITY MAINTENANCE	TAR-specific
182	联防队	JOINT DEFENSE TEAM	TAR-specific
183	巡逻队	PATROL TEAM	TAR-specific
184	入户宣传	HOUSEHOLD PROPAGANDA VISITS	TAR-specific
185	排查并化解社会矛盾	INVESTIGATE AND RESOLVE SOCIAL CONTRADICTIONS	TAR-specific
186	防止村民越级上访	PREVENT VILLAGERS FROM PETITIONING HIGHER AUTHORITIES	TAR-specific
187	消除隐患	ELIMINATE HIDDEN THREATS / UNSEEN THREATS	TAR-specific
188	宗教活动场所视频监控安装联网	INSTALLATION AND NETWORKING OF VIDEO SURVEILLANCE AT RELIGIOUS SITES	TAR-specific
189	先进双联户	ADVANCED DOUBLE-LINKED HOUSEHOLDS	TAR-specific
190	强基惠民	SOLIDIFY THE FOUNDATIONS, BENEFIT THE MASSES	TAR-specific
191	驻寺工作组	MONASTERY-STATIONED GOVERNMENT WORK UNIT	TAR-specific
192	四条标准	FOUR STANDARDS FOR MONKS AND NUNS	TAR-specific
193	铜墙铁壁	COPPER RAMPARTS, IRON WALLS	TAR-specific
194	没有缝子，没有盲点，没有空白点	NO CRACKS, NO BLIND SPOTS, NO GAPS	TAR-specific
195	感党恩听党话跟党走	FEEL THE PARTY'S KINDNESS, LISTEN/FOLLOW THE PARTY	TAR-specific
196	四讲四爱	FOUR STRESSES AND FOUR LOVES	TAR-specific
197	和谐模范寺庙	HARMONIOUS MODEL MONASTERY	TAR-specific
198	群众监督评议委员会	MASSES SUPERVISION AND APPRAISAL COMMITTEE	TAR-specific
199	11类59种重点人员	11 TYPES AND 59 KINDS OF KEY PERSONS	TAR-specific
200	标本兼治	FIXING ROOT AND BRANCH TOGETHER	TAR-specific
201	红袖标巡逻	RED ARMBAND PATROLS	TAR-specific
202	藏传佛教活佛转世管理办法	MGMT MEASURES FOR REINCARNATION OF LIVING BUDDHAS	TAR-specific
203	反自焚工作暂行规定	INTERIM ANTI-SELF-IMMOLATION PROVISIONS	TAR-specific
204	访惠聚	"BECOMING FAMILY" CAMPAIGN	XUAR-specific
205	访民情、惠民生、聚民心	VISIT THE PEOPLE'S CONDITIONS, BENEFIT THE PEOPLE'S LIVELIHOOD, GATHER THE PEOPLE'S HEARTS	XUAR-specific

No.	Chinese Term	English Translation	Type of Term
206	便民卡	CONVENIENCE CARD	XUAR-specific
207	严厉打击暴力恐怖活动专项行动	STRIKE HARD CAMPAIGN AGAINST VIOLENT TERRORISM	XUAR-specific
208	宗教极端主义	RELIGIOUS EXTREMISM	XUAR-specific
209	民族团结	ETHNIC UNITY	XUAR-specific
210	是否维族人	WHETHER A PERSON IS UYGHUR	XUAR-specific
211	维族人识别准确率不低于97%	UYGHUR-IDENTIFICATION ACCURACY NO LOWER THAN 97%	XUAR-specific
212	汉族	HAN ETHNICITY	XUAR-specific
213	非汉族人员识别以及独立报警	IDENTIFICATION OF NON-HAN PERSONS INCLUDING INDEPENDENT ALARM	XUAR-specific
214	关注的人员	PERSONS OF CONCERN	XUAR-specific
215	四关联	FOUR ASSOCIATIONS	XUAR-specific
216	关联案件线索	LINKED TO CASE CLUES	XUAR-specific
217	关联在逃人员	LINKED TO FUGITIVES	XUAR-specific
218	关联境外人员	LINKED TO PERSONS ABROAD	XUAR-specific
219	关联关注人员	LINKED TO PERSONS UNDER SPECIAL WATCH	XUAR-specific
220	手机调查反馈	MOBILE PHONE INVESTIGATION FEEDBACK	XUAR-specific
221	法制教育转化学校	LEGAL TRANSFORMATION THROUGH EDUCATION SCHOOL	XUAR-specific
222	三维人像及综合数据门	THREE-DIMENSIONAL PORTRAIT AND INTEGRATED DATA DOORS	XUAR-specific
223	天山反恐云	TIANSHAN ANTI-TERRORISM CLOUD	XUAR-specific
224	东突暴恐活动数据库	EAST TURKISTAN TERRORIST ACTIVITY DATABASE	XUAR-specific
225	综合轨迹系统	INTEGRATED TRACKING SYSTEM	XUAR-specific
226	智能手机取证系统	SMARTPHONE FORENSIC SYSTEMS	XUAR-specific
227	清除思想病毒	ERADICATING IDEOLOGICAL VIRUSES	XUAR-specific
228	蓝灯大数据系统	ITAP BIG DATA POLICE SYSTEM	XUAR-specific
229	知谱	ZHIPU KNOWLEDGE GRAPH	XUAR-specific
230	反恐利剑	ANTI-TERRORISM SWORD	XUAR-specific
231	三维画像一体化数据门	THREE-DIMENSIONAL PORTRAIT INTEGRATED DATA DOORS	XUAR-specific
232	百姓安全	CITIZEN SAFETY APP	XUAR-specific
233	防回流	BACKFLOW PREVENTION	XUAR-specific
234	断通联	SEVERED COMMUNICATIONS	XUAR-specific
235	微线索	MICRO-CLUES	XUAR-specific
236	隐性涉恐维族人员	UYGHURS WITH HIDDEN TERRORIST INCLINATIONS (CODE 3185)	XUAR-specific
237	清真寺视频联网系统	MOSQUE VIDEO NETWORKING SYSTEM	XUAR-specific
238	不放心人员	UNTRUSTWORTHY PERSONS	XUAR-specific
239	出境未归人员	PERSONS WHO WENT ABROAD AND DID NOT RETURN	XUAR-specific
240	三非一品	THREE ILLEGALS AND ONE PRODUCT	XUAR-specific
241	泛清真化	PAN-HALALIZATION	XUAR-specific
242	全民健康体检	PHYSICALS FOR ALL	XUAR-specific
243	教育培训局	EDUCATION AND TRAINING BUREAU	XUAR-specific

No.	Chinese Term	English Translation	Type of Term
244	四个不允许	FOUR NEVERS	XUAR-specific
245	积分制	POINT-BASED SCORING SYSTEM	XUAR-specific
246	教育转化培训中心	CONCENTRATED TRANSFORMATION CENTERS	XUAR-specific
247	转移就业	LABOR TRANSFER EMPLOYMENT	XUAR-specific
248	农村富余劳动力	RURAL SURPLUS LABORERS	XUAR-specific
249	结对认亲	PAIR UP AND BECOME FAMILY	XUAR-specific
250	十户联防	TEN FAMILY JOINT DEFENCE	XUAR-specific
251	发声亮剑	SPEAK OUT AND BRANDISH SWORDS	XUAR-specific
252	四项活动	FOUR ACTIVITIES REQUIRING STATE PERMISSION	XUAR-specific
253	靓丽工程	BEAUTY PROJECT	XUAR-specific
254	减掉	SUBTRACTION (UYGHUR: KIYETTI)	XUAR-specific
255	二类暴恐软件	SECOND-CLASS VIOLENT AND TERRORIST SOFTWARE	XUAR-specific
256	平安内蒙古	SAFE INNER MONGOLIA	Inner Mongolia-specific
257	蒙古语 / 蒙语	MONGOLIAN LANGUAGE	Inner Mongolia-specific
258	牧区	PASTORAL AREA	Inner Mongolia-specific
259	社区干预	COMMUNITY INTERVENTION	Inner Mongolia-specific
260	蒙古文舆情监测系统	MONGOLIAN LANGUAGE PUBLIC OPINION MONITORING SYSTEM	Inner Mongolia-specific
261	铸魂工程	SOUL-CASTING ENGINEERING PROJECT	Inner Mongolia-specific
262	智慧边境一张图管理平台	SMART BORDER ONE MAP MANAGEMENT PLATFORM	Inner Mongolia-specific
263	微震探测周界安防系统	MICRO-SEISMIC DETECTION PERIMETER SECURITY SYSTEM	Inner Mongolia-specific
264	人车闭环管控分析比对平台	PERSON-VEHICLE CLOSED-LOOP CONTROL ANALYSIS PLATFORM	Inner Mongolia-specific
265	牧区一键报警	PASTORAL AREA ONE-KEY ALARM	Inner Mongolia-specific
266	智慧放牧	SMART HERDING	Inner Mongolia-specific
267	居边护边堡垒户	BORDER-DWELLING, BORDER-GUARDING FORTRESS HOUSEHOLD	Inner Mongolia-specific
268	漠北驼铃护边队	NORTH DESERT CAMEL BELL BORDER PATROL TEAM	Inner Mongolia-specific
269	网络轻骑兵	INTERNET LIGHT CAVALRY	Inner Mongolia-specific
270	一体化互联网舆情应急指挥平台	INTEGRATED INTERNET PUBLIC OPINION EMERGENCY COMMAND PLATFORM	Inner Mongolia-specific
271	刮骨疗毒	SCRAPE THE BONES TO REMOVE THE POISON	Inner Mongolia-specific
272	五个不变	FIVE NO CHANGES	Inner Mongolia-specific

No.	Chinese Term	English Translation	Type of Term
273	三务融合	THREE AFFAIRS INTEGRATION	Inner Mongolia-specific
274	北疆文化	NORTHERN FRONTIER CULTURE	Inner Mongolia-specific
275	互嵌式社区环境	MUTUALLY EMBEDDED COMMUNITY ENVIRONMENT	Inner Mongolia-specific
276	第二代民族政策	SECOND GENERATION ETHNIC POLICY	Inner Mongolia-specific
277	祖国正北党旗红	PARTY FLAG RED IN THE TRUE NORTH	Inner Mongolia-specific
278	意识形态风险点排查预警处置	IDEOLOGICAL RISK POINT INVESTIGATION/EARLY WARNING	Inner Mongolia-specific
279	铸牢中华民族共同体意识教育系统专项培训	FORGING COLLECTIVE CONSCIOUSNESS SPECIAL TRAINING	Inner Mongolia-specific
280	[N/A, source data is in English]	PALMPRINT	Hong Kong-specific
281	[N/A, source data is in English]	FINGERPRINT	Hong Kong-specific
282	[N/A, source data is in English]	POLICE	Hong Kong-specific

Endnotes

1. Tibet in this report refers to the traditional cultural and ethnographic region encompassing the three provinces of Ü-Tsang, Amdo, and Kham, as commonly used by Tibetan exile organizations and international advocacy groups. This is distinct from the Tibet Autonomous Region (TAR), the narrower administrative unit established by the People's Republic of China in 1965, which covers roughly half of this area. Where this report refers specifically to the PRC administrative unit, it uses "TAR." Provided that the documents analyzed come from the PRC's administration of the region, this report often uses "TAR."
2. This report refers to the Xinjiang Uyghur Autonomous Region (XUAR) as "the Uyghur region," unless referring to existing legal structures, i.e., governments and financial entities.
3. Adrian Zenz and James Leibold, "Chen Quanguo: The Strongman Behind Beijing's Securitization Strategy in Tibet and Xinjiang," *China Brief* 17, no. 12 (September 21, 2017), <https://jamestown.org/chen-quanguo-the-strongman-behind-beijings-securitization-strategy-in-tibet-and-xinjiang/>.
4. PEN America and Southern Mongolian Human Rights Information Center, "Save Our Mother Tongue: Online Repression and Erasure of Mongolian Culture in China" (New York: PEN America, January 20, 2026), <https://pen.org/report/inner-mongolia-china-repression/>; and Jessie Yeung, "Hong Kong Plans to Install Thousands of Surveillance Cameras. Critics Say It's More Proof the City Is Moving Closer to China," CNN, October 5, 2024, <https://www.cnn.com/2024/10/05/asia/hong-kong-police-cameras-facial-recognition-intl-hnk-dst/index.html>.
5. Minxin Pei, *The Sentinel State: Surveillance and the Survival of Dictatorship in China* (Cambridge, MA: Harvard University Press, 2024); nd Josh Chin and Liza Lin, *Surveillance State: Inside China's Quest to Launch a New Era of Social Control* (New York: St. Martin's Press, 2022).
6. Human Rights Watch, "China Uses 'Rule of Law' to Justify Falun Gong Crackdown," November 9, 1999, <https://www.hrw.org/news/1999/11/09/china-uses-rule-law-justify-falun-gong-crackdown>; "China's Sprawling Spy Agencies Are Designed to Root Out the 'Five Poisons' at Home and Abroad, British Intelligence Says," *Caliber.az*, August 5, 2023, <https://caliber.az/en/post/china-s-sprawling-spy-agencies-are-designed-to-root-out-the-five-poisons-at-home-and-abroad-british-intelligence-says>; and Katherine Gordon, "China's Fifth Poison," *Australian Outlook* (Australian Institute of International Affairs), May 2, 2014, <https://www.internationalaffairs.org.au/australianoutlook/chinas-fifth-poison/>.
7. Center for Security and Emerging Technology, "China's Sharp Eyes Program Aims to Surveil 100% of Public Space," Georgetown University, March 2, 2021, <https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/>; Charlotte Lam, "China Accused of Erasing Mongolian Culture Online," *Genocide Watch*, February 11, 2026, <https://www.genocide-watch.com/single-post/china-accused-of-erasing-mongolian-culture-online>; and PEN America, "Chinese Government Destroying Mongolian Language," press release, January 20, 2026, <https://pen.org/press-release/chinese-government-destroying-mongolian-language/>.
8. Garance Burke, Dake Kang, and Byron Tau, "US Government Allowed, and Even Helped, US Firms Sell Tech Used for Surveillance in China, AP Finds," *Associated Press*, 2025, <https://www.ap.org/news-highlights/spotlights/2025/us-government-allowed-and-even-helped-us-firms-sell-tech-used-for-surveillance-in-china-ap-finds/>; republished as "Chinese Surveillance, Silicon Valley, and Uyghurs: US Tech Reaches Xinjiang," *AP News*, <https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-00bed6421ad8d2ccc6e69f104babe892>.
9. Tibet in this report refers to the traditional cultural and ethnographic region encompassing the three provinces of Ü-Tsang, Amdo, and Kham, as commonly used by Tibetan exile organizations and international advocacy groups. This is distinct from the Tibet Autonomous Region (TAR), the narrower administrative unit established by the People's Republic of China in 1965, which covers roughly half of this area. Where this report refers specifically to the PRC administrative unit, it uses "TAR." Provided that the documents analyzed come from the PRC's administration of the region, this report often uses "TAR."
10. This report refers to the Xinjiang Uyghur Autonomous Region (XUAR) as "the Uyghur region," unless referring to existing legal structures, i.e., governments and financial entities.
11. Pei, *The Sentinel State*.
12. Pei, *The Sentinel State*.
13. Charles Rollet, "China PRC Government New National Video Surveillance Standards," *IPVM*, May 14, 2019, <https://ipvm.com/reports/prc-gov-video-standards>; and Christie Smythe, "US Sanctions Uniview," *IPVM*, December 11, 2024, <https://ipvm.com/reports/uniview-sanction>. Historically, Uniview's role has been more concentrated in TAR, while Hikvision's has been more concentrated in the Uyghur Region, although each company has worked in both regions. Uniview supplied surveillance systems that Tibetan authorities reportedly used to identify and detain nearly 200 monks following a protest, with monks describing the systems' purpose as existing to make them "feel fear." Uniview has separately been characterized as a major supplier of customized mass-surveillance infrastructure, having deployed 741 Safe City and 249 Sharp Eyes projects.
14. Samantha Hoffman and Peter Mattis, "Managing the Power Within: China's State Security Commission," *War on the Rocks*, July 18, 2016, <https://warontherocks.com/managing-the-power-within-chinas-state-security-commission/>; Sarah Cook, "Falun Gong's

Secrets for Surviving in China,” Freedom House, July 22, 2019, <https://freedomhouse.org/article/falun-gongs-secrets-surviving-china>; Human Rights Watch, “China Uses ‘Rule of Law’ to Justify Falun Gong Crackdown”; “China’s Sprawling Spy Agencies,” Caliber.az; and Gordon, “China’s Fifth Poison.”

15. Safeguard Defenders, *110 Overseas: Chinese Transnational Policing Gone Wild* (Madrid: Safeguard Defenders, September 12, 2022), [https://safeguarddefenders.com/sites/default/files/pdf/110%20Overseas%20\(v5\).pdf](https://safeguarddefenders.com/sites/default/files/pdf/110%20Overseas%20(v5).pdf).

16. “China’s Great Firewall,” Stanford University, accessed September 1, 2026, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

17. Center for Security and Emerging Technology, “China’s Sharp Eyes Program Aims to Surveil 100% of Public Space.”

18. State Council of the People’s Republic of China, “Policy Directive,” February 4, 2018, https://www.gov.cn/zhengce/2018-02/04/content_5263807.htm.

19. Center for Security and Emerging Technology, “China’s Sharp Eyes Program”; Lam, “China Accused of Erasing Mongolian Culture Online”; and PEN America, “Chinese Government Destroying Mongolian Language.”

20. Congressional-Executive Commission on China, “Chairs Seek Export Controls on Technology Used for Mass Biometric Data Collection in Tibet,” press release, October 23, 2023, <https://www.cecc.gov/media-center/press-releases/chairs-seek-export-controls-on-technology-used-for-mass-biometric-data>; and AFP, “Hong Kong to Install Surveillance Cameras with AI Facial Recognition,” *Hong Kong Free Press*, October 4, 2025, <https://hongkongfp.com/2025/10/04/hong-kong-to-install-surveillance-cameras-with-ai-facial-recognition/>.

21. Human Rights Watch, “‘Break Their Lineage, Break Their Roots’: China’s Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims,” April 19, 2021, <https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots>; Human Rights Watch, “China: How Mass Surveillance Works in Xinjiang,” May 2, 2019, <https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang>; Government of the United States, “China,” in *2021 Country Reports on Human Rights Practices*, U.S. Department of State, April 12, 2022, <https://www.state.gov/reports/2021-country-reports-on-human-rights-practices>; Human Rights Watch, “China,” in *World Report 2026* (New York: Human Rights Watch, 2026), <https://www.hrw.org/world-report/2026/country-chapters/china>; Congressional-Executive Commission on China, “Surveillance, Suppression, and Mass Detention: Xinjiang’s Human Rights Crisis,” hearing, <https://www.cecc.gov/events/hearings/surveillance-suppression-and-mass-detention-xinjiangs-human-rights-crisis>; and Human Rights Watch, “China: Unrelenting Crimes against Humanity Targeting Uyghurs,” August 31, 2023, <https://www.hrw.org/news/2023/08/31/china-unrelenting-crimes-against-humanity-targeting-uyghurs>. Alex Joske, *Spies and Lies: How China’s Greatest Covert Operations Fooled the World* (Melbourne: Hardie Grant Books, 2022); Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis, MD: Naval Institute Press, 2019); “Alex Joske on How China’s Ministry of State Security Operates,” *The Wire China*, January 1, 2023, <https://www.thewirechina.com/2023/01/01/alex-joske-on-how-chinas-ministry-of-state-security-operates/>; Martin Purbrick, “The Long Arm of the Law(less): The PRC’s Overseas Police Stations,” *China Brief* 23, no. 11 (June 12, 2023), <https://jamestown.org/the-long-arm-of-the-lawless-the-prcs-overseas-police-stations/>. Cheryl Yu, “Harnessing the People: Mapping Overseas United Front Work in Democratic States” (Washington, DC: The Jamestown Foundation, February 11, 2026), <https://jamestown.org/harnessing-the-people-mapping-overseas-united-front-work-in-democratic-states/>; Safeguard Defenders, *110 Overseas: Chinese Transnational Policing Gone Wild* (Madrid: Safeguard Defenders, September 12, 2022), [https://safeguarddefenders.com/sites/default/files/pdf/110%20Overseas%20\(v5\).pdf](https://safeguarddefenders.com/sites/default/files/pdf/110%20Overseas%20(v5).pdf).

22. Drew Harwell and Eva Dou, “Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says,” *Washington Post*, December 8, 2020, <https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/>; Charles Rollet, “Hikvision Uyghur,” *IPVM*, November 11, 2019, <https://ipvm.com/reports/hikvision-uyghur>.

23. “China’s ‘Stability’ Norm Entrepreneurship: Taking Tibet Repression Globally,” International Campaign for Tibet, May 6, 2026, <https://savetibet.org/chinas-stability-norm-entrepreneurship/>.

24. “China’s ‘Stability’ Norm Entrepreneurship,” International Campaign for Tibet.

25. Human Rights Watch, “China: Alarming New Surveillance, Security in Tibet,” March 20, 2013, <https://www.hrw.org/news/2013/03/20/china-alarming-new-surveillance-security-tibet>.

26. Human Rights Watch, “China Poised to Repeat Tibet Mistakes,” January 20, 2017, <https://www.hrw.org/news/2017/01/20/china-poised-repeat-tibet-mistakes>.

27. Human Rights Watch, “Relentless: Detention and Prosecution of Tibetans under China’s ‘Stability Maintenance’ Campaign,” May 22, 2016, <https://www.hrw.org/report/2016/05/22/relentless/detention-and-prosecution-tibetans-under-chinas-stability-maintenance>.

28. “China’s ‘Stability’ Norm Entrepreneurship: Taking Tibet Repression Globally,” International Campaign for Tibet; and “Mass Surveillance and 5G in Tibet: Between Oppression and Espionage,” Tibet Policy Institute, 2020, <https://tibetpolicy.net/mass-surveillance-and-5g-in-tibet-between-oppression-and-espionage/>.

29. Turquoise Roof and Tibet Watch, “Weaponising Big Data: Decoding China’s Digital Surveillance in Tibet,” February 7, 2024, <https://turquoiseroof.org/weaponising-big-data-decoding-chinas-digital-surveillance-in-tibet/>.

30. Government of the United States. “Report: China Increasing Digital Surveillance of Tibetans,” *Voice of America, News*, February 7, 2024, <https://www.voanews.com/a/report-china-increasing-digital-surveillance-of-tibetans/7477574.html>.

31. C4ADS data holdings, available upon request.

32. As outlined in the methodology, a contract is classified as surveillance-related if it meets at least two of the terms listed in the Appendix.
33. C4ADS data holdings, available upon request.
34. Government of the United States, "Chairs Seek Export Controls on Technology Used for Mass Biometric Data," Congressional-Executive Commission on China, press release, October 23, 2023, <https://www.cecc.gov/media-center/press-releases/chairs-seek-export-controls-on-technology-used-for-mass-biometric-data>.
35. C4ADS data holdings, available upon request.
36. Human Rights Watch, "China: New Evidence of Mass DNA Collection in Tibet," September 5, 2022, <https://www.hrw.org/news/2022/09/05/china-new-evidence-mass-dna-collection-tibet>.
37. Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using AI to Profile a Minority," *New York Times*, May 22, 2019, <https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html>.
38. Tara Francis Chan, "How a Chinese region that accounts for just 1.5% of the population became one of the most intrusive police states in the world," *Business Insider*, July 31, 2018, <https://www.businessinsider.com/xianjiang-province-china-police-state-surveillance-2018-7>.
39. Newlines Institute for Strategy and Policy and Raoul Wallenberg Centre for Human Rights, *The Uyghur Genocide: An Examination of China's Breaches of the 1948 Genocide Convention* (Washington, DC, and Montreal, March 2021), <https://newlinesinstitute.org/intl-law-peace/the-uyghur-genocide-an-examination-of-chinas-breaches-of-the-1948-genocide-convention/>; Charles Rollet, "Dahua and Hikvision Win Over \$1 Billion In Government-Backed Projects In Xinjiang," IPVM, April 23, 2018, <https://ipvm.com/reports/xinjiang-dahua-hikvision>; and Charles Rollet, "Hikvision Growing Xinjiang Operations," IPVM, November 30, 2020, <https://ipvm.com/reports/hik-xinjiang>; and IPVM Team, "China Public Video Surveillance Guide: From Skynet to Sharp Eyes," IPVM, June 14, 2018, <https://ipvm.com/reports/sharpeyes>.
40. Government of the United States, "Ministerial to Advance Religious Freedom: Statement on China," U.S. Department of State, July 26, 2018, <https://2021-2025.state.gov/ministerial-to-advance-religious-freedom-statement-on-china/>.
41. Newlines Institute for Strategy and Policy and Raoul Wallenberg Centre for Human Rights, *The Uyghur Genocide: An Examination of China's Breaches of the 1948 Genocide Convention* (Washington, DC, and Montreal, March 2021), <https://static1.squarespace.com/static/5ab13c5c620b859944157bc7/t/6050f9851169a961976289c3/1615919497690/Chinas-Breaches-of-the-GC-1.pdf>; Uyghur Tribunal, "Summary Judgment," December 9, 2021, <https://uyghurtribunal.com/wp-content/uploads/2021/12/Uyghur-Tribunal-Summary-Judgment-9th-Dec-21.pdf>; Human Rights Watch, "China: How Mass Surveillance Works in Xinjiang," May 1, 2019, <https://www.hrw.org/news/2019/05/01/china-how-mass-surveillance-works-xinjiang>; Danielle Cave et al., "Uyghurs for Sale," Australian Strategic Policy Institute, March 1, 2020, <https://www.aspi.org.au/report/uyghurs-sale>; United Nations, *OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China*, UN Office of the High Commissioner for Human Rights, August 31, 2022, <https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf>; and Matthew Hill, David Campanale, and Joel Gunter, "Uyghurs: 'Credible Case' China Carrying Out Genocide," *BBC News*, February 2, 2021, <https://www.bbc.com/news/world-asia-china-55794071>.
42. Uyghur Tribunal, "Judgment," December 9, 2021, <https://uyghurtribunal.com/>; Conor Healy, "Hikvision, Xinjiang, Uyghurs & Human Rights Abuses – White Paper," IPVM, October 17, 2023, <https://ipvm.com/reports/hikvision-wp>; Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *The New York Times*, May 22, 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html?eafs_enabled=false; and Uyghur Tribunal, "Summary Judgment, para. 170."
43. Independent Tribunal into Forced Organ Harvesting from Prisoners of Conscience in China, "Judgment," March 1, 2020, <https://chinatribunal.com/final-judgment/>; and Matthew Hill, David Campanale, and Joel Gunter, "'Their Goal Is to Destroy Everyone': Uighur Camp Detainees Allege Systematic Rape," *BBC News*, February 2, 2021, <https://www.bbc.com/news/world-asia-china-55794071>.
44. C4ADS data holdings, available upon request.
45. As outlined in the methodology, a contract is classified as surveillance-related if it meets at least two of the terms listed in the Appendix.
46. U.S. Department of Commerce, Bureau of Industry and Security, "Addition of Entities to the Entity List," *Federal Register*, December 11, 2024, <https://public-inspection.federalregister.gov/2024-29136.pdf>.
47. Uniview, "About Us: Company," accessed September 1, 2026, https://www.uniview.com/About_Us/Company/.
48. C4ADS data holdings, available upon request.
49. "Analysis of XUAR surveillance-related contract terms, 2022–2026," C4ADS data holdings, available upon request. While the statistical overview provided in earlier stages represents a general brushstroke against the data, projects may not overtly mention biometric data capabilities and therefore were not included; however, that does not mean they do not exist. The following details from other projects in this dataset illustrate that, as of 2022, according to Chinese government documents, Hikvision, Uniview, and other sanctioned companies continued to provide services to surveillance-related projects in XUAR. In fact, one of the projects that features Hikvision technology also leverages GPUs designed by U.S. companies (these GPUs fall below export control thresholds but can be used to empower AI tools). A Hikvision project that mentions surveillance and potentially can analyze biometric data, also boasts the following technical details, "supports manual selection of tracking targets and maintains continuous, stable tracking for a set duration, supports automatic switching between multiple tracking targets; target switching time is less than 1 second." In this particular project, Hikvision

serves the XPCC with the following services: “functions related to mobile tags – including but not limited to targets with GPS signals such as individual personnel, inspection vehicles, and low-altitude surveillance vehicles – allowing for real-time display on the monitoring screen and the execution of operational applications. These allow for the automatic or manual detection of behaviors such as area intrusion, line crossing, and entering or exiting a zone. The system can trigger alarms and coordinate PTZ tracking, thereby meeting high-level security requirements.”

50. WireScreen; U.S. Department of the Treasury, Office of Foreign Assets Control, “Xinjiang Supply Chain Business Advisory,” July 13, 2021, https://ofac.treasury.gov/system/files/126/20210713_xinjiang_advisory_0.pdf.

51. Uyghur Human Rights Sanctions Review Act, S. 585, 118th Cong. (March 1, 2023), <https://www.congress.gov/bill/118th-congress/senate-bill/585/text>.

52. C4ADS data holdings, available upon request.

53. C4ADS data holdings, available upon request; and Emile Dirks and James Leibold, *Genomic Surveillance* (Canberra: Australian Strategic Policy Institute, June 17, 2020), <https://www.aspi.org.au/report/genomic-surveillance/>.

54. WireScreen, search terms: “smart exploration apps,” “data verification systems,” “DNA laboratory management systems,” “investigation systems,” “sound and audio detection,” “forensic identification systems,” “net exploration software,” “mobile evidence collection devices,” and “digital detection cloud capture services.”

55. Dirks and Leibold, *Genomic Surveillance* (Canberra: ASPI, June 17, 2020).

56. WireScreen, overseas investment records: United States: Harbin Wright Brothers Technology Development Company Limited American Branch (哈尔滨莱特兄弟科技开发有限公司美国分公司), Aiden Systems (艾登系统公司), Touch Infinite Technology (USA) Limited Liability Company (触景无限科技(美国)有限责任公司), and Shuimu Future (USA) Technology Company Limited (水木未来(美国)科技有限公司); Germany: Top Europe Limited (泰璞欧洲有限公司); Singapore: Zhiyu Technology Company Limited (智誉科技有限公司); Netherlands: Wright Brothers Flight Technologies Netherlands Branch (莱特兄弟飞行技术荷兰分公司); and Canada: Time Technology Company Limited (时间科技有限公司).

57. WireScreen.

58. C4ADS data holdings, available upon request. All contract-description claims are drawn from this source unless otherwise specified.

59. “Cadre Materials,” Xinjiang Documentation Project, University of British Columbia, accessed September 1, 2026, <https://xinjiang.sppga.ubc.ca/chinese-sources/cadre-materials/p25154/>.

60. Baidu Baike, s.v. “智器云南京信息科技有限公司” (Zhiqi Cloud Nanjing Information Technology Co., Ltd.), accessed September 1, 2026, <https://baike.baidu.com/item/%E6%99%BA%E5%99%A8%E4%BA%91%E5%8D%97%E4%BA%AC%E4%BF%A1%E6%81%AF%E7%A7%91%E6%8A%80%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8>. (Note: during research for this report, Chinese-language sources of this kind could not be archived via the Wayback Machine or saved as PDFs, suggesting increasingly sophisticated efforts to restrict access to this material.)

61. “情报分析领军企业智器云完成近5000万B轮融资” (Leading intelligence analysis company Zhiqiyun completes nearly 50 million yuan Series B financing), 甲子光年 (Jazzyyear), July 30, 2021, archived September 10, 2026, https://web.archive.org/web/20260910130752/https://www.jazzyyear.com/article_info.html?id=402.

62. WireScreen.

63. WireScreen; and OpenSanctions, “Canada National Research Organizations List,” accessed September 1, 2026, https://www.opensanctions.org/datasets/ca_named_research_orgs/; and U.S. Department of Commerce, Bureau of Industry and Security, “Additions and Revisions to the Entity List,” *Federal Register*, September 16, 2025.

64. “High-Tech Suppression of China’s Mongol Region Provokes Protests,” *Mind Matters*, September 2020, <https://mindmatters.ai/2020/09/high-tech-suppression-of-chinas-mongol-region-provokes-protests/>; PEN America, *Inner Mongolia: China’s Culture of Repression* (New York: PEN America, January 20, 2026), <https://pen.org/report/inner-mongolia-china-repression/>; and “China’s Inner Mongolia Cracks Down on Bilingual Education amid Assimilation Fears,” *Los Angeles Times*, September 3, 2020, <https://www.latimes.com/world-nation/story/2020-09-03/china-inner-mongolia-bilingual-education-assimilation-xinjiang-resistance-crackdown>.

65. PEN America, *Inner Mongolia: China’s Culture of Repression*; and Southern Mongolian Human Rights Policy Act, S. 5305, 118th Cong. (2024), <https://www.govinfo.gov/content/pkg/BILLS-118s5305is/html/BILLS-118s5305is.htm>.

66. PEN America, *Inner Mongolia: China’s Culture of Repression*.

67. PEN America, *Inner Mongolia: China’s Culture of Repression*; Southern Mongolian Human Rights Policy Act, S. 5305, 118th Cong. (2024); and “High-Tech Suppression of China’s Mongol Region Provokes Protests,” *Mind Matters*.

68. Minority Rights Group International, “Mongols,” accessed September 1, 2026, <https://minorityrights.org/communities/mongols/>; “Pastoralism and the State in China’s Inner Mongolia,” *Current History* 120, no. 827 (2021), <https://online.ucpress.edu/currenthistory/article/120/827/227/118337/Pastoralism-and-the-State-in-China-s-Inner>.

69. C4ADS data holdings, available upon request.

70. C4ADS data holdings, available upon request.

71. U.S. Department of Commerce, Bureau of Industry and Security, “Addition of Certain Entities to the Entity List,” *Federal Register*, October 9, 2019.

72. WireScreen.

73. C4ADS data holdings, available upon request.
74. Hebei Brilliance Technology Development Co., Ltd. (河北博士林科技开发有限公司), corporate website, accessed September 1, 2026, <http://www.briltech.com.cn/>, and “About,” accessed September 1, 2026, <http://www.briltech.com.cn/?about/>.
75. WireScreen.
76. C4ADS data holdings, available upon request.
77. C4ADS data holdings, available upon request.
78. C4ADS data holdings, available upon request.
79. C4ADS data holdings, available upon request.
80. C4ADS data holdings, available upon request.
81. C4ADS data holdings, available upon request.
82. C4ADS data holdings, available upon request.
83. C4ADS data holdings, available upon request.
84. C4ADS data holdings, available upon request.
85. C4ADS data holdings, available upon request.
86. C4ADS, “Do As I Say, Not As I Do: Foreign Supply of Repressive Equipment to Hong Kong,” March 16, 2023, <https://c4ads.org/commentary/doasisaynotasido/>; and “Hong Kong Court Convicts 47 Pro-Democracy Activists,” *BBC News*, <https://www.bbc.com/news/world-asia-china-52765838>.
87. Susan V. Lawrence and Michael F. Martin, China’s National Security Law for Hong Kong: Issues for Congress, CRS Report R46473 (Washington, DC: Congressional Research Service, August 3, 2020), https://www.congress.gov/crs_external_products/R/PDF/R46473/R46473.2.pdf.
88. U.S. Department of State, Bureau of East Asian and Pacific Affairs, *2024 Hong Kong Policy Act Report*, March 2024, <https://www.state.gov/bureau-of-east-asian-and-pacific-affairs/releases/2024/03/2024-hong-kong-policy-act-report>.
89. U.S. Department of State, Bureau of East Asian and Pacific Affairs, *2024 Hong Kong Policy Act Report*.
90. Amnesty International, “Hong Kong: Arbitrary Arrests, Brutal Beatings, and Torture in Police Detention Revealed,” September 2019, <https://www.amnesty.org/en/latest/press-release/2019/09/hong-kong-arbitrary-arrests-brutal-beatings-and-torture-in-police-detention-revealed/>.
91. Hong Kong Democracy Council, “Hong Kong Political Prisoners,” accessed September 1, 2026, <https://www.hkdc.us/hong-kong-political-prisoners>.
92. C4ADS data holdings, available upon request. “Hong Kong to Install Surveillance Cameras with AI Facial Recognition,” *Hong Kong Free Press*, October 4, 2025, <https://hongkongfp.com/2025/10/04/hong-kong-to-install-surveillance-cameras-with-ai-facial-recognition/>; “Hong Kong to Increase the Number of Facial Recognition Cameras,” *Biometric Update*, October 2025, <https://www.biometricupdate.com/202510/hong-kong-to-increase-the-number-of-facial-recognition-cameras>; and “Hong Kong Police to Deploy Facial Recognition in CCTV,” *Facia.ai*, <https://facia.ai/news/hong-kong-police-to-deploy-facial-recognition-in-cctv/>.
93. Hong Kong Police Force, “News,” <https://www.police.gov.hk/offbeat/615/news1.html>; and “Gemalto Technologies Asia Limited,” LT Directory, <https://www.ltdir.com/companies/gemalto-technologies-asia-limited/>.
94. *Hong Kong Government Gazette*, notice no. 20212530, accessed September 1, 2026, <https://egazette.gld.gov.hk/pdfjs/web/viewer.html?file=https%3A%2F%2Fegazette.gld.gov.hk%2Fos%2Fgazette%2F20212530%2Fegn202125304755.pdf>.
95. Thales Group, “List of Non-French Companies Held by Thales as of 30 June 2025,” June 2025, <https://www.thalesgroup.com/sites/default/files/2025-09/List-of-non-French-companies-held-by-Thales-2025-06-EN.pdf>. Thales Group, “Thales Completes Acquisition of Gemalto to Become Global Leader in Digital Identity,” news release, April 2, 2019, <https://www.thalesgroup.com/en/news-centre/press-releases/thales-completes-acquisition-gemalto-become-global-leader-digital>; Thales Group, “Homepage,” accessed September 1, 2026, <https://www.thalesgroup.com/en>; and “Thales Digital Identity and Security (DIS),” Infinigate, accessed September 1, 2026, <https://www.infinigate.com/vendors/thales-digital-identity-and-security-dis/>.
96. Thales Group, “Thales Digital Identity and Security (DIS),” Infinigate; Thales Group, “Cyber and Digital,” accessed September 1, 2026, <https://www.thalesgroup.com/en/about-thales/cyber-and-digital>.
97. C4ADS data holdings, available upon request.
98. *Hong Kong Government Gazette*, notice no. 20242804, accessed September 1, 2026, <https://egazette.gld.gov.hk/pdfjs/web/viewer.html?file=https%3A%2F%2Fegazette.gld.gov.hk%2Fos%2Fgazette%2F20242804%2Fegn20242804560.pdf>.
99. C4ADS data holdings, available upon request.
100. C4ADS data holdings, available upon request.
101. *Hong Kong Government Gazette*, notice no. 20252917, accessed September 1, 2026, <https://egazette.gld.gov.hk/pdfjs/web/viewer.html?file=https%3A%2F%2Fegazette.gld.gov.hk%2Fos%2Fgazette%2F20252917%2Fegn202529172591.pdf>.
102. International Security Technology Limited, “About Us,” accessed September 1, 2026, https://en.ist-china.com/en_about/65.html; “Contact,” accessed September 1, 2026, https://en.ist-china.com/en_contact/81.html.
103. International Security Technology Limited, “News,” accessed September 1, 2026, https://en.ist-china.com/en_news/show/82.html.
104. ChinaFile, “Methodology,” <https://www.chinafile.com/methodology>; ChinaFile, “State Surveillance in China,” <https://www.chinafile.com/state-surveillance-china>; and ChinaFile, “Message Control in China: Methodology,” all accessed September 1, 2026, <https://www.chinafile.com/message-control-china-methodology>.

105. Dahlia Peterson, Center for Security and Emerging Technology, *Designing Alternatives to China's Surveillance State* (Washington, DC: Georgetown University, CSET), October 2020, <https://cset.georgetown.edu/wp-content/uploads/CSET-Designing-Alternatives-to-Chinas-Surveillance-State.pdf>.
106. Dahlia Peterson, "How China Harnesses Data Fusion to Make Sense of Surveillance Data," Brookings Institution, September 23, 2021, <https://www.brookings.edu/articles/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/>.
107. Human Rights Watch, "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," May 1, 2019, <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass>.
108. Pengxiang Liang, Xiaohan Li, and Yuanyuan Guo, "Local Governments and the Diffusion of Video Surveillance in China: Evidence from Public Procurement Contracts," *Journal of Chinese Political Science* 30 (2025): 421–447, <https://link.springer.com/article/10.1007/s11366-025-09916-7>.
109. Björn Alpermann, "From Seeing to Understanding: How Public Surveillance Targets Uyghurs with AI Cameras throughout China," Remote Ethnography XUAR, July 2, 2024, <https://www.remote-xuar.com/post/from-seeing-to-understanding-how-public-surveillance-targets-uyghurs-with-ai-cameras-throughout-c>.
110. Emile Dirks and James Leibold, "Genomic Surveillance," Australian Strategic Policy Institute, June 17, 2020, <https://www.aspi.org.au/report/genomic-surveillance/>; and Danielle Cave, Samantha Hoffman, Fergus Ryan, and Elise Thomas, "Mapping China's Tech Giants," Australian Strategic Policy Institute, April 18, 2019, <https://www.aspi.org.au/report/mapping-chinas-tech-giants/>.

