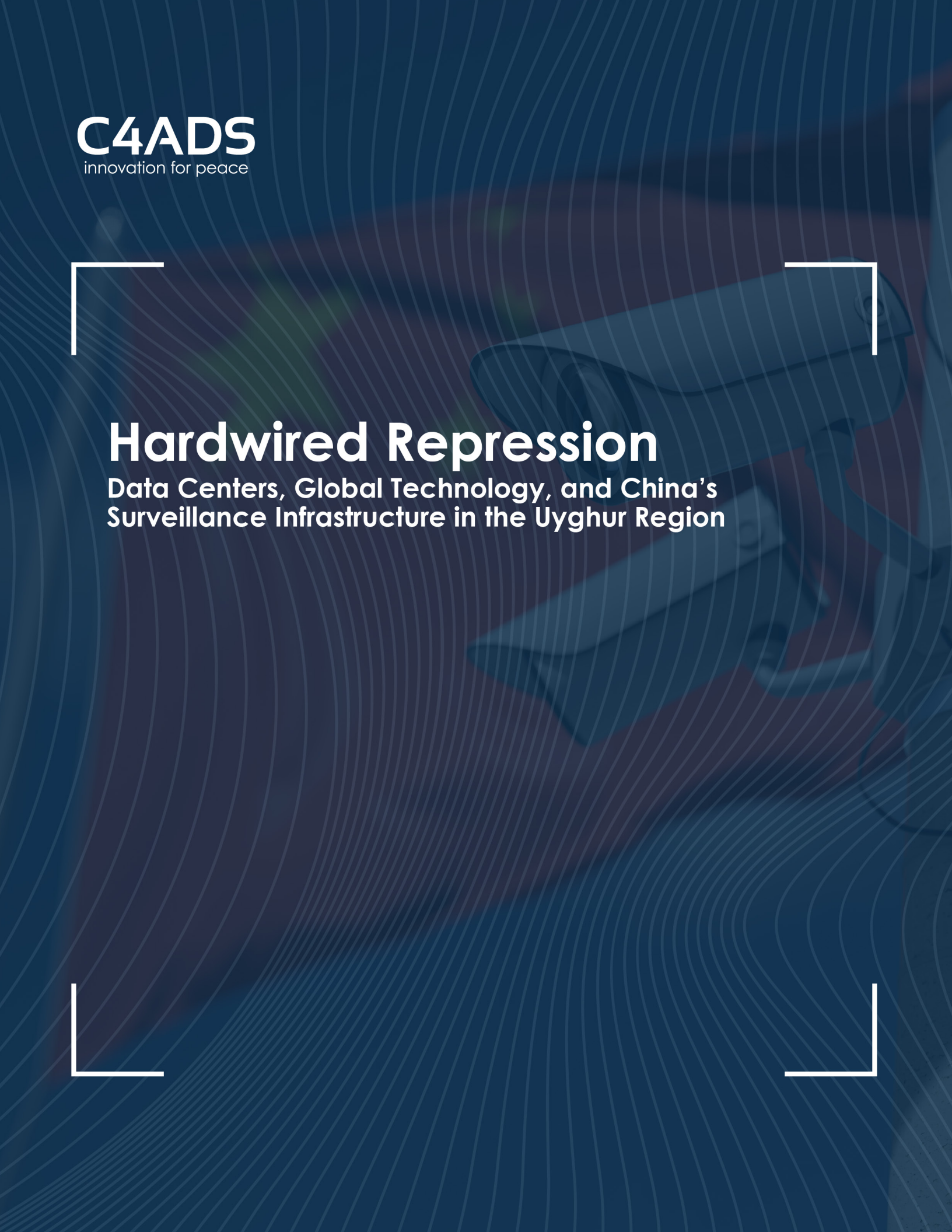
C4ADS
innovation for peace

Hardwired Repression

Data Centers, Global Technology, and China's Surveillance Infrastructure in the Uyghur Region



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.

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 analyzes PRC-linked activities and developments related to critical minerals, emerging technologies, artificial intelligence (AI) chip smuggling, surveillance technology, 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, and National Cheng Kung University in Taiwan.

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.

Acknowledgments

C4ADS would like to thank all those who provided guidance, time, and support during this project, including current and former C4ADS staff. Special thanks to Jacob Feldgoise, Senior Data Research Analyst, Center for Security and Emerging Technology (CSET). C4ADS is also grateful to its technology partners, whose software and systems were integral to the project's success.

aws wire|screen

Table of Contents

Executive Summary

The People's Republic of China (PRC) operates one of the most expansive mass surveillance systems in the world, and data centers are its foundation. These facilities provide the physical infrastructure that stores, processes, and acts on the biometric data, communications records, and behavioral patterns used to monitor citizens, especially ethnic minorities. Despite significant international attention to forced labor, atrocity crimes, and surveillance in the Uyghur region, the digital backbone enabling those abuses has received comparatively little scrutiny.

Beijing's "Eastern Data, Western Computing" initiative has accelerated this buildout, and the Chinese Communist Party (CCP) has designated the region a "crucial component" of the Belt and Road Spatial Information Corridor, with plans to use the data centers in the Uyghur region to extend Chinese data infrastructure into Central Asia. The region simultaneously functions as a testing ground for digital authoritarianism: government records reveal comprehensive digitization of medical, educational, judicial, and administrative systems, with surveillance triggers that include indications of ethnic identity. Individuals identified as high risk can face interrogation, coercive labor, or detention.

Two case studies illustrate the global dimensions of this infrastructure. The first examines the Yanqi Vocational Technical School, operated by the Xinjiang Production and Construction Corps (XPCC), a sanctioned paramilitary organization. A 2024 government contract reveals that U.S. technology – including processors, graphics cards, and facial recognition hardware – tracks students' movements, meals, and curfew compliance in real time. Vocational schools in the Uyghur region have drawn criticism as sites of indoctrination, forced assimilation, and detention. The required semiconductors ("chips") specified in these documents fall below the threshold for export-controlled AI chips, revealing a critical gap: current controls do not adequately address the PRC's surveillance technology pipeline. The second case study examines China Telecom Xinjiang, a subsidiary of a U.S.-sanctioned state-owned enterprise that operates at least four data centers in the region. The subsidiary holds active contracts with the XPCC and provides services to entities designated as military or intelligence agencies – activity its parent company's OFAC listing has not prevented. Meanwhile, China Telecom, the sanctioned parent company, claims to still operate data centers in the United States.

C4ADS's analysis of 2024-2025 Xinjiang Uyghur Autonomous Region (XUAR) government documents found references to American and Taiwanese technology across data center projects in the region. Whether above or below export control thresholds, American and Taiwanese technology continues to flow into surveillance infrastructure targeting a population subject to documented atrocity crimes. Meaningful change will require action beyond the corporate level. C4ADS recommends adding China Telecom and its provincial subsidiaries to the Commerce Department's Entity List and mandating post-shipment verification for dual-use technology exports destined for regions with documented records of atrocity crimes – with clearer liability standards for exporters whose hardware reaches military or intelligence-affiliated end users.

Introduction: China's Surveillance Infrastructure

The People's Republic of China (PRC) operates one of the most documented and expansive mass surveillance systems in the world, and at its foundation is a critical but often overlooked piece of infrastructure: data centers.[1]

The country's digital surveillance apparatus continuously monitors the population, including through an estimated 700 million facial recognition cameras.[2] In the Uyghur region,[3] authorities subject people to heightened monitoring, including at checkpoints, through Wi-Fi sniffers, and via biometric data collection, with data centralized and processed via platforms such as the Integrated Joint Operations Platform (IJOP).[4] System triggers include indications of ethnic identity – for example, whether an individual "looks Uyghur."[5] Individuals identified as high risk can face interrogation, coercive labor, or detention.[6]

The Uyghur region also serves as a laboratory for digital authoritarianism. Government records on data center projects reveal comprehensive digitization of medical, administrative, judicial, and educational systems, with unified data platforms, artificial intelligence (AI)-enhanced decision-making, state-controlled encryption, and significant reliance on domestic technology.[7] The PRC uses the Uyghur region as a testing ground for digital surveillance, modernized policing, and information integration, creating a governance model that Beijing exports worldwide, along with the enabling technologies.[8]

Since 2017, China has detained millions of Uyghurs in so-called "vocational education and training centers" as part of its campaign that the United States and others have designated a genocide.[9] That system has since evolved. The highly visible, militarized internment camps, surrounded by armed guards and watchtowers, were gradually wound down around 2019-2020, not as a sign of easing repression, but as a tactical shift in accordance with China's long-term strategy in the region.[10] The Chinese Communist Party (CCP) did not reduce coercion;[11] it restructured it into a more diffuse and economically integrated forced labor apparatus.[12] This shift from overt internment to embedded economic coercion forms the backdrop for this report..

The surveillance system's continued expansion depends on data centers – physical facilities that house the large-scale computing hardware required to process the large quantities of data the system generates. They range from small server closets to hyperscale facilities spanning millions of square feet.[13] The larger facilities require substantial energy and supporting infrastructure, including high-capacity electricity, internet connectivity, backup systems, and robust cooling systems to manage heat generation.[14]

This analysis focuses on data centers in the Uyghur region.[15] State-sponsored forced labor and other atrocity crimes in the Uyghur region are well documented and have tainted global supply chains in some of the most strategic industries, including conflict minerals, pharmaceuticals, solar-grade polysilicon, and electric vehicles.[16] Less understood, however, is the surveillance apparatus that enables these abuses: the system relies on a digital backbone that extends far beyond cameras and checkpoints. Data centers, which incorporate Western technology, process vast quantities of biometric data, communications records, and behavioral patterns, forming the technological foundation for the systematic monitoring of Uyghur and other ethnic minorities, both in the Uyghur region and across the PRC.[17]

This investigation examines some of the companies building, operating, and maintaining data centers in the Uyghur region, as well as their ties to the Chinese state, military, police, and intelligence apparatus. It also examines whether and how Western technology continues to flow into this infrastructure, despite export controls and sanctions regimes. Through two case studies, the investigation illustrates how data centers enable surveillance at scale within China, and how the participating companies and input technologies rely on global supply chains.

The analysis begins with an examination of how the PRC has incorporated the Uyghur region into its broader authoritarian digital infrastructure, including through the integration of American and Taiwanese technology in pursuit of global technological primacy. The report concludes with an assessment of broader implications for human rights, global technology markets, and regulatory frameworks, followed by a set of recommendations for government, private-sector, and civil society actors.

Methodology and Limitations

The analysis draws on a review of approximately 420,000 projects approved in the Uyghur region by local Xinjiang Uyghur Autonomous Region (XUAR) authorities and the Xinjiang Production and Construction Corps (新疆生产建设兵团), or XPCC. C4ADS identified projects mentioning data centers or "数据中心."[18] XPCC is a paramilitary organization that operates as a quasi-state entity and controls significant portions of the region's economy. Throughout this paper, "Uyghur region" refers to XUAR, unless the context requires reference to existing legal structures, such as governments and financial entities.

C4ADS mapped the corporate actors collaborating with local government and paramilitary authorities to build, operate, and maintain these data centers, as well as their connections to U.S. and other non-PRC companies. This analysis helped reveal the role that global technology plays in China's authoritarian infrastructure.

The first case study focuses on a so-called "vocational technical school" and was selected for its close connections to the XPCC to illustrate the nexus between data centers and known surveillance actors.

The second case study focuses on China Telecom's Xinjiang subsidiary, China Telecom Xinjiang (中国电信股份有限公司新疆分公司). C4ADS selected it for its size, volume of mentions in government documents, and ties to the Chinese defense industry. The case study examines its ties to U.S. and global technology companies to demonstrate that U.S. technology remains integral to Chinese data centers – and by extension, to China's surveillance architecture – despite international sanctions and export controls.

The case studies illustrate specific examples rather than comprehensive trends; readers should not extrapolate broader patterns from them. China's restrictive information environment limits publicly available evidence of coercive land transfers, environmental harms, or adverse impacts of energy development related to data center construction. However, other sources have documented ongoing coercive land transfers in the region and the absence of such evidence or its discussion here does not indicate that such practices are absent from this industry.[19]

Eastern Data, Western Computing

In 2022, Beijing officially launched the "Eastern Data, Western Computing" (EDWC, 东数西算) initiative to build eight major data center hubs across China.[20] These hubs include the Beijing-Tianjin-Hebei Metropolitan Region, the Yangtze River Delta, the Guangdong-Hong Kong-Macau Greater Bay Area in eastern China, the Chengdu-Chongqing region, Guizhou, Inner Mongolia, Gansu, and Ningxia in central and western China.[21] Although the XUAR and the Tibetan Autonomous Region (TAR, or Tibet) are not named in the EDWC, the policy's influence is evident across the country, and local officials often use central government initiatives as justification to pursue related projects.[22] Since its launch, data center development has accelerated in western border regions,[23] including the XUAR and Tibet, driven by provincial and central authorities drawing on the EDWC framework.[24] AI's rapidly advancing processing demands will only accelerate this trend.

The coordinated party-state effort advances Chinese President Xi Jinping's push to build a "digital China" by capitalizing on the western regions' abundant energy resources to supply computing power to the country's eastern economic hubs.[25] The strategy also pushes these resource-intensive data centers away from major population centers, shifting the associated displacement and pollution to vulnerable populations in the periphery.[26] Though discussions around such a plan began as early as 2000, AI's massive energy demands expedited its implementation.[27] By integrating data governance, AI infrastructure, and energy policy under one national framework, the EDWC creates the infrastructure conditions that make digital surveillance at scale viable.[28]

The Uyghur Region as a Laboratory for Digital Authoritarianism

The Uyghur region's sparsely populated land offers ample physical space for large-scale facilities that would be difficult to develop in China's more densely populated regions. The region's colder temperatures reduce the energy required to cool data center hardware, one of the most significant operational costs of running such facilities.[29] While these remote facilities face latency issues for many commercial applications in the eastern hubs of the country,[30] they are well-suited for the computationally intensive work of training algorithms, including those powering China's predictive policing and social control systems.[31]

Domestically, Chinese local governments incentivize companies through subsidies and land access to rapidly construct data centers across the country.[32] The computational intensity of training these models makes energy-rich western regions attractive, despite their distance from end users.

The Uyghur region and Tibet are the two westernmost regions in the country, and researchers have documented a deliberate feedback loop in which surveillance initiatives first piloted in Tibet have been imposed in the Uyghur region, and intrusive measures that debuted in the Uyghur region were subsequently applied back to Tibet.[33]

As of 2025, XPCC owned and operated several of the data centers in the Uyghur region.[34] A paramilitary economic organization operating under direct central government authority, XPCC holds a special administrative status in the Uyghur region and runs cities, farms, and companies, while providing education, policing, and other governance functions for the areas under its control.[35] Its role in the region's security apparatus and involvement in industries linked to forced labor allegations have drawn significant international scrutiny. The United States, the United Kingdom, Canada, the EU, and Australia have sanctioned XPCC for its role in the persecution of the Uyghur population.[36] Despite these sanctions, C4ADS found that XPCC continues to require compatibility with Western technology in its infrastructure.

The region is also central to China's push for global technological dominance. The CCP has designated Uyghur region infrastructure a "crucial component" of the Belt and Road Spatial Information Corridor.[37] Bordering eight countries, the region anchors the PRC's Digital Silk Road ambitions,[38] as the critical node for cross-border fiber optic networks, data flows, and telecommunications infrastructure connecting China to Central Asia and beyond.[39] Chinese tech giants have established cloud computing hubs and 5G networks that extend Beijing's digital standards and governance models westward.[40]

The PRC does not even need to directly export its model to influence data sovereignty beyond its borders. The CCP plans to utilize data centers in the Uyghur region to serve Central Asian countries, deepening regional dependence on its data infrastructure and enabling cross-border data processing services.[41] This arrangement raises concerns over the data sovereignty of the jurisdictions those centers serve. Meanwhile, some Chinese companies involved in data center development are now expanding internationally while obscuring their connections to Chinese state-owned entities (SOEs) – for example, by restructuring through Cayman Islands' holding companies or other secrecy jurisdictions – raising concerns about data sovereignty and security in Central Asia, Southeast Asia, and other markets where they establish facilities.[42] Under PRC law, Chinese SOEs can be compelled to provide data to the Chinese government, meaning that data stored in these facilities – even if located outside China – may be accessible to Beijing.[43]

Case Study 1: Yanqi Vocational Technical School Smart Campus

Government surveillance programs targeting Uyghurs and other ethnic minorities in the Uyghur region have drawn global condemnation; vocational schools, in particular, face criticism as sites of indoctrination and forced assimilation.[44] At Yanqi Vocational Technical School, every aspect of student life – attendance, meals, social interactions, dorm movements, and schedule compliance – is tracked, analyzed, and stored in databases linking behavior to performance.[45] This monitoring relies on Western technology, with biometric systems powered by Intel processors and Nvidia GPUs, exemplifying how imported technologies continue to enable the repression of vulnerable populations.[46]

Yanqi's smart campus project illustrates how data centers function as a fundamental part of the surveillance infrastructure. Surveillance requires active collection, processing, and storage of vast streams of information from campus sensors and cameras, enabling sophisticated surveillance and predictive policing. Data centers provide the critical infrastructure for such large-scale storage and processing. In October 2024, the Yanqi school in the Uyghur region's Yanqi Hui Autonomous County contracted for a 796,900 RMB (US$113,000) "Smart Campus" surveillance system.[47] The project, which was to be completed by March 2025,[48] demonstrates the continued central role of global technology in enabling Chinese surveillance, despite sanctions and international condemnation of the CCP's human rights violations.[49]

C4ADS' analysis of Chinese government documents shows that the platform that generates attendance reports for students entering and leaving the dormitory building specifies Nvidia GeForce RX 4060 and AMD Radeon RX 7600 graphics cards as options, as well as Hikvision surveillance hardware.[50] The documentation also shows Nvidia RTX3050 6GB required for the video editing machine.[51] The project implements international and Chinese technology for the purpose of "dormitory management."[52] Nvidia RTX 4060, RTX 3050 6GB, and AMD RX 7600 sit below the performance threshold of high-performance AI chips and have not been subject to export control restrictions.[53]

While the chips used in the Yanqi surveillance system were not subject to export controls, the fact that they are integral to surveillance systems undermines the common assumption that export controls adequately address the surveillance technology pipeline. In other words, the fact that unrestricted chips are leveraged for monitoring purposes highlights another fundamental enforcement problem: once a chip is sold, ensuring that it reaches only its declared buyer and is not resold, rerouted, or repackaged is extraordinarily difficult in practice.

Project details also reveal the integration of dormitory check-ins, cafeteria access, and physical movements within the campus into a connected system that tracks and logs individual student activity.[54] The system deploys 15 Hikvision facial recognition devices across campus: five terminals controlling cafeteria access and 10 managing building entry. Each device maintains a 50,000-face database, processes identifications in under 0.2 seconds, includes anti-spoofing technology to prevent photo impersonation, and automatically generates alerts with photographic evidence when students violate curfews or access restrictions.[55] The

automated dormitory monitoring system doesn't merely record movements but actively checks for compliance, transmitting real-time alerts containing photos and complete student information whenever someone breaks the routine.[56]

The hardware specifications of this project reveal pervasive dependence on non-Chinese technology. Ten ASUS desktop computers powered by Intel Core i5-13490F processors and Nvidia GeForce RTX 4060 Ti graphics cards handle AI-powered facial recognition processing. A sophisticated video editing workstation features an Intel Core i7-12700 processor, an Nvidia RTX 3050 graphics card, and a massive 64 TB RAID storage array built from eight enterprise-grade hard drives. The Hikvision facial recognition terminals enable real-time video transmission, central monitoring, and automated behavioral alerts.[57]

Case Study 2: China Telecom Co., LTD Xinjiang

China Telecom Xinjiang offers a prominent example of how telecommunications companies can become vectors for human rights abuses and entanglement with China's defense industry.[58] The company's involvement in data center projects in the Uyghur region illustrates how the line between commercial and government service providers has been dissolved in China's surveillance economy. For international companies and democratic governments, this creates an unavoidable problem: engagement on commercial terms is inseparable from complicity in documented human rights violations and exposure to state sanctions, exposing global markets to significant risks.

China Telecom's Global Footprint

China Telecom Xinjiang is a wholly owned subsidiary of China Telecom Corporation Limited (China Telecom). China Telecom is an SOE with close ties to the PRC's military-industrial complex; it is also one of the largest internet and phone service providers in the world.[59] China Telecom is majority owned by China Telecommunications Corporation, a cloud operator approved by the Cyberspace Administration of China, indicating that it has undergone the security assessment mandated for operators serving Chinese government agencies and critical infrastructure.[60] China Telecom is also part of China's quantum industry and is considered one of the top AI companies in China.[61]

Such layered structures of SOEs obscure the boundary between commercial and state actors in China. Both state and commercial entities may be complicit in human rights violations or subject to export controls and state sanctions; complex ownership structures complicate due diligence. Before 2021, many global investment funds, including BlackRock, held investments in China Telecom.[62] In 2021, the United States added China Telecom to the Department of the Treasury's Office of Foreign Assets Control's (OFAC's) Chinese Military Industrial Complex Companies List,[63] which prohibits U.S. persons from trading in the company's publicly listed securities, and to the U.S. General Services Administration's System for Award Management (SAM) Exclusion List, which bars the company from receiving U.S. government contracts.[64] As a result, China Telecom was delisted from the New York Stock Exchange, and BlackRock and other foreign investors divested the majority of their stakes in 2021.[65]

Critically, however, neither designation restricts China Telecom from investing in or operating infrastructure within the United States; that would fall under the separate purview of the Committee on Foreign Investment in the United States. According to its website, the company appears to continue operating data centers in the United States,[66] suggesting a potential gap in the overall regulatory framework governing Chinese military-affiliated entities on U.S. soil. China Telecom also maintains active branches in Europe and Australia.[67]

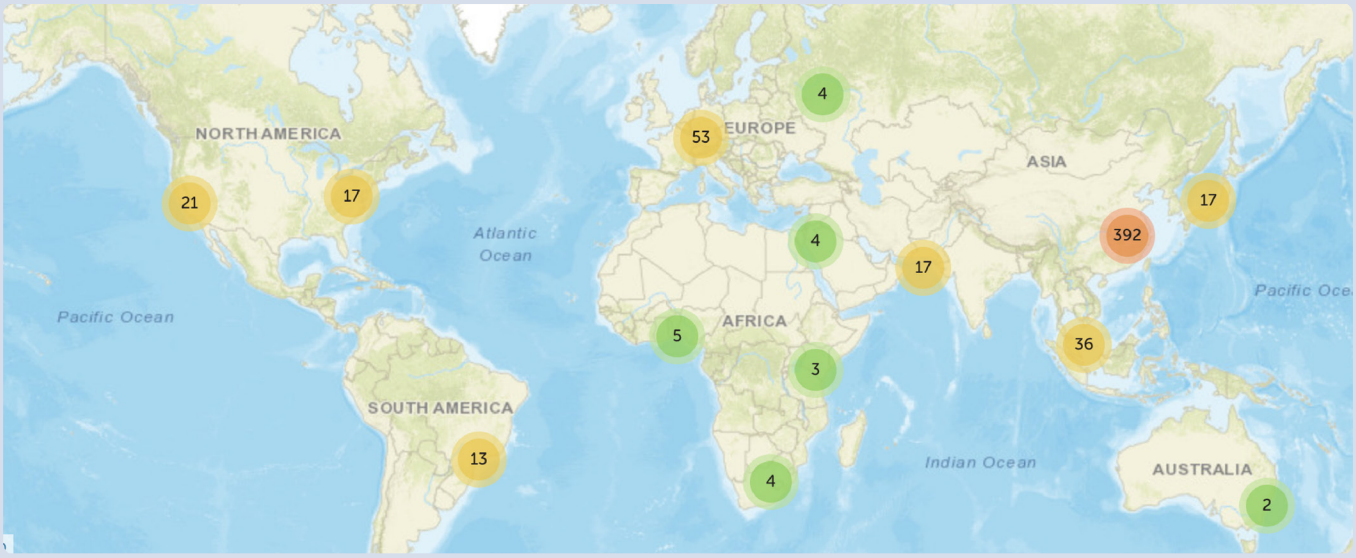


Figure 1: China Telecom Global Data Center Operations[68]

China Telecom Xinjiang operates as a separate legal entity from its parent company. Unlike OFAC's Specially Designated Nationals List, in which the '50% rule' automatically extends restrictions to subsidiaries majority owned by a listed entity, the restrictions applied to China Telecom do not automatically extend to all subsidiaries.

As of March 2026, China Telecom operates at least four data centers in the Uyghur region, located in Aksu, Urumqi, Hami, and Korla.[69] It provides both commercial and government services in the Uyghur region, raising concerns that seemingly neutral technology services may directly support state security systems. For example, China Telecom Xinjiang continues to participate in "poverty alleviation" schemes, which have been linked to the CCP's campaign against the Uyghurs.[70] "Poverty alleviation" is the policy term through which the CCP administers forced displacement, cultural erasure, and economic exploitation of Uyghurs, operating in parallel with and reinforced by the internment camp system.[71]

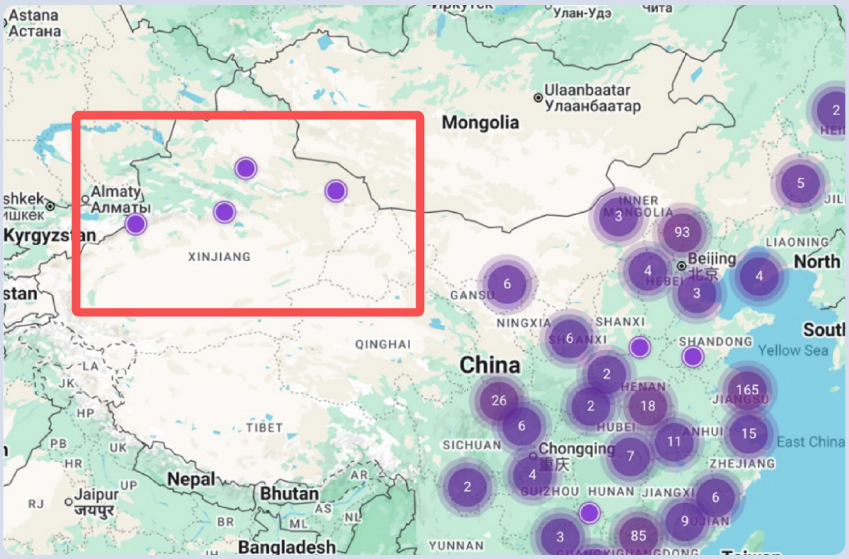


Figure 2: China Telecom Data Center Operations in China[72]

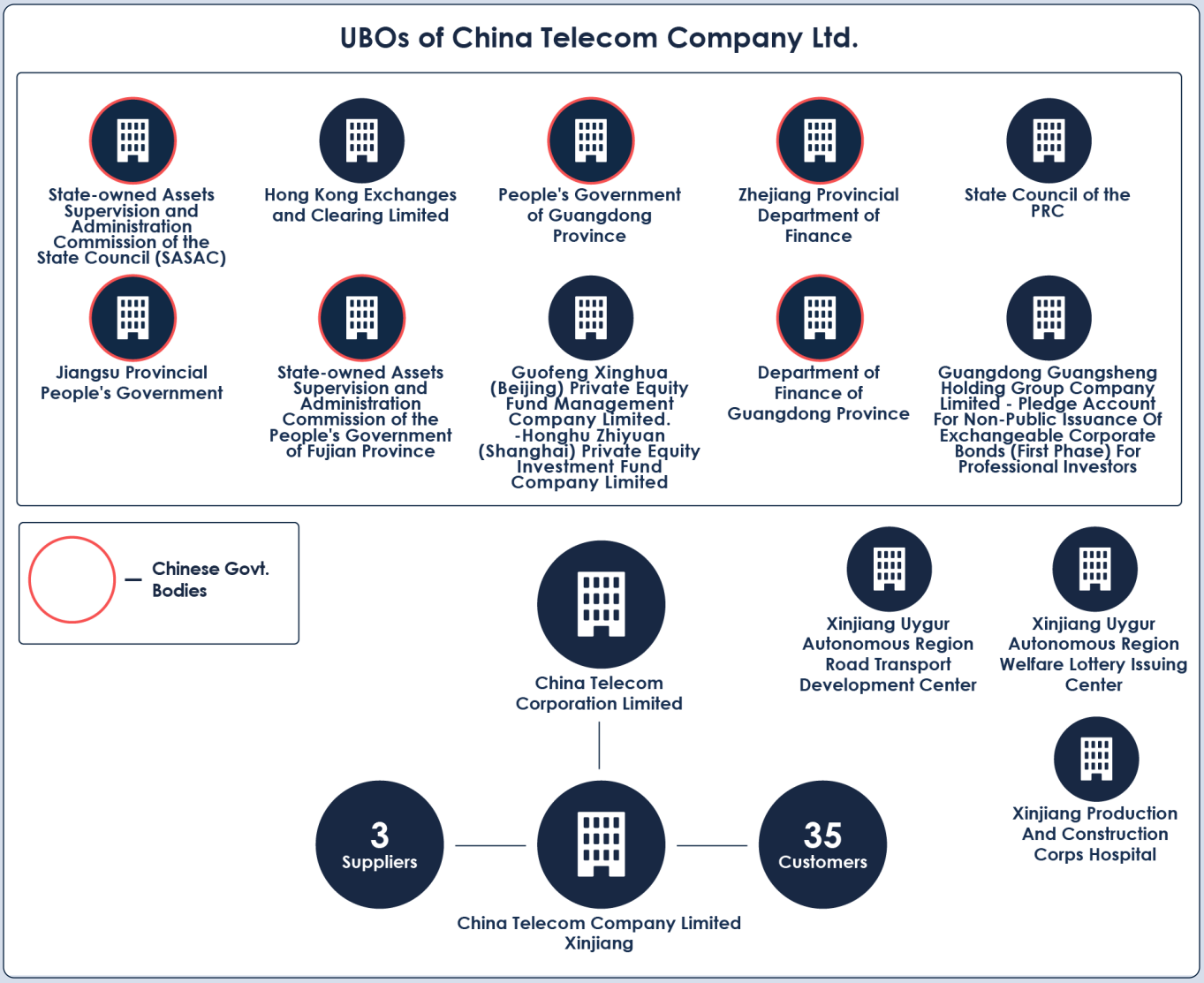


Figure 3: Ultimate Beneficial Owners (UBOs) of China Telecom Company Ltd. See the full list of its suppliers and customers at C4ADS.org/reports/hardwired-repression Source: WireScreen.

XPCC Contracts and Entanglement with State Security

China Telecom Xinjiang also holds active contracts with the XPCC relating to data centers in the region.[73] According to 2025 XPCC documents, for example, China Telecom Xinjiang will build and maintain a dedicated facility for the Xingtuan Statistics Bureau to house its servers, storage systems, and networking equipment; the four-year contract also requires China Telecom Xinjiang to perform routine maintenance.[74] Another contract stipulates that China Telecom Xinjiang will provide one year of services for the equipment room of the XPCC Education Bureau and its subordinate units, including vocational schools.[75] The most expensive China Telecom Xinjiang contract with the XPCC, worth approximately 7.6 million RMB (US$1.1 million), is for the construction of the XPCC Medical Insurance Information Platform. For this project, China Telecom Xinjiang will complete the renewal of server racks, transmission link renewal, and other services.[76]

Beyond its contracts with the XPCC, China Telecom Xinjiang serves more than 21 additional entities in the region, including the Chinese military and intelligence.[77] The company's role extends beyond data center construction to active infrastructure management. For example, it serves the XUAR Highway Development Center and the Urumqi Customs Logistics Management Center.[78] These activities underscore China Telecom Xinjiang's significant contribution to establishing the Uyghur region as a major trading hub and a critical node in China's exports to Central Asia, Europe, and beyond.[79]

While not strictly data center contracts, China Telecom Xinjiang's broader service relationships are relevant as risk indicators. China Telecom Xinjiang provides services to "A Unit," a Chinese government designation generally used for military or intelligence agencies.[80] Additionally, it receives transmission construction services and security management services from Chinese defense contractors, such as Eracom Contracting and Engineering Company Limited (中时讯通信建设有限公司), CCS Public Information Industry Company Limited (中通服公众信息产业股份有限公司), and China Telecom Digital Intelligence Technology Company Limited (中电信数智科技有限公司).[81] These relationships suggest that China Telecom Xinjiang's service footprint extends into military and intelligence-adjacent operations in the region, a relevant consideration when assessing the broader risk profile of its data center expansion.

This case study demonstrates that data centers in the Uyghur region are nodes in an integrated system that connects civilian telecommunications, state surveillance, military contracting, and the coercive labor and social control apparatus directed at the Uyghurs. For Western companies, the layered structure of state-owned enterprise relationships makes clean separation impossible. Every supply chain interaction with China Telecom Xinjiang is more than a purely commercial transaction. Each carries implicit ties to a state-linked entity closely connected to the Chinese government whose infrastructure is implicated in documented human rights violations.

Figure 4: China Telecom Xinjiang has procured goods/services from these defense-related entities. Source: WireScreen.

Why Western Technology Remains Embedded in Chinese Data Centers

As China has escalated efforts to develop competitive domestic technology and achieve technological self-sufficiency, its data infrastructure has continued to rely on American technology.[82] President Xi Jinping began pushing for self-sufficiency in key technologies as early as 2013.[83] That drive was codified through successive state-led initiatives: "Made in China 2025" (2015), the "New Generation AI Development Plan" (2017), and the 14th and 15th Five-Year Plans (2021 and 2026), each reinforcing the strategic objective of technological self-reliance.[84] Since 2022, the United States has implemented trade restrictions limiting China's access to advanced chips and semiconductor technology, prompted by growing concerns over China's Military-Civil Fusion policy, which deliberately blurs the line between civilian industrial development and military applications.[85]

C4ADS' analysis of 2024-2025 government documents reinforces Associated Press findings that American technology continues to play a key role in China's data center infrastructure and, by extension, in the PRC's predictive policing and surveillance capabilities, including those in the Uyghur region.[86] Project specifications reveal a transitional technological landscape: Western components continue to be required in Chinese data center infrastructure, alongside Asian technology such as QNAP (威联通), a Taiwanese company, even as acquisition documents increasingly emphasize preferences for domestic alternatives such as Huawei (华为), H3C (新华三集团), Inspur (浪潮), and Tencent Cloud (腾讯云).[87]

At the same time, the CCP incentivizes data center developers to use Chinese technology by providing subsidies, creating nontariff barriers that favor Chinese firms, and implementing favorable regulatory frameworks.[88] Some projects reviewed explicitly require adherence to localization regulations (国产化), mandating the use of domestic technology (国产品牌) such as Kylin OS (银河麒麟), a Chinese alternative to Windows.[89]

The project requirements for compatibility with Western technology – often involving technologies not subject to export controls – highlight the limitations of that approach. Several explanations may account for this apparent tension between that requirement and the simultaneous push to incentivize domestic alternatives.[90] First, new Chinese systems may need to maintain integration with existing Western-built infrastructure, as moving from one technological ecosystem to another takes time and compatibility is necessary during the transition. Second, as it pertains to export-controlled technologies, China may be anticipating future policy changes that could restore legal avenues for accessing American and other Western technology. Third, as Western technology remains the global industry standard, China may want to ensure interoperability. Finally, for controlled items, Beijing may be calculating that it will be able to circumvent U.S. export controls through smuggling and third-party transshipment – that is, accessing the technology illegally. Taken together, these explanations suggest that the dual requirement reflects Beijing's likely expectation of continued, even if limited, access to U.S. chips and processors, allowing China to hedge between Western technology integration and complete technological self-reliance.

This technological hybridity exposes non-PRC technology companies to the risk of inadvertently supporting Chinese surveillance infrastructure and human rights violations, even as Beijing pursues technological self-sufficiency. The documents show that Intel processors appear across data center-related projects in the Uyghur region, that some projects require Nvidia and AMD compatibility, and that others rely on products made by Dell, HP, Microsoft, Cisco, VMware, and QNAP.[91] The technology identified in those documents fell below the threshold for export-banned chips. A separate Bloomberg analysis found that Chinese firms plan to install more than 115,000 Nvidia AI chips across at least three dozen data centers in the Uyghur region and neighboring Qinghai Province – chips that were subject to U.S. export controls at the time.[92]

Whether above or below these continuously evolving export restrictions, the fact remains that Western companies might inadvertently continue to enable the computational backbone of repressive surveillance systems targeting Uyghurs and other ethnic minorities in the PRC. The due diligence practices of international technology companies have proven effectively insufficient to address risks associated with defense ties and human rights abuses. Meaningful change will require action beyond the corporate level.

Implications Beyond the Uyghur Region

The Uyghur region's surveillance-linked data centers serve a dual purpose: they underpin the CCP's ability to monitor and control its minority populations at home while positioning China as the dominant provider of data infrastructure along its overland corridors into Central Asia.[93] They are not merely tools of repression; they are fundamental to China's governance model, both internally and as an export.[94] Chinese companies with ties to the state surveillance and military apparatus thus maintain access to foreign markets and are well positioned to expand China's extraterritorial data infrastructure, exposing foreign markets to risks associated with human rights abuses and data privacy.

The consolidation of education, medical, and other sectoral data – as documented in XUAR government records – combined with the stated goal of cross-regional data-sharing infrastructure that EDWC and related initiatives aim to enable, points to an unprecedented expansion of authoritarian oversight capabilities.[95] This threat is compounded by the CCP's broader shift from informant-dependent surveillance toward an AI-enabled system capable of monitoring diverse populations continuously and at scale.[96]

This expansion is tied to the PRC's defense and security apparatus in ways that create due diligence and other legal compliance risks for international entities. Funding for surveillance-related projects in the Uyghur region flows directly from Chinese defense and counterterrorism budgets, making the commercial telecommunications sector inseparable from the security state.[97] China Telecom and its subsidiaries – among the largest actors in data center construction in the region – exemplify this entanglement.[98] Any hardware, software, or investment connected to these entities carries inherent risk: the infrastructure they support serves state, military, and surveillance functions – not commercial ones alone.

The Uyghur region's data center development also has a cross-border dimension. Half of the PRC's economic corridors originate there, and Beijing's need to develop the region economically while enforcing political compliance among its population is not incidental but strategic.[99] Data centers are critical infrastructure for both purposes, connecting domestic surveillance to China's broader geopolitical ambitions across Central Asia and beyond.

Conclusion

Western technology, some of which falls under the threshold of high-end, controlled technologies, remains integral to data centers powering China's surveillance apparatus in the Uyghur region, despite export restrictions on some of this technology and international condemnation of the human rights abuses it enables. The data center projects in the Uyghur region continue to require compatibility with Dell, Nvidia, Intel, HP, Microsoft, Cisco, VMware, Western Digital, Seagate, AMD, and QNAP technology. And the Uyghur region is only the starting point for Beijing's AI ambitions and the CCP's drive to maintain strict control over it. The EDWC initiative, Digital Silk Road, and related provincial and central policy efforts optimize China's computing and energy infrastructure. These policies – and the data center infrastructure built to support them – underpin oppressive surveillance and human rights abuses in the PRC, especially in ethnic minority autonomous regions. The role of Uyghur region-based companies in supplying technology services to prisons and governments in other provinces further highlights the interconnected nature of China's digital infrastructure and the replication of repressive tactics across these regions.

This technological interdependence operates largely below the threshold of official Western sanctions designations and export control frameworks most commonly applied to Chinese mass surveillance. Democratic governments must deploy export controls, sanctions, and procurement restrictions to prevent Western technology from enabling surveillance infrastructure targeting Uyghurs and other minorities, and address the implications of this exposure. Technology companies, investors, and multinational corporations must conduct rigorous due diligence to identify and eliminate such exposure to surveillance infrastructure in the Uyghur region.

Recommendations

Based on this analysis, C4ADS offers the following recommendations for governments, private sector actors, as well as civil society and academic institutions:

1. Close the ownership structure opacity gap in sanctions regimes.

The existing U.S. sanctions regime has limited reach when applied to the layered ownership structures of state-owned enterprises and their subsidiaries, through which sanctioned actors continue to operate. China Telecom Corporation Limited carries designations across multiple U.S. sanctions regimes, yet the impact is narrow. The Chinese Military-Industrial Complex Company (CMIC) listing prevents U.S. persons from trading the company's public securities, and the General Services Administration Systems for Award Management (GSA SAM) exclusion bars the company from U.S. government contracts. Neither restriction meaningfully constrains China Telecom Xinjiang, a subsidiary, which is not publicly listed and is unlikely to seek U.S. government contracts. The more consequential policy gap is China Telecom's absence from the Entity List. Adding China Telecom and its provincial subsidiaries, including China Telecom Xinjiang, to the Commerce Department's Entity List would impose license requirements on any U.S. exports to these entities, including hardware, software, and technology, and would create a meaningful barrier to the kind of data center buildout documented in this report.

2. Mandate end-use monitoring and verification for technology exports.[100]

The continued need for Western technology in the Uyghur region's data center infrastructure exposes a core limitation of current export controls. Much of this equipment does not require a license for export to China; however, the mechanisms for verifying where the technology is deployed and who operates

it are insufficient to prevent it from reaching facilities serving military, intelligence-linked entities, and government bodies responsible for carrying out atrocity crimes. Policymakers should consider requiring mandatory, rather than discretionary, post-shipment verification for dual-use technology exports destined for entities operating in regions with documented atrocity crimes and human rights abuses. Policymakers should also establish clearer liability standards for exporters whose hardware reaches the military or intelligence-affiliated end users. [101]

Endnotes

1.Yueyang Lin, "China's Homegrown Tech Boosts Global Surveillance, Social Controls: Report," *Radio Free Asia*, February 20, 2025, https://www.rfa.org/english/china/2025/02/20/china-ai-neuro-quantum-surveillance-security-threat/. 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/. Paul Mozur and Don Clark, "China's Surveillance Infrastructure Powered by U.S. Tech," *The New York Times*, November 2020, Summarized in *China Digital Times*, https://chinadigitaltimes.net/2020/11/chinas-surveillance-infrastructure-powered-by-u-s-tech/.

2. Lars Daniel, "China's Surveillance State Is Losing Its Grip," *Forbes*, December 5, 2024, https://www.forbes.com/sites/larsdaniel/2024/12/05/chinas-surveillance-state-is-losing-its-grip/.

3. The paper uses “Uyghur region” to refer to the Xinjiang Uyghur Autonomous Region, unless referring to existing legal structures, such as governments and financial entities.

4. "How Mass Surveillance Works in Xinjiang," Xinjiang Data Project, ASPI, April 2019, https://xjdp.aspi.org.au/explainers/how-mass-surveillance-works-in-xinjiang/.

5. “China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass; and Xinjiang Police Files, accessed April 15, 2026, https://www.xinjiangpolicefiles.org/.

6. "How Mass Surveillance Works in Xinjiang," Human Rights Watch; and "China's Algorithms of Repression," Xinjiang Police Files.

7. C4ADS data holdings, data available upon request.

8. Adrian Zenz and James Leibold, "Xinjiang's Rapidly Evolving Security State," *China Brief* 17, no. 4 (Jamestown Foundation, March 14, 2017), https://jamestown.org/xinjiangs-rapidly-evolving-security-state/; Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (January 2019): 53–67. Human Rights Watch, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App* (New York: Human Rights Watch, May 1, 2019), https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass; International Consortium of Investigative Journalists, "Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm," ICIJ, November 24, 2019, https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/. Paul Scharre, "The Dangers of the Global Spread of China's Digital Authoritarianism," testimony before the U.S.-China Economic and Security Review Commission, 118th Cong., May 4, 2023, Center for a New American Security, https://www.cnas.org/publications/congressional-testimony/the-dangers-of-the-global-spread-of-chinas-digital-authoritarianism; Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023). Valentin Karpa, Torben Klarl, and Michael Rochlitz, "Exporting the Tools of Dictatorship: The Politics of China's Technology Transfers," *Perspectives on Politics* (January 21, 2025), https://www.cambridge.org/core/journals/perspectives-on-politics/article/exporting-the-tools-of-dictatorship-the-politics-of-chinas-technology-transfers/D1A5B1D7C7A21FB5E601A553E6E8833F; Darren J. Lim and Victor Ferguson, "Digital Authoritarianism, China and COVID," Lowy Institute, November 2020, https://www.lowyinstitute.org/publications/digital-authoritarianism-china-covid; Steven Feldstein, “The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression,” *Journal of Democracy* 30, no. 1 (2019): 40–52.

9. Adrian Zenz, “Statement before the Subcommittee on Asia and the Pacific,” House Committee on Foreign Affairs, U.S. House of Representatives, 115th Congress, 2nd Session, September 26, 2018, https://www.congress.gov/115/meeting/house/108718/witnesses/HHRG-115-FA05-Wstate-ZenzA-20180926-SD001.pdf.

10. Adrian Zenz, "Innovating Repression: Policy Experimentation and the Evolution of Beijing's Re-Education Campaign in Xinjiang," *Journal of Contemporary China* 34, no. 152 (2024): 328–349, https://doi.org/10.1080/10670564.2024.2302484.

11. The PRC is the state, the CCP is the ruling party. Although the two are deeply intertwined in practice, the CCP exercises control over the PRC’s government, military, and judiciary, and the two entities are not synonymous. Government of the United States, "China Primer: China's Political System," Congressional Research Service, July 1, 2024, https://s3.documentcloud.org/documents/24786018/china-primer-chinas-political-system-july-1-2024.pdf.

12. John Sudworth, "The Faces from China's Uyghur Detention Camps," BBC News, May 24, 2022, https://www.bbc.co.uk/news/extra/85qihtvw6e/the-faces-from-chinas-uyghur-detention-camps; and Adrian Zenz, "Innovating Penal Labor: Reeducation, Forced Labor, and Coercive Social Integration in the Xinjiang Uyghur Autonomous Region," *The China Journal* 90 (2023), https://doi.

org/10.1086/725494, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4468500; and Zenz, "Innovating Repression."

13. China's largest datacenter is 10.7 million square feet, located in Inner Mongolia. Phill Powell and Ian Smalley, "What Is a Hyperscale Data Center?" IBM Think, accessed April 15, 2026, https://www.ibm.com/think/topics/hyperscale-data-center.

14. Konstantin Pilz and Lennart Heim, "Compute at Scale: A Broad Investigation into the Data Center Industry," arXiv preprint arXiv:2311.02651, November 5, 2023, https://arxiv.org/pdf/2311.02651; and Brian Potter, "How to Build an AI Data Center," Information Technology and Innovation Foundation, June 20, 2024, https://ifp.org/how-to-build-an-ai-data-center/.

15. In the future, C4ADS plans to replicate this analysis in other autonomous regions, including Tibet.

16. Mishel Kondi, *Side Effects: The Human Rights Implications of Global Pharmaceutical Supply Chain Linkages to XUAR* (Washington, DC: C4ADS, October 8, 2024), https://c4ads.org/reports/side-effects/; C4ADS, *Fractured Veins: The World's Reliance on Minerals from the Uyghur Region* (Washington, DC: C4ADS, October 11, 2023), https://c4ads.org/reports/fractured-veins/; "Asleep at the Wheel: Car Companies' Complicity in Forced Labor in China," Human Rights Watch, February 1, 2024, https://www.hrw.org/report/2024/02/01/asleep-wheel/car-companies-complicity-forced-labor-china; "Why It's So Hard for the Solar Industry to Quit Xinjiang," *Energy Connects*, December 2021, https://www.energyconnects.com/news/renewables/2021/december/why-it-s-so-hard-for-the-solar-industry-to-quit-xinjiang/; and European Parliament, Directorate-General for External Policies of the Union, *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights* (Brussels: European Parliament, 2024), https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450(SUM01)_EN.pdf.

17. Steven Feldstein, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (2019), https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/; and Andy Lin, Mackenzie Hawkins, Colum Murphy, and James Mayger, "China Wants to Use 115,000 Banned Nvidia Chips to Power Data Centers in the Desert," *Bloomberg Technology*, July 8, 2025, https://www.bloomberg.com/graphics/2025-china-data-centers-nvidia-chips/.

18. C4ADS data holdings, data available upon request.

19. Kondi, *Side Effects: The Human Rights Implications of Global Pharmaceutical Supply Chain Linkages to XUAR*; C4ADS, *Fractured Veins: The World's Reliance on Minerals from the Uyghur Region*; and Adrian Zenz and I-Lin Lin; "Forced Labor, Coercive Land-Use Transfers, and Forced Assimilation in Xinjiang's Agricultural Production," International Network for Critical China Studies, December 10, 2024, SSRN Working Paper, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5053281.

20. "China invests $61 bln in computing, data center project, official says," Reuters, August 29, 2024, https://www.reuters.com/technology/china-invests-61-bln-computing-data-center-project-official-says-2024-08-29/.

21. "东数西算," ("Eastern Data Western Computing"), National Center for Science and Technology Information (NCSTI), archived July 8, 2025, https://web.archive.org/web/20250708135739/https://www.ncsti.gov.cn/kjdt/ztbd/dsxs/; and "Eastern Data, Western Computing Network," Huawei Technologies, February 2022, https://www.huawei.com/en/huaweitech/publication/202202/eastern-data-western-computing-network.

"Inner Mongolia is an Autonomous Region with a significant ethnic minority population. Inner Mongolia: Overview," *The Paper (*澎湃新闻*)*, archived April 27, 2026, https://web.archive.org/web/20260427050147/https://m.thepaper.cn/baijiahao_12783429.

Gansu is a relatively impoverished province with two autonomous prefectures and a significant ethnic minority population including Tibetans and the Hui (a Muslim ethnic minority group); "Gansu Province Overview," *China Daily (Gansu Edition)*, April 23, 2021, http://gansu.chinadaily.com.cn/2021-04/23/c_613426.htm; and "Gansu" Asia Harvest, accessed 2024, https://www.asiaharvest.org/china-resources/gansu.

Ningxia is an autonomous region with a significant ethnic minority population. "Ningxia;" *Asia Harvest*, accessed April 15, 2024, https://www.asiaharvest.org/china-resources/ningxia; and "Ningxia: A Profile," Ningxia Hui Autonomous Region Foreign Affairs Office, September 8, 2020, http://fao.nx.gov.cn/ENGLISH/ningxiatoday/ningxiaaprofile/202009/t20200908_2224494.html.

22. Wei Liu, Toby S. James, and Caixia Man, "Governance and Public Administration in China," *Policy Studies* 43 (3) (2022): 387–402, doi:10.1080/01442872.2022.2054091.

23. The PRC's western regions encompass several provinces and autonomous regions where non-Han ethnic groups have historically formed a majority share of the population, including the XUAR, TAR, Inner Mongolia, Yunnan, Qinghai, and Guangxi. These areas are officially designated as "autonomous regions" or contain autonomous prefectures, which is an administrative classification that, in theory, is meant to grant limited self-governance rights to recognized ethnic minorities. However, in practice, local governments are under strict rule from Beijing. For more, see: Bonny Lin and Soo Kim, "Why Minorities Make Beijing Nervous," Center for Strategic

and International Studies, China Power project, September 30, 2024, https://chinapower.csis.org/analysis/why-minorities-make-beijing-nervous/.

24. Eastern Data, Western Computing's initial western hub nodes included Inner Mongolia and Ningxia, both autonomous regions, as well as the provinces of Guizhou, Gansu, and Sichuan, all of which have significant ethnic minority populations. While XUAR and TAR are not in the original eight EDWC hub nodes, they are frequently discussed alongside the initiative. "Eastern Data, Western Computing Network," Huawei Technologies, February 2022, https://www.huawei.com/en/huaweitech/publication/202202/eastern-data-western-computing-network. Paul Triolo and Kevin Allison, "China's Latest National Infrastructure Project Spotlights Computing Capabilities," Net Politics blog, Council on Foreign Relations, November 1, 2022, https://www.cfr.org/blog/chinas-latest-national-infrastructure-project-spotlights-computing-capabilities; and "China to Build 8 Computing Hub Regions under 'East-West' Strategy," *China Daily* / National People's Congress, January 10, 2024, https://subsites.chinadaily.com.cn/npc/2024-01/10/c_954912.htm.

25. "China invests $61 bln in computing, data center project, official says," Reuters, August 29, 2024, https://www.reuters.com/technology/china-invests-61-bln-computing-data-center-project-official-says-2024-08-29/.

26. "为什么新疆智算中心越来越多?," ("Why are there more and more intelligent computing centers in Xinjiang?"), Tencent Cloud Developer, November 17, 2024, https://cloud.tencent.com/developer/news/1928266.

27. "为什么新疆智算中心越来越多?," ("Why are there more and more intelligent computing centers in Xinjiang?"), Tencent Cloud Developer.

28. National Development and Reform Commission, (国家发展和改革委员会), "一图读懂 | '东数西算'工程解读," ("A Visual Guide to the 'East Data, West Computing' Initiative"), NDRC.gov.cn, February 17, 2022, https://web.archive.org/web/20220315112608/https://www.ndrc.gov.cn/xxgk/jd/zctj/202202/t20220217_1315797.html.

29. "China's Data Centers Push Cooling to the Limit Amidst Unprecedented Growth," Enertherm Engineering, August 20, 2025, https://enertherm-engineering.com/chinas-data-centers-push-cooling-to-the-limit-amidst-unprecedented-growth/; Yingbo Zhang, Hangxin Li, and Shengwei Wang, "Decarbonizing Data Centers through Regional Bits Migration: A Comprehensive Assessment of China's 'Eastern Data, Western Computing' Initiative and Its Global Implications," *Applied Energy* 392 (2025): 126020, https://doi.org/10.1016/j.apenergy.2025.126020; and "The China Data Centre Advantage," *Oxford Energy Comment*, Oxford Institute for Energy Studies, February 2026, https://www.oxfordenergy.org/wpcms/wp-content/uploads/2026/02/Comment-The-China-data-centre-advantage.pdf.

30. Andrew Stokols, "China's Data Center Boom: A View from Zhangjiakou," *Sinocities* (Substack), November 17, 2025, https://sinocities.substack.com/p/chinas-data-center-boom-a-view-from.

31. Stokols, "China's Data Center Boom: A View from Zhangjiakou."

32. Stokols, "China's Data Center Boom: A View from Zhangjiakou"; "China Data Centers: New Cross-Regional Plan to Boost Computing Power," *China Briefing*, March 30, 2022, https://www.china-briefing.com/news/china-data-centers-new-cross-regional-plan-to-boost-computing-power-across-regions/.

33. The Origin of the 'Xinjiang Model' in Tibet under Chen Quanguo: Securitizing Ethnicity and Accelerating Assimilation," International Campaign for Tibet, December 19, 2018, https://savetibet.org/the-origin-of-the-xinjiang-model-in-tibet-under-chen-quanguo-securitizing-ethnicity-and-accelerating-assimilation/; and Kelsang Dolma, "Tibet Was China's First Laboratory of Repression," *Foreign Policy*, August 31, 2020, https://foreignpolicy.com/2020/08/31/tibet-china-repression-xinjiang-sinicization/.

34. Lin, Hawkins, Murphy, et al., "China Wants to Use 115,000 Banned Nvidia Chips to Power Data Centers in the Desert."

35. Government of the People's Republic of China, "The History and Development of the Xinjiang Production and Construction Corps., White Paper" (Beijing: State Council Information Office, October 5, 2014), https://english.www.gov.cn/archive/white_paper/2014/10/05/content_281474992384669.htm; Laura T. Murphy, Nyrola Elimä, and David Tobin, "*Until Nothing Is Left: China's Settler Corporation and Its Human Rights Violations in the Uyghur Region*" (Sheffield: Sheffield Hallam University, Helena Kennedy Centre for International Justice, July 2022), https://shura.shu.ac.uk/34919/1/Murphy%20Elima%20Tobin%20--%20Until%20Nothing%20is%20Left.pdf.

36. "Uighurs: Western Countries Sanction China over Rights Abuses," BBC News, March 22, 2021, https://www.bbc.com/news/world-europe-56487162.

37. Aiping Zhang, "The Belt and Road and the Path of Constructing Xinjiang Big Data Center Under the Background of Global Governance," Xinjiang University, School of Politics and Public Administration, no. 3 (2018), https://doi.org/10.13677/j.cnki.cn65-1285/c.2018.03.11.

38. The Belt and Road Initiative is far more than ports, roads, and railways. Embedded within is a sweeping digital agenda. Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*, (New York: Harper Business, 2021).

39. "Xinjiang Leads China in Cross-Border Rail Traffic, Central Asian Connectivity in 2025." Xinhua. January 16, 2026. https://english.news.cn/20260116/0fb1da5b24754e2f9c13dc1fc112a3b6/c.html. C4ADS data holdings, data available upon request.

40. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*.

41. "新疆筑牢算力底座助力数字经济高质量发展" ("Xinjiang Consolidates Computing Foundation to Support High-Quality Development of the Digital Economy"), Xinhua, October 22, 2024, http://www.news.cn/digital/20241022/94f4397836ff48f6a11210d589dc4846/c.html.

42. WireScreen; and C4ADS data holdings, data available upon request.

43. "National Intelligence Law of the People's Republic of China (2017)," translated by China Law Translate, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/. National People's Congress of the People's Republic of China, "Data Security Law of the People's Republic of China," December 9, 2021, http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html. "Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," translated by DigiChina, Stanford University, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/. National People's Congress of the People's Republic of China, "National Security Law of the People's Republic of China," June 27, 2017, http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529.htm. National People's Congress of the People's Republic of China, "Counter-Espionage Law of the People's Republic of China," November 7, 2016, http://www.npc.gov.cn/zgrdw/npc/zfjc/zfjcelys/2016-11/07/content_2034939.htm. National Counterintelligence and Security Center, "People's Republic of China (PRC) Laws Potentially Impacting U.S. Organizations," Safeguarding Our Future Bulletin, Office of the Director of National Intelligence, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.

44. United Nations, "China: Xinjiang's Forced Separations and Language Policies Against Uyghur Children," UN Human Rights Office, Press release, September 26, 2023, https://www.ohchr.org/en/press-releases/2023/09/china-xinjiangs-forced-separations-and-language-policies-uyghur-children.

45. C4ADS data holdings, data available upon request.

46. C4ADS data holdings, data available upon request.

47. "How Mass Surveillance Works in Xinjiang," Human Rights Watch, May 2, 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang.

48. There are no publicly available sources confirming the status of this project.

49. Government of the United Kingdom, "UK Sanctions Perpetrators of Gross Human Rights Violations in Xinjiang alongside EU, Canada and US," UK Foreign, Commonwealth & Development Office, Press release, March 22, 2021, https://www.gov.uk/government/news/uk-sanctions-perpetrators-of-gross-human-rights-violations-in-xinjiang-alongside-eu-canada-and-us; Government of Canada, "Canadian Sanctions Related to China," Global Affairs Canada, accessed April 15, 2026, https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/china-chine.aspx?lang=eng; Government of the United States, "Treasury Sanctions Chinese Entity and Officials Pursuant to Global Magnitsky Human Rights Accountability Act," U.S. Department of the Treasury, July 9, 2020, https://home.treasury.gov/news/press-releases/sm1055; and United Nations, *OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China*, Office of the United Nations High Commissioner for Human Rights, August 31, 2022, https://www.ohchr.org/sites/default/files/documents/2022-08-31/22-08-31-final-assesment.pdf.

50. C4ADS data holdings, data available upon request.

51. C4ADS data holdings, data available upon request.

52. C4ADS data holdings, data available upon request.
A full list of non-PRC technologies mentioned in government records for this project:
ASUS: Listed as the brand for three items: desktop computers, monitors, and a standalone computer.
Intel: Appears in the desktop specifications as an optional CPU (Core i5-13490F with B760 chipset motherboard), in the standalone computer specifications (i7-12700), and in the video editing machine specifications (Core i7-12700 up to 4.9GHz, 12 cores).
NVIDIA: Appears in the desktop specifications as an optional graphics card (GeForce RTX 4060 Ti) and in the video editing machine specifications (RTX 3050 6GB).

AMD: Appears in the desktop specifications as an alternative CPU option (Ryzen 5 7600 with B650 chipset motherboard) and as an alternative graphics card option (Radeon RX 7600 XT).
Exact language: "NVIDIA GeForce RTX 4060 Ti/AMD Radeon RX 7600 XT" and "Graphics Card: Nvidia RTX 3050 6GB."

53. Lennart Heim, "Understanding the Artificial Intelligence Diffusion Framework: Can Export Controls Create a U.S.-Led Global Artificial Intelligence Ecosystem?" RAND Perspectives (Santa Monica, CA: RAND Corporation, 2025), https://www.rand.org/pubs/perspectives/PEA3776-1.html.

54. C4ADS data holdings, data available upon request.

55. C4ADS data holdings, data available upon request.

56. C4ADS data holdings, data available upon request.

57. C4ADS data holdings, data available upon request.

58. WireScreen.

59. WireScreen; and C4ADS data holdings, data available upon request.

60. WireScreen.

61. WireScreen; and "China Telecom Develops Country's First MoE Models Trained Entirely on Huawei's AI Chips," *South China Morning Post*, January 20, 2026, https://www.scmp.com/tech/big-tech/article/3340591/china-telecom-develops-countrys-first-moe-models-trained-entirely-huaweis-ai-chips.

62. "China Telecom: BlackRock Sells $200 Million China Telecom Stake after U.S. Ban," *South China Morning Post, MarketScreener*, January 15, 2021, https://www.marketscreener.com/quote/stock/CHINA-TELECOM-CORPORATION-1412702/news/China-Telecom-BlackRock-sells-200-million-China-Telecom-stake-after-U-S-ban-32204080/.

63. Government of the United States, "Recent OFAC Actions," U.S. Department of the Treasury, Office of Foreign Assets Control, June 3, 2021, https://ofac.treasury.gov/recent-actions/20210603; and "Excluded Parties List: Entity S4MRQP5ZQ," System for Award Management (SAM.gov), accessed April 15, 2026, https://sam.gov/search/?index=ex&page=1&pageSize=25&sort=-relevance&sfm%5BsimpleSearch%5D%5BkeywordTags%5D%5B0%5D%5Bvalue%5D=S4MRQP5ZQ.

64. "China Telecom Seeks to Deregister Its American Depositary Shares and Terminate Reporting Obligations Under the U.S. Securities Exchange Act," WireScreen, China Telecom Corporation Limited, Press release, February 25, 2022, Archived at https://web.archive.org/web/20220309044816/https://www.chinatelecom-h.com/en/media/news/p220225.pdf; Julia Kollewe and Rupert Neate, "New York Stock Exchange to Delist Three Chinese Telecom Firms over Alleged Military Links," *The Guardian*, January 1, 2021, https://www.theguardian.com/business/2021/jan/01/new-york-stock-exchange-nyse-to-delist-three-chinese-telecom-firms-alleged-military-links; and Ana Swanson, "The N.Y.S.E. Plans to Delist Three Chinese Telecom Companies," *The New York Times*, January 1, 2021, https://www.nytimes.com/2021/01/01/business/nyse-delist-china-mobile.html.

65. Jonathan Stempel and Jennifer Ablan, "BlackRock sells $200 mln in China Telecom stake after US ban," Reuters, January 15, 2021, https://www.reuters.com/business/media-telecom/blackrock-sells-200-mln-china-telecom-stake-after-us-ban-2021-01-15/.

66. "Global Data Center Map," CT Americas, accessed April 15, 2026, https://www.ctamericas.com/global-data-center-map/; and "China Telecom Locations: United States," DataCenters.com, accessed April 15, 2026, https://www.datacenters.com/providers/china-telecom/locations/united-states.

67. "About China Telecom Europe," China Telecom Europe, website, accessed April 17, 2026, https://www.chinatelecomeurope.com/; and "Locate Us," China Telecom Asia Pacific, accessed April 17, 2026, https://www.chinatelecomasiapacific.com/locate-us/.

68. "Global Data Center Map," CT Americas; and "Data Centers in China," DataCenters.com.

69. "Global Data Center Map," CT Americas; and "Data Centers in China," DataCenters.com.

70. *Annual Report 2024*, China Telecommunications Corporation, accessed April 17, 2026, https://www.chinatelecom-h.com/en/ir/report/annual2024.pdf.

71. United Nations, "UN Experts Alarmed by Reports of Forced Labour of Uyghur, Tibetan and Other Minorities," Office of the United Nations High Commissioner for Human Rights, Press release, January 22, 2026, https://www.ohchr.org/en/press-releases/2026/01/un-experts-alarmed-reports-forced-labour-uyghur-tibetan-and-other-minorities; and Adrian Zenz, "The Conceptual Evolution of Poverty Alleviation through Labor Transfer in the Xinjiang Uyghur Autonomous Region," *Central Asian Survey* 42, no. 4 (2023), https://doi.org/10.1080/02634937.2023.2227225.

72. "Data Centers in China," DataCenters.com, https://www.datacenters.com/locations/china.

73. C4ADS proprietary data, available upon request; and Government of the United States, "Treasury Sanctions Chinese Entity and Officials Pursuant to Global Magnitsky Human Rights Executive Order," Department of the Treasury, July 31, 2020, https://home.treasury.gov/news/press-releases/sm1073.

74. While not defined explicitly in the government document, maintenance can mean any renewal, repair, replacement, upgrade, or restoration of any of the following: IT equipment, such as servers, storage systems, networking equipment, and related infrastructure.

75. Vocational schools in the Uyghur region have historically played a key role in state sponsored forced labor in the region. Lindsay Maizland, "China's Repression of Uyghurs in Xinjiang," Council on Foreign Relations, October 3, 2025, https://www.cfr.org/backgrounder/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights.

76. C4ADS data holdings, data available upon request.

77. WireScreen.

78. WireScreen.

79. WireScreen.

80. WireScreen.

81. WireScreen

82. John Krige, "Debate: Building a U.S. Regulatory Empire in the Chip War with China," *Technology and Culture* 65, no. 4 (2024): 1081-1108. https://dx.doi.org/10.1353/tech.2024.a940462.

83. South China Morning Post, "Tech War: Chinese Leader Xi Jinping Called for Tech Self-Sufficiency a Decade Ago, According to Speech in New Book," *Yahoo Finance*, June 1, 2023, https://finance.yahoo.com/news/tech-war-chinese-leader-xi-093000295.html.

84. WireScreen.

85. John Krige, "Debate: Building a U.S. Regulatory Empire in the Chip War with China," Technology and Culture 65, no. 4 (2024): 1081-1108. https://dx.doi.org/10.1353/tech.2024.a940462.

86. South China Morning Post, "Tech War: Chinese Leader Xi Jinping Called for Tech Self-Sufficiency a Decade Ago, According to Speech in New Book," Yahoo Finance, June 1, 2023, https://finance.yahoo.com/news/tech-war-chinese-leader-xi-093000295.html.

87. Ghulam Ali, "China's Technological Self-Reliance in Response to U.S. Containment," *China-US Focus*, June 17, 2025, https://www.chinausfocus.com/finance-economy/chinas-technological-self-reliance-in-response-to-us-containment; Congressional Research Service, "China's 15th Five-Year Plan: S&T and Economic Priorities," CRS In Focus IF13204, April 16, 2026, https://www.congress.gov/crs-product/IF13204.

88. Sujai Shivakumar, Charles Wessner, and Thomas Howell, "The Limits of Chip Export Controls in Meeting the China Challenge," CSIS, April 14, 2025, https://www.csis.org/analysis/limits-chip-export-controls-meeting-china-challenge; Government of the United States, "U.S. Export Controls and China: Advanced Semiconductors," Congressional Research Service, September 19, 2025, https://www.congress.gov/crs-product/R48642. Cole McFaul, Sam Bresnick, and Daniel Chou, "Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage," Center for Security and Emerging Technology, September 2025, https://cset.georgetown.edu/publication/pulling-back-the-curtain-on-chinas-military-civil-fusion.

89. 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, October 30, 2025, https://apnews.com/article/chinese-surveillance-silicon-valley-trump-administration-congress-21c5f961b1fd22f9a9e563ebe64e5582.

90. Jasmine, "China Mandates 50% Domestic Chip Usage in Data Centers: A Strategic Shift Towards Semiconductor Self-Reliance," Made-in-China.com Business Insights, August 25, 2025, https://insights.made-in-china.com/China-Mandates-50-Domestic-Chip-Usage-in-Data-Centers-A-Strategic-Shift-Towards-Semiconductor-Self-Reliance_hfHavwMlZQiy.html.

91. C4ADS data holdings, data available upon request.

92. Baker McKenzie, "China: Cloud Compliance Center," ResourceHub, March 2023, https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/apac/china; Giulia Interesse, "China's Data Center Sector: Industry and Regulatory Insights," *China Briefing*, August 31, 2023, https://www.china-briefing.com/news/chinas-data-center-sector-industry-and-regulatory-insights/;

Yake Liu, "China Sets Requirements for Government Procurement of Data Center Equipment, Services," *Enviliance*, May 2, 2023, https://enviliance.com/regions/east-asia/cn/report_10060; Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," Center for Strategic and International Studies, August 2, 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china; Georges Haour, "Why China's New Cybersecurity Law Is a Threat to International Businesses and Innovation," IMD, November 2016, https://www.imd.org/research-knowledge/technology-management/articles/why-chinas-new-cybersecurity-law-is-a-threat-to-international-businesses-and-innovation/; and "China Issues New Measures on Cybersecurity Review (2022)," White & Case, February 8, 2022, https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022.

93. C4ADS data holdings, data available upon request.

94. Jasmine, "China Mandates 50% Domestic Chip Usage in Data Centers: A Strategic Shift Towards Semiconductor Self-Reliance," *Made-in-China.com Business Insights*, August 25, 2025, https://insights.made-in-china.com/China-Mandates-50-Domestic-Chip-Usage-in-Data-Centers-A-Strategic-Shift-Towards-Semiconductor-Self-Reliance_hfHavwMlZQiy.html.

95. C4ADS data holdings, data available upon request.

96. Andy Lin, Mackenzie Hawkins, Colum Murphy et al., “China Wants to Use 115,000 Banned Nvidia Chips to Power Data Centers in the Desert.”

97. Graham Greenleaf and Tamar Kaldani, "Data Privacy Laws in Central Asia: Between Ex-SSR and 'Belt & Road'," *International Data Privacy Law* 15, no. 1 (February 2025): 67–90, https://doi.org/10.1093/idpl/ipaf001.

98. Greenleaf and Kaldani, “Data Privacy Laws in Central Asia: Between Ex-SSR and 'Belt & Road.'”

99. Xinjiang Uyghur Autonomous Region Digital Development Bureau (新疆维吾尔自治区数字化发展局), "实干进行时丨数据'跑路'算力撑腰 加快数字新疆建设——访自治区数字化发展局党组书记、副局长李长修" ("Putting Work into Practice: Data 'Running Errands,' Computing Power Providing Support—Accelerating the Construction of Digital Xinjiang: An Interview with Li Changxiu, Party Secretary and Deputy Director of the Autonomous Region's Digital Development Bureau"), *Shiliu Cloud / Xinjiang Daily* (石榴云/新疆日报), January 20, 2026, https://sfj.xinjiang.gov.cn/xjszfzj/bmxw/202601/290467f8937a4aae8b9ec81a0175afab.shtml. It remains unclear whether state telecommunications backbone infrastructure is integrated with private cloud platforms.

100. Specifically, see Government of the United States, “The Commerce Control List,” Department of Commerce, 15 C.F.R. pt. 774, supp. 1, accessed April 17, 2026, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-774.

101. Society for Threatened Peoples, “Written Statement Submitted by Society for Threatened Peoples, a Non-Governmental Organization in Special Consultative Status,” UN Doc. A/HRC/59/NGO/239, United Nations Human Rights Council, 59th sess. May 26, 2025, https://docs.un.org/en/A/HRC/59/NGO/239.