The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 73-97.

Tyranny of City Brain: How China Implements Artificial Intelligence to Upgrade its Repressive Surveillance Regime

CHAMILA LIYANAGE

Abstract

Despite a growing body of research on Chinese mass artificial intelligence (AI) surveillance, there is hardly any study that analyzes its technological architecture and its exact implementation to advance authoritarianism at home and abroad. This article examines the use of AI within Chinese mass surveillance, focusing on its technological architecture, implementation, and impact. The article also explores how Chinese mass AI surveillance grows exponentially, creating its home ecosystem, the all-encompassing smart city, governed by City Brain. The study draws on evidence using in-depth qualitative analysis of key Chinese AI companies and their surveillance technologies verified through their primary research on AI. This evidence helps analyze the implementation of AI surveillance and its impact on civil liberties. The study argues that mass AI surveillance is a means, not an end, a part of a broader goal to create smart cities to forge a home ecosystem for next-generation smart authoritarianism. It is essential to understand Chinese AI surveillance, its implementation, and its impact, as this can be replicated anywhere in the world with China's export of surveillance technologies. The study findings highlight a close relationship between Chinese AI and a quest to develop precision authoritarianism to crush freedom and exert precision social control that can be exported worldwide.

Keywords: Chinese AI surveillance, smart authoritarianism, smart city, city brain, Chinese surveillance exports

Chamila Liyanage
Co-founder, Centre for the Study of Emerging Security Threats (CSEST)
Research Contributor, GNET, King's College London, UK
chamila.c.liyanage@gmail.com

DOI: 10.53483/XCQW3581

Shixian and Zhen, writing in the *People's Weekly* in 2017, explained the Chinese Skynet (天网 *Tiān wǎng*) in simple terms: "The 50,000 surveillance cameras are like 50,000 sleepless police officers, remembering faces when people pass by."[1] They explain the Skynet, which is a countrywide motor vehicle and pedestrian detection and recognition system with 20 million surveillance cameras.[2]

Shixian and Zhen's analogy stands out as it emphasizes the bottlenecks of mass surveillance. Millions of surveillance cameras are far less useful without an effective real-time monitoring system for their footage. Who will do the monitoring? This study examines how artificial intelligence (AI) steps in to create benchmarks for a new authoritarianism of precision control. This new authoritarianism, or what this study calls "smart authoritarianism," attains the pinnacle of authoritarian power, reaching beyond human abilities to exert precision social control.

This study analyzes the rollout of AI in Chinese state surveillance, focusing on its technological architecture, implementation, and impact. In essence, authoritarianism is a centralized power of repression with a natural urge for control. AI and cloud computing raise the bar, offering ubiquitous precision control to upgrade not only Chinese mass surveillance but authoritarianism itself. AI surveillance in its home ecosystem of the futuristic smart city transforms brute force authoritarianism into smart authoritarianism. The study is significant due to the lack of research on the Chinese AI surveillance architecture to assess its implementation and impact. The article provides evidence to prove how exactly China uses AI to upgrade mass surveillance, its technological architecture, AI implementation, its impact on civil liberties, and how AI transforms authoritarianism, boosting its capacity to become a sophisticated model of oppression, which is ideal for denying freedom to millions of people with precision.

First, the article includes a literature review and methodology. Second, it investigates how AI upgrades Chinese mass surveillance, assimilating it into smart cities. Third, it analyzes the practical implementation of AI and its impact. It also shows how China exports not only technologies, but Chinese surveillance rules (algorithms), and the impacts of this abroad. The article establishes that China upgrades mass surveillance and exports AI algorithms, replicating repressive surveillance abroad.

Illiberalism and Chinese AI Surveillance

Doctrinal liberalism builds on a quest to safeguard individual liberty, while illiberalism advances ideals that promote centralized, traditional hierarchies. Illiberalism wages a metapolitical cultural battle to bring atomized liberal loyalties centered on individual rights back to group loyalties envisioned in the "nation, [the] sovereign," strongman leaders, "culture, and tradition."[3] Laruelle conceptualizes illiberalism as an "ideology" rather than a "regime type": it is a "doctrinally fluid, and a (thin) ideology" that varies in different contexts, but it always relates to its antithesis, which is liberalism.[4] Laruelle's definition of illiberalism has it characteristically confronting liberalism in different ways in different contexts to promote ideals

1 Chen Shixian and Li Zhen, "What is 'Skynet' About?" *People's Weekly*, September 23, 2017, http://paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm.

2 Global Times, "Facial recognition, AI and big data poised to boost Chinese public safety," *People's Daily Online*, October 17, 2017, http://en.people.cn/n3/2017/1017/c90000-9280772.html.

3 Marlene Laruelle, "Illiberalism: A Conceptual Introduction," *East European Politics* 38, no. 2 (June 2022): 304, https://doi.org/10.1080/21599165.2022.2037079.

4 Laruelle, "Illiberalism,"303–304.

antithetical to liberalism. Chinese President Xi Jinping fully embraces what Laruelle observes as a "backlash against today's liberalism,"[5] which occurs in and is fanned by the context of the global rise of authoritarianism. Xi's illiberalism goes beyond that of China's regime type. He advances a global quest for digital social control as opposed to individual freedoms. Chinese mass AI surveillance shows a clear practice of illiberalism as it confronts liberal loyalties, squeezing out individual rights and freedoms. China wipes out political freedoms and civil liberties, targeting minorities and demonstrating the rise of technological illiberalism borne out of rapidly evolving technologies such as AI and big data analytics.

China offers algorithms to promote illiberalism and controls people through algorithm-guided AI, exerting social control that serves illiberal ends alongside autocratic, ultranationalist, anti-Western, and traditionalist group loyalties, but above all, it is in confrontation with liberal ideals and norms. AI and big data, the tools of technological illiberalism that can be deployed in both liberal democracies and illiberal states, have become instrumental for mass surveillance. However, as Feldstein notes, illiberal states tend to use such technologies to erase already scarce political freedoms, abusing technologies to achieve coercive control over people.[6]

This article shows how state actors wield AI for political and social control, using surveillance to suppress civil liberties, human rights, and political dissent, and to repress minorities. States are defined as illiberal not by regime type but by ideology-driven, real-world policy practices such as implementing AI for coercive social and political control (illiberalism is as illiberalism does). This article contributes to the idea of technological illiberalism proposed by Laruelle and Dall'Agnola in this special issue, demonstrating how AI enables the rise of technological illiberalism. Technological illiberalism is a policy practice that one must be wary of in different contexts. However, it takes on its definitive form in terms of the algorithms that govern AI surveillance systems. Chinese tech giants shape a form of technological illiberalism, producing mass AI surveillance systems and smart cities ruled by illiberal algorithms to exert precision social control.

This study surveys the Chinese AI surveillance architecture, providing evidence of AI technologies forging ahead, exerting technological illiberalism. China aims to create a world based on diverse civilizations[7] while reviving its own cultural nationalism[8] to justify authoritarianism. At its core is the spirit of illiberalism, aimed at crushing any traces of the struggle to maintain and spread individual liberty.

AI Surveillance in China

AI is revolutionizing surveillance technology, and China has wasted no time in implementing AI to fine-tune its vast surveillance ecosystem. This article uses the Chinese AI development framework to analyze how China uses AI to push the limits of surveillance. AI development depends on big data, which indicates the

5 Laruelle, "Illiberalism,"304.

6 Steven Feldstein, "Surveillance in the Illiberal State," in *Routledge Handbook of Illiberalism*, ed. András Sajó, Renáta Uitz, and Stephen Holmes (New York and Abingdon: Routledge, 2022), 351–352.

7 Michael Schuman, Jonathan Fulton, and Tuvia Gering, "How Beijing's Newest Global Initiatives Seek to Remake the World Order," *Atlantic Council*, June 21, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-beijings-newest-global-initiatives-seek-to-remake-the-world-order/.

8 Jason Cong Lin, "Rising China Is Not a 'Sick Man' Anymore: Cultural Nationalism in the Xi Jinping Era," *Journal of Contemporary China* 33, no. 145 (January 2024): 83–100. https://doi.org//10.1080/10670564.2023.2214513.

substantial value, variety, volume, and velocity of massive datasets vital to train AI.[9] AI is trained on large datasets to identify patterns, following algorithms or sets of rules. Beraja et al. examine big data, which is essential for developing AI to reveal how the availability of government data to tech firms fast-forwards AI innovation in China.[10] AI development is a policy priority of the Chinese government since it relies on AI, such as face recognition, to suppress social unrest.[11] Ding analyzes China's AI strategy, which is a state-led "national-strategic level priority," and China's aim to become the world's primary AI innovator by 2030.[12] But neither Beraja et al. nor Ding analyze how AI upgrades mass surveillance in China.

Chin and Lin examine the Chinese surveillance state through the eyes of its victims.[13] Theirs is a vital account of how the surveillance state infiltrates people's lives in China. They analyze how this big data collection impacts ethnic Uyghurs in China's western Xinjiang province. The Chinese state takes Uyghurs' blood samples and biometrics, monitors their whereabouts through GPS, and tracks their travel history, online habits, religious practices, and nearly every aspect of their lives.[14] Algorithms guide AI in analyzing personal data, providing parameters for selecting the unsafe ones. Their evidence reveals how AI becomes an authoritarian governance mechanism for social control. However, Chin and Lin do not provide evidence on how AI transforms the surveillance state itself. Peterson examines AI surveillance in China, focusing on "mass control and behavior modification,"[15] a surveillance goal disturbingly common in Xinjiang, and how AI exports replicate similar practices of Chinese mass surveillance in other countries.[16] Feldstein examines how AI empowers autocrats, focusing on big data, machine learning, and algorithm development.[17] China is the leading supplier of AI surveillance technology; however, Japan and the US are also major suppliers.[18] In contrast to democracies, autocracies, illiberal regimes, and regimes with a record human rights abuse show a high probability of using AI technologies for the suppression of civil liberties.[19] Surveillance can face public backlash from civil society and human rights groups. Political pluralism hinders mass surveillance. These constraints are mainly absent in non-democracies.

9 John Gantz and David Reinsel, "Extracting Value from Chaos," International Data Corporation, IDC iView (Framingham, Mass.: IDC, 2011), 6, https://www.yumpu.com/en/document/view/3703408/extracting-value-from-chaos-emc.

10 Martin Beraja, David Y. Yang, and Noam Yuchtman, "Data-Intensive Innovation and the State," NBER Working Papers (Cambridge, Mass.: National Bureau of Economic Research, August 2021), 1–2, https://www.nber.org/papers/w27723.

11 Martin Beraja, Andrew Kao, David Y. Yang, and Noam Yuchtman, "AI-tocracy," *Quarterly Journal of Economics* 138, no. 3 (August 2023): 1349–1402, https://doi.org/10.1093/qje/qjad012.

12 Jeffrey Ding, "The Interests behind China's AI Dream," in *AI, China, Russia, and the Global Order*, ed. Nicholas D. Wright (Washington, DC: Department of Defense, 2018), 37, https://apps.dtic.mil/sti/pdfs/AD1066673.pdf.

13 Josh Chin and Liza Lin, *Surveillance State* (New York: St. Martin's Press, 2022).

14 Chin and Lin, *Surveillance State*, 1–4.

15 Dhalia Peterson, "AI and the Surveillance State," in *Chinese Power and Artificial Intelligence*, eds. William C. Hannas and Huey-Meei Chang, Asian Security Studies, series eds. Sumit Ganguly, Andrew Scobell, and Alice Ba (Abingdon: Routledge, 2023), 205.

16 Peterson, "AI and the Surveillance State," 205.

17 Steven Feldstein, "How Artificial Intelligence Is Reshaping Repression," in "The Road to Digital Unfreedom," ed. Mark F. Plattner, special issue, *Journal of Democracy* 30, no. 1 (January 2019), 40, https://doi.org/10.1353/jod.2019.0003.

18 Steven Feldstein, "The Global Expansion of AI Surveillance" (Washington, DC: Carnegie Endowment for International Peace, 2019), 21, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

19 Feldstein, "The Global Expansion of AI Surveillance," 1–2.

Addressing the conflicting interests of security, surveillance, and human rights, Human Rights Watch (HRW) reverse-engineered a mass surveillance app used by the Xinjiang Police. The app communicates with "the Integrated Joint Operations Platform (IJOP)," a big data analytics system in Xinjiang.[20] HRW reveals how China's AI capabilities translate as a form of authoritarian social control in practice. Focusing on the impact of AI surveillance on civil liberties, Qiang examines how China's surveillance state abolishes freedom.[21] Heeks et al. analyze Chinese digital technology proliferation along the Digital Silk Road (DSR), contributing to the scarce knowledge on this accelerating phenomenon.[22]

This study differs from the above sources as it analyzes the real Chinese AI surveillance architecture, its implementation, and impact. The existing literature mainly focuses on the impact of surveillance. This knowledge base mainly examines the clash of security, surveillance, and human rights. The literature on China's AI technological architecture, which is largely shrouded in mystery, is scarce. Without analyzing China's AI surveillance architecture, it is impossible to fully understand its implementation, impact, and how AI enhances authoritarian governing practices. This study contributes to the literature by focusing on two clear aspects to provide a complete picture of: (1) Chinese AI capabilities, and (2) China's AI implementation, as mapped out using its impact on human rights. It offers clear insights into how exactly AI upgrades both mass surveillance and authoritarianism, allowing it to wield formidable precision control over people.

Methodology

This study: (1) examines Chinese AI surveillance architecture, and (2) analyzes evidence for its use. The study adopts Mantelero and Esposito's Human Rights Impact Assessment (HRIA), a "methodology and a model" to assess the impact of data-intensive AI systems.[23] HRIA offers a framework with which to: (1) examine the varieties and key characteristics of AI products in use, and (2) to assess their impact on human rights. The methodology offers a robust model to analyze: (1) Chinese AI surveillance capabilities and (2) China's AI implementation, exposed through its impact on human rights. The study uses a qualitative approach. Thematic and keyword analysis are used to establish patterns, connections, meaning, ideas, and concepts across the dataset, which creates a comprehensive story concerning AI surveillance architecture, its implementation, and its impact.

This study develops its epistemological position, or its way of knowing AI surveillance in China, identifying three phenomena that resolutely work to build the AI surveillance architecture in China: (1) AI companies, (2) AI technologies, and (3) research. These are the workhorses that build the AI surveillance architecture, offering fundamental insights into mass surveillance in China. The study derives evidence using in-depth qualitative analysis of leading AI companies designated as the national AI team,

20 Human Rights Watch, "China's Algorithms of Repression," Human Rights Watch website, 2019, 1, https://www.hrw.org/sites/default/files/report_pdf/china0519_web5.pdf.

21 Xiao Qiang, "The Threat of Postmodern Totalitarianism," in "The Road to Digital Unfreedom," ed. Mark F. Plattner, special issue, *Journal of Democracy* 30, no. 1 (January 2019): 53, https://doi.org/10.1353/jod.2019.0004.

22 Heeks, et al., "China's Digital Expansion in the Global South: Special Issue Introduction," eds. Heeks et al., special issue, *The Information Society*" 40, no. 2 (March–April 2024): 65–68, https://doi.org/10.1080/01972243.2024.2315868.

23 Alessandro Mantelero and Maria Esposito, "An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA)," *Computer Law & Security Review* 41 (July 2021), https://doi.org/10.1016/j.clsr.2021.105561.

and their AI technologies, verified through essential research published by their scientists and the critical research of the Chinese Academy of Sciences Institute of Automation (CASIA), the leading national AI research center, with a reputation for its brain-inspired research. The study uses Chinese- and English-language sites of AI companies, and their technologies showcased at the World Artificial Intelligence Conference (WAIC), Hunan Security Expo, and Security China Expo. The study then analyzes evidence for AI implementation, examining its impact on human rights in China and beyond. The study uses original accounts from three witnesses: Abduweli Ayup (a former political prisoner in Xinjiang), Ramila Chanisheff (President of the Australian Uyghur Tangritagh Women's Association), and Wendy Rogers (chairperson of the International Advisory Board of the International Coalition to End Transplant Abuse in China [ETAC]), along with several secondary witness accounts and reports from human rights groups, revealing the true impact of Chinese AI surveillance in China and abroad.

Chinese AI Upgrade: Technological Architecture

China aims to achieve optimal social control through AI surveillance. The focus is on monitoring people, a practice justified as "grassroots stability maintenance,"[24] aiming to "establish a hyper-stability structure with new technologies."[25] The Skynet project, initiated in 2005 with 20 million surveillance cameras, marked the initial phase of mass surveillance. It was upgraded to the Sharp Eyes program in 2015, which included initial AI implementation.[26] AI outperforms non-AI surveillance standards. This section analyzes how AI upgrades mass surveillance, eliminating the bottlenecks of real-time analytics of massive surveillance data and producing benchmarks for precision social control.

China's AI national team includes leading e-commerce giant Alibaba, Internet service provider Baidu, Video technology giant Tencent, AI technology provider iFlyTek, leading AI company SenseTime, surveillance equipment supplier Hikvision, telecommunications giant Huawei, AI technology developer Megvii, and AI technology producer Yitu. Alibaba's *Technology Forecast 2023* features "cloud-native security,"[27] which refers to security platforms accessible over the Internet, making them ubiquitous and deployable anywhere.[28] Alibaba highlights "Dual-engine Decision Intelligence," data-driven and mathematical models[29] that optimize AI's decision intelligence.[30] Alibaba notes the revolutionary advancements of computational imaging that surpass conventional imaging technologies as it analyzes the "light field information"[31] for error-free surveillance. Faraday first proposed the concept of a light field, identifying light as an electromagnetic field

24 International Consortium of Investigative Journalists (ICIJ), "Read the China Cables Documents," ICIJ website, November 24, 2019, https://www.icij.org/investigations/china-cables/read-the-china-cables-documents/.

25 Hsin-Hsien Wang and Wei-Feng Tzeng, "Building a Hyper-Stability Structure," *Issues & Studies* 57, no. 01 (March 2021), https://doi.org/10.1142/S1013251121500028.

26 Internet Protocol Video Market, "China Public Video Surveillance Guide: From Skynet to Sharp Eyes," IPVM.com, June 14, 2018, https://ipvm.com/reports/sharpeyes.

27 Alibaba Group, "Alibaba Unveils Top Technology Trend Forecasting for 2023," Alibaba Group website, January 11, 2023, 9–10, https://www.alibabagroup.com/en-US/document-1549931199227494400.

28 Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology website (Gaithersburg, Md.: NIST, 2011), 2, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

29 Alibaba Group, "Alibaba Unveils Top Technology Trend Forecasting for 2023," 15–16.

30 Alibaba Group, 17–18.

31 Alibaba Group, 17.

transferred through vibration.[32] Gershun defined the light field as "the amount of light travelling in every direction through every point of space."[33] Computational imaging and machine vision capture light field information digitally, offering a detailed and comprehensive view.

AI upgrades the core technologies of mass surveillance. AuthenMetric produces industry-standard face recognition[34] and video surveillance systems for AI pattern recognition.[35] AI pattern recognition has made groundbreaking advancements in anti-counterfeiting, vehicle analysis, video analysis, pedestrian detection, and optical character recognition (OCR, a way of converting text images to machine-readable format), among other computer vision areas.[36] DeepEyes Binocular Depth Learning is a face anti-counterfeiting technology that penetrates spoofing, such as glasses, hats or face covering.[37] AuhtenMetric produces the Aojing series Binocular Anti-Counterfeiting Camera, Witness Verification and Live Anti-Counterfeiting Software System, Face Authentication Private Cloud Platform, and Intelligent Monitoring and Detection Platform.[38] These AI systems are instrumental in face detection, comparison, anti-spoofing, and face verification. Deep learning AI detects faces, analyzes facial attributes, and checks age, gender, expression, emotion, appearance, skin condition, and related characteristics to retrieve similar faces from the database for comparison and verification, analyzing multiple factors in real time in a lightning-fast detection, analysis, retrieval, comparison, and a verification process.[39] According to AuthenMetric, the face recognition speed is so fast—just a millisecond response—that it produces beyond-human capability to manage multiple face recognition scenarios in large crowds.[40]

Megvii is a global leader in machine vision and AI face recognition systems. Megvii face technology is based on MegEngine, its proprietary deep learning system. It provides accurate face detection, face attributes analysis, and facial attributes recognition, penetrating any spoofing.[41] Megvii Intelligent IP camera[42] is loaded with algorithms for face recognition through visible and infrared light, intelligent sensing, and rapid detection in complex environments. It includes face capture, face clustering, face anti-spoofing, object linking, detection, and other intelligent operational capabilities.[43] Megvii face recognition uses a database of 10 billion faces to identify face matches; the time for such operations is lightning-fast and works down to milliseconds.[44]

32 Michael Faraday, "LIV. Thoughts on Ray-Vibrations," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 28, no. 188 (May 1846), 346, https://doi.org/10.1080/14786444608645431.

33 Arun Gershun, "The Light Field," Translated by Parry Moon and Gregory Timoshenko, *Journal of Mathematics and Physics* 18 (1939): 55, https://doi.org/10.1002/sapm193918151.

34 AuthenMetric, "Core Technology," AuthenMetric website, http://www.authenmetric.com.

35 AuthenMetric.

36 AuthenMetric.

37 AuthenMetric.

38 AuthenMetric.

39 AuthenMetric.

40 AuthenMetric.

41 Megvii, "AI Algorithms," Megvii website, https://en.megvii.com/technologies/face_recognition.

42 An IP camera is a network camera connected to a network.

43 Megvii, "Intelligent IP Camera (IPC)," Megvii website, https://en.megvii.com/products/hardware/Smart_Network_Camera.

44 Megvii, "Intelligent IP Camera (IPC)."

Cloudwalk develops "closed loop" (continuous machine feedback without human intervention) AI systems, which learn rapidly.[45] Systems map data, learn, and gain insights, providing intelligent decisions. Cloudwalk closed-loop technology has multimodal perception, such as "visual cognition, language cognition, and environmental cognition, [working as an] intelligent decision-making system."[46] It can be used for "*in vivo* (physiological) detection, object detection, voice recognition, language processing, optical character recognition, automated feature generation, video structuring, and machine learning."[47] Cloudwalk partners with the Shanghai Centre for Brain Science and Brain-Inspired Technology to produce AI systems with human-like perception, cognition, contextual awareness, and intent mapping capabilities.[48]

Cloudwalk AI Definition Box, with algorithm engines, performs full target and attribute detection and behavior analysis of humans and vehicles.[49] Huawei produces AI network cameras that capture human figures, motion, and behavior based on behavior trajectories.[50] These cameras can flag behavior as suspicious to send an alarm through the system.[51] China deploys over 500 million security cameras.[52] AI optimizes these cameras, analyzing real-time data and comparing images against massive databases. Huawei produces a cloud Graph Engine Service (GES), a complete AI system with reasoning abilities that emulates the human brain, but with machine precision.[53] Huawei HoloSens intelligent video and data analysis products lead the market. For example, the Huawei HoloSens Intelligent Vision Software Defined Camera (SDC), equipped with an AI processor and recording modules,[54] is not just another surveillance camera but an AI camera with perception.

45 Cloudwalk, "Core Technologies," Cloudwalk website, https://www.cloudwalk.com/en/Technology.

46 Cloudwalk, "Core Technologies."

47 Cloudwalk.

48 Cloudwalk.

49 Cloudwalk.

50 Huawei Forum, "Introduction of Huawei IP Camera Features," March 9, 2023, https://tinyurl.com/mr3dkkzj.

51 Hamza Chanouf, "Leveraging Huawei's AI Camera Technology for Surveillance," Huawei Forum, October 3, 2023, https://tinyurl.com/bdd2z5v2.

52 Paul Bischoff, "Surveillance Camera Statistics," Comparitech website, May 23, 2023, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities.

53 Huawei Cloud, "Graph Engine Service (GES)," Huawei Cloud website, https://www.huaweicloud.com/intl/en-us/product/ges.html.

54 iF Design Award, "HoloSens SDC Security camera," iF Design website, https://ifdesign.com/en/winner-ranking/project/holosens-sdc/317626.

FIGURE 1: Huawei HoloSens SDC.
Source: https://ifdesign.com/en/winner-ranking/project/holosens-sdc/317626.

Hikvision specializes in imaging, video, and AI technologies such as high-definition (HD) and low-light imaging, image stabilization, video streaming with Ultra HD multi-dimensional perception, multi-lens synergy,[55] AI analysis, and cloud computing.[56] Hikvision multi-dimensional perception uses sensing, working beyond visual range as it picks up X-rays, visible light, infrared rays, millimeter waves, sound waves, and temperature variations, sensing the environment.[57] Hikvison thermal imaging and radar-assisted video push the boundaries of surveillance, detecting and tracking movements in real time. Hikvision Intelligent Security Camera is a multi-eye system that uses infrared, starlight, full color, smart, and intelligent image capture capabilities, using smart analysis servers to analyze real-time footage.[58] Hikvision multi-lens cameras capture panoramic and zoom images in real time, adding many inputs for analysis.[59] Hikvision Network Video Recorders (NVR) and analyzers, especially its DeepMind series, offer image-processing AI modules to analyze footage.[60] AI detects objects and movements even in low light conditions using Hikviosn ColorVu[61] and DarkFighterX[62] cameras while deep learning to gain insights. These systems enable a powerful machine perception through deep learning AI.

55 Hikvision, "Multi-Lens Synergy," Hikvision website, https://www.hikvision.com/us-en/core-technologies/multi-lens-synergy.

56 Hikvision, "Unveiling New Technologies," Hikvision website, https://www.hikvision.com/uk/products/IP-Products/Network-Cameras/colorvu-products.

57 Hikvision, "What Is Multi-Dimensional Perception?" Hikvision website, https://www.hikvision.com/au-en/core-technologies/multi-dimensional-perception.

58 Hikvision, "Video Surveillance," http://tinyurl.com/5n6hcjut.

59 Hikvision, "Video Surveillance."

60 Hikvision, "DeepinMind Series NVRs," https://tinyurl.com/4bvp5fsd.

61 Hikvision, "Unveiling New Technologies."

62 Hikvision, "Dark FighterX," https://www.hikvision.com/en/core-technologies/see-clearer-technology/darkfighterx.

Powerful microprocessors bring AI to life guided by algorithms, offering deep learning systems with machine vision and cognition. Smart city automates city functions through digital technology and AI. Smart city is behind a revolution in urban management with its ability to oversee city functions, offering a one-stop solution for city management. In China, the concept of intelligent urban governance is behind its smart city, envisioned to create a world with ubiquitous intelligence. China wants context-aware machines to maintain precision control—and AI comes in handy for this task. The smart city is the blueprint behind the Chinese dream of achieving total control through AI and is the Chinese Communist Party's (CCP) brainchild for its next-generation smart authoritarianism. Smart city comes with safe city technologies. The future of authoritarianism is built into the safe city functions of a smart city, exerting smart authoritarianism.

Cloudwalk's smart city solutions transform governance through big data and AI.[63] It integrates public security systems, enabling full-scale AI surveillance.[64] Megvii "Wanxiang," which translates to English as "panoptic," is a comprehensive city governance software platform.[65] Megvii smart city technology integrates functions such as traffic management, city services, government services, city security, and infrastructure maintenance, implementing AI for comprehensive urban management.[66] Huawei's smart city technology offers integrated digital government, safe city functions, and other city services, seamlessly optimized by AI to ensure the ultimate city function, enhancing its precision governance.[67] Its Intelligent Operations Center (IOC) integrates the city's functions through interagency and interregional collaboration.[68] The SenseTime Urban Management Platform and SenseFoundry Software Platform,[69] with SenseCore AI Cloud,[70] also enable smart cities. AI analyzes real-time city data for insights, alerts, and actions. These systems provide data on city services, mobility, traffic management, emergency responses, security, and environmental protection, integrating services and demands into a smart city AI solution.[71]

Hikvision provides depictions of its formidable safe city AI platform, revealing its characteristics. It is not just another city security platform—it applies unfailing machine learning and machine cognition to several layers of formidable safe city apparatus, which creates benchmarks for smart authoritarianism. It is the ultimate total control ecosystem overseen by the ever-growing perception of AI.

63 Cloudwalk, "Smart Governance and Smart City," Cloudwalk website, https://www.cloudwalk.com/en/Business?id=2.

64 Cloudwalk, "View Intelligence Comprehensive Application Solution," Cloudwalk website, https://www.cloudwalk.com/en/business/program/id/18.

65 Megvii, "Megvii Unveiled Wanxiang," Twitter (X), November 26, 2020, https://twitter.com/Megvii/status/1331921478183387136.

66 Megvii, "Smart City Management Solution," Megvii website, https://en.megvii.com/solutions/Smart_Urban_Governance_Solution.

67 Huawei, "Huawei Smart City Solution," https://www.academia.edu/29082640/Huawei_Smart_City_Solution.

68 Yu Dong, "Build Platforms, Drive Cooperation," *ICT Insights*, no. 23 (August 2018), 14, 24. https://e-file.huawei.com/-/media/EBG/Download_Files/Publications/en/ICT-23-smart-city-en-0312.pdf.

69 SenseTime, "SenseFoundry," SenseTime website, https://www.sensetime.com/en/product-business?categoryId=1077.

70 SenseTime, "SenseCore," https://www.sensecore.cn/about.

71 SenseTime, "Smart City," SenseTime website, https://www.sensetime.com/en/product-index.

FIGURE 2: Hikvision safe city.
Source: Hikvision: Hikvision website, https://www.hikvision.com/en/solutions/solutions-by-industry/safe-city.

Hikvision's safe city program is part of its smart city technology. It has many layers of security:[72] (1) the air control system has high zoom, panoramic series cameras, and drones for ground surveillance; (2) the mobile control system is for agile surveillance; (3) the alarm layer is for emergencies; (4) the ground control system deploys a vast network of cameras and sensors citywide; and (5) the intelligent control system uses AI for analysis, learning, early warning, and response.[73] These five layers create an advanced AI operation to absorb city security under its oversight. This is the foolproof future of smart authoritarianism, where none can hide from discerning machine vision, and the all-knowing, fast-growing, rapid responses come from the AI's situational awareness.

Smart cities are equipped with a city brain, which is a central software system for overall management. Smart city infrastructure, including AI cameras and sensors, collects real-time city data. The city brain software processes this information, using AI, organizing and managing big data. Alibaba Cloud Intelligence Brain[74] processes large multi-source data feeds with speed, accuracy, and efficiency.[75] Megvii Brain++ equips smart cities with cognition, perception, comprehension, and reasoning, elevating city management to an entirely new level.[76] Baidu Brain 6.0 comes with cognition, perception, machine vision, and a fusion of various signals, sensing, and knowledge processing to make for a comprehensive semantic awareness of its environment.[77] Baidu Brain is based on an extensive knowledge graph with "over 550 billion facts" to develop its cognitive understanding of the world.[78] Huawei smart

72 Hikvision, "Advance Security, Safer Society," Hikvision website, https://www.hikvision.com/en/solutions/solutions-by-industry/safe-city.

73 Hikvision, "Advance Security, Safer Society."

74 Alibaba Cloud, "Alibaba Cloud Intelligence Brain," https://archive.org/details/alibaba-cloud-intelligence-brain-2/Alibaba%20Cloud%20Intellgence%20Brain%201.png.

75 Alibaba Cloud, "Alibaba Cloud Intelligence Brain."

76 Megvii, "Brain++, Megvii's Proprietary AI Productivity Platform," Megvii website, https://en.megvii.com/brainpp.

77 Baidu Research, "Exploring Baidu Brain 6.0," Sep 24, 2020, Baidu website, http://research.baidu.com/Blog/index-view?id=147.

78 Baidu Research, "Exploring Baidu Brain 6.0."

city's brain seamlessly manages 10 key city operations and 50 government services.[79] SenseTime city brain covers "all walks of life," offering smart city solutions with smart security, smart economy, and a smart community to realize the full potential of an integrated smart society.[80]

What we understand as mass AI surveillance seamlessly assimilates into the smart city ecosystem. As Ding states, "The expansion of surveillance in Xinjiang is part of a broader, nationwide effort to build 'safe' and 'smart' cities."[81] AI surveillance increasingly occurs in rapidly expanding smart cities. Early smart cities in Xinjiang, such as Karamay, integrated all aspects of life, creating a "computerized Police State."[82] Feldstein underlines the key systems that propagate AI surveillance globally: (1) smart city/safe city platforms, (2) facial recognition systems, and (3) smart policing.[83] However, facial recognition and smart policing are increasingly becoming part of the safe city technologies of the smart city.

The first batch of national smart city pilot projects was launched in August 2013.[84] China had 290 smart city pilot projects by 2015; pilot cities are completed in 3–5 years.[85] The national smart city pilots, under the Ministry of Housing and Urban-Rural Development and the Ministry of Science and Technology, was initiated in 2012.[86] This initiative was part of the urbanization strategy of the CCP Central Committee and the State Council.[87] Initially, 80 billion RMB was invested in building smart cities in China.[88] Between 2013–2015, there were nine smart city pilot projects in Xinjiang province: in Korla, Kuitun, Ürümqi, Karamay, Yining, Changji City, Fuyun County, Altay Prefecture, and in the Xinjiang Production and Construction Corps (XPCC) localities, comprising Shihezi City and Wujiaqu City.[89] Xinjiang's capital, Ürümqi, was developed as a smart city in 2013. According to an article in the *Xingtuan Daily*,[90] the completion of the city brain in Shihezi smart city will integrate all other sectors, such as the city's comprehensive grid management center, emergency command center, and government service hotline center, to create a smart command center integrating "city services, social governance, and emergency command."[91] The grid system[92] is a comprehensive social governance system wherein

79 Huawei, "Smart City Solution Service," Huawei website, https://e.huawei.com/en/solutions/services/smart-city.

80 SenseTime, "Sensecore Smart City and Commerce," https://www.sensecore.cn/en/solution/zhihuichengshiyushangye.

81 Ding, "The Interests behind China's AI Dream," 39.

82 Mafeez Ahmed, "Silicon Valley's Scramble for China," Coda, May 24, 2019, https://www.codastory.com/authoritarian-tech/silicon-valleys-scramble-for-china.

83 Feldstein, "The Global Expansion of AI Surveillance," 1.

84 Liu Shunhai, "List of National Smart City Pilots: There Are Currently 290 National Smart City Pilots," Sohu.com, April 06, 2019, https://www.sohu.com/a/306290066_416839.

85 Liu, "List of National Smart City Pilots."

86 Liu. "List of National Smart City Pilots."

87 Shifu Wang, Dantong Chen, Lianbi Liu, "The Practice and Prospect of Smart Cities in China's Urbanization Process," *Frontiers of Urban and Rural Planning*, 1, no.7 (2023): 3, https://doi.org/10.1007/s44243-023-00007-w.

88 Liu. "The Practice and Prospect of Smart Cities in China's Urbanization Process"

89 Liu. "The Practice and Prospect of Smart Cities in China's Urbanization Process"

90 *Xingtuan Daily*, also known as *Xinjiang Daily*, is the official newspaper of the Chinese Communist Party (CCP) in the Xinjiang region.

91 Kang Lizhu and Liu Weisheng, "Shihezi City Invests 32.42 Million Yuan to Promote the Construction of Smart City," *Xingtuan Daily*, June 9, 2020, http://news.ts.cn/system/2020/06/09/036306522.shtml.

92 Jianhua Xu and Siying He, "Can Grid Governance Fix the Party-State's Broken Windows? A Study of Stability Maintenance in Grassroots China," *China Quarterly* 251 (June 2022): 843–865, https://doi.org/10.1017/S0305741022000509.

cities are divided into easily manageable units for monitoring. Smart cities are ecosystems for precision social control.

Human Rights Impact Assessment

The policy plan for AI implementation is laid out in key policy directives such as the State Council's Next Generation Artificial Intelligence Development Plan of July 8, 2017.[93] This is "the key guiding document of China's AI strategy in both the domestic and international realms."[94]

The document explains how it will accelerate the in-depth application of AI to improve social governance intelligence.[95] The directive's instructions seek to ensure public security by establishing an "AI public security monitoring, early warning, and control system."[96]

> Focusing on the urgent needs of comprehensive social governance, crime investigation, counterterrorism, etc., develop intelligent security and police products that integrate multiple detection and sensing technologies, video image information analysis and recognition technologies, biometric recognition technologies, and an intelligent monitoring platform.[97]

The companies of China's AI national team produce AI technologies, spearheading the state agenda for AI deployment. Chinese society is under the CCP's watchful eye, snooping into every aspect of people's lives. The Xinjiang Uyghur Autonomous Region is subjected to draconian surveillance that is justified in terms of counterterrorism and national security.[98] Freedom House highlights the Chinese official policy of suppressing ethnic minorities in "Xinjiang, Tibet, and Inner Mongolia."[99] The China Cables, a trove of leaked Chinese government files, reveal how the CCP justifies mass surveillance in Xinjiang, claiming to maintain "social stability" or "grassroots stability."[100] The CCP uses "grassroots stability maintenance forces" and "Autonomous Regional Party Committee Command," using the Integrated Joint Operations Platform (IJOP),[101] a mass AI surveillance system in Xinjiang.

In 2018, the UN Committee on the Elimination of Racial Discrimination revealed that it has credible evidence that China holds one million ethnic Uyghurs in internment camps in Xinjiang.[102] According to Human Rights Watch, by June 2022, China held around "half a million people" in arbitrary detention in a vast network of facilities

93 State Council, Next Generation Artificial Intelligence Development Plan (新一代人工智能发展规划: Xīn yīdài réngōng zhìnéng fāzhǎn guīhuà), July 8, 2017, https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

94 Ding, "The Interests behind China's AI Dream," 37.

95 State Council.

96 State Council.

97 State Council.

98 State Council.

99 Freedom House, *Freedom in the World 2023* (Washington, DC: Freedom House, 2023), 7, https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf.

100 ICIJ, "Read the China Cables Documents."

101 ICIJ.

102 Stephanie Nebehay, "U.N. Says It Has Credible Reports That China Holds Million Uighurs in Secret Camps," Reuters (news agency), August 12, 2018, https://www.reuters.com/article/us-china-rights-un/u-n-says-it-has-credible-reports-that-china-holds-millionuighurs-in-secret-camps-idUSKBN1KV1SU/.

in Xinjiang.[103] The target is Uyghurs and other Turkic Muslims, whose children are removed to state-run "boarding schools" or orphanages. In collaboration with SenseTime and Megvii, Leon Technology established safe city face recognition systems in Xinjiang for mass surveillance.[104] In 2018, the Xinjiang Police Files, a cache of leaked data from the police servers in Xinjiang, revealed to the world the true magnitude of the Chinese state's mass incarceration of Uyghurs and other ethnic minorities.[105] The Qaraqash List, a 137-page document leaked in 2020, further revealed mass surveillance and arbitrary detention in Qaraqash, Xinjiang.[106]

The next section analyzes China's AI implementation and its impact, examining what China calls "social stability maintenance," "social governance," and "grassroots stability maintenance," and what the wider world has identified as mass surveillance, "mass control and behaviour modification,"[107] and authoritarian repression.

Big Data in Practice[108]

The Chinese State Security Police detained Abduweli Ayup, a Uyghur scholar, linguist, and poet, for 15 months from August 2013 to November 2014. He was subjected to torture and rape. His crime was starting a Uyghur-language kindergarten in Kashgar, Xinjiang. The State Security Police accused him of trying to separate Xinjiang by promoting the Uyghur language. His story reveals the true impact of mass surveillance on its individual victims.

Ayup first saw a camera that recognized him in 2005 at the Chinese Embassy in Ankara, Turkey. He was a visiting scholar in Ankara, and he went to the Chinese Embassy upon request and pressed the button on the gate. It called his name, asking him to come in. He was thinking, "How do they know?" He went inside and probed, "I just came in front of your gate, and you called my name. How do you know it's me?" They answered, "We have a camera."[109] This incident left a strong impression on him. In 2008, the Chinese government installed cameras on Ürümqi streets in Xinjiang before the Summer Olympics torch relay in July 2008. When riots began in Ürümqi on July 5, 2009, many people died, and thousands were arrested. The Ürümqi riots were a direct consequence of the oppression faced by the ethnic Uyghurs in Xinjiang.[110] "The cameras installed in 2008 for the Olympics worked well to arrest people; the Chinese government learned a lot from this protest and learned a lot about the participants because they have cameras."[111]

Ayup filled out a questionnaire that collected data on his religious practices: "How many Qurans do you have at home? How many times have you visited Mecca? Do

103 Maya Wang, "China's 'Beautiful Xinjiang' Continues to Oppress Uyghurs," September 13, 2023, https://www.hrw.org/news/2023/09/13/chinas-beautiful-xinjiang-continues-oppress-uighurs.

104 Jeffery Ding, "Complicit: China's AI Unicorns and the Securitization of Xinjiang," ChinAI Newsletter no. 29, September 24, 2028, https://tinyurl.com/y5h7nrdv.

105 Xinjiang Police Files, https://www.xinjiangpolicefiles.org.

106 Uyghur Human Rights Project, "Ideological Transformation," Uyghur Human Rights Project website, February 2020, p. 5, https://docs.uhrp.org/pdf/UHRP_QaraqashDocument.pdf.

107 Peterson, "AI and the Surveillance State," 205.

108 The following account is based on the original, consented, face-to-face personal interview, using an open-ended, unstructured questionnaire with Abduweli Ayup on July 21, 2024.

109 Abduweli Ayup, personal interview.

110 Human Rights Watch, "We Are Afraid to Even Look for Them: Enforced Disappearances in the Wake of Xinjiang's Protests," news release, HRW.org, October 21, 2009, https://www.hrw.org/report/2009/10/20/we-are-afraid-even-look-them/enforced-disappearances-wake-xinjiangs-protests.

111 Ayup, interview.

you know Quranic verses? If you know, how did you learn? Who taught you?" etc. Ayup's DNA, biometrics, and human gait were taken. Gait recognition maps the human silhouette, motion, walking posture, hip extension, or how a person stands and walks, which indicates physiological and behavioral biometrics to guide AI pattern recognition.[112] Gait indicators are part of harvesting personal data for mass surveillance.

> They collect fingerprints, saliva, blood samples, iris scans, and toe prints. They take photos and videos from every angle: walk this way, walk that way, sitting, standing, looking this and looking that, voice samples, you read a book and then they record it. For example, if I call my family, they know it's me.[113]

Chin and Lin also reveal how the Chinese state collects blood, fingerprints, voice samples, and recordings of facial features from different angles.[114] After his encounter at the Chinese Embassy in Ankara, cameras started to identify Ayup. AI matches personal profiles in real time when people pass through checkpoints. According to Ayup, he swipes his ID card, and the authorities know everything: "you stayed in this hotel, you went to this place, they tell me what happened to me, where I live, where I go, everything … How do you know? Because you swipe your ID card, our camera shows up, and we will know."[115] Once Ayup went to another city in May 2013. The People's Liberation Army (PLA) stopped him on the way. They asked him to stand, took a photo, and said, "You are blacklisted." He wondered how they knew; it was only a photo, and they did not ask to swipe his ID. If they did, Ayup knew it would show up. It was the first time he heard about the Integrated Joint Operations Platform (IJOP) database. "It is called big data: your electricity card, your ID card, your bank account, library card, cell phone, shopping history, everything in one data[base]; they take a picture and know who I am, it's called face recognition."[116]

The leaked "Qaraqash List" shows how IJOP even monitors personal relationships, and people were detained and sent to internment camps based on regular activities such as going abroad, going abroad for pilgrimage, having contacts overseas, having a beard, praying regularly, and even applying for a passport.[117] In 2014, the Chinese government built walls around Uyghur neighborhoods with gates equipped with face recognition machines. People must swipe ID cards and look at the screen that takes a photo. There is a button: if it turns green, the person can go through; if it turns yellow, the person will be questioned; if it turns red, police will be there to take the person to the police station.[118] For Uyghurs, there is a road colored in yellow and red. When they drive, they must get out and go to the machines to verify. "Lots of cameras, cameras are everywhere; if you are a blacklisted family, they install a camera at your home; every mosque had cameras to be watched and recorded."[119]

At the prison, the tyranny of machines reached a whole new level. There were three cameras inside the cell. Once, when the inmates were eating, a person next to him asked Ayup whether he knew about prayer times. Before Ayup answered, the camera

112 Watrix AI, "Gait Recognition," Watrix website, http://watrix.ai/index.

113 Ayup, interview.

114 Chin and Lin, *Surveillance State*, 1.

115 Ayup, interview.

116 Ayup.

117 Uyghur Human Rights Project, "Ideological Transformation," 14–15.

118 Ayup, interview.

119 Ayup.

shouted, "Shut your mouth." Ayup assumed that the cameras were able to detect movements. He then realized that they were capable of listening. Ayup was taken out for questioning. They asked him what he was doing. He said, "I did not do anything; someone asked me a question, and before I answered, the camera watched and shouted. I wanted to say I don't know."[120] They showed Ayup a big screen constituting small screens with room numbers, which can be enlarged: "Look what we have here, cameras take pictures, video, and audio. Everything you are doing here is under documentation."[121]

In the prison, Ayup and others were subjected to medical tests. The authorities distribute pills to prisoners to swallow in front of prison guards. Prisoners get a paper to sign but are not allowed to read it. Abuduweli revealed this experience to the journal *Nature*.[122]

> One person, he rejected, he just pretends to swallow it, and puts it in the mouth, and keeps it, then spit it out to the toilet. The camera watched and shouted. He was taken out. He disappeared. One Uyghur person died because he took that medicine.[123]

The Uyghur population is under mass surveillance. Uyghurs, including children, are given questionnaires, aiming to record their behavior and religious practices. Every 10 Uyghur families were made into one unit. Once in every three weeks, everyone must write a confession letter reporting the behavior of others, such as, "My father prays at home, my sister reads Uyghur history books," etc., which will implicate them. "People became afraid to talk to each other."[124] Uyghurs must download an app. The app controls everything. This is the infamous Jingwang, or the Xiangjiang police app, which is a spyware app. Rajagopalan explains how this app scans mobile phones, transferring their contents out.[125]

The China Cables, the leaked Chinese government files, give instructions to "fully draw on grassroots stability maintenance forces and ten households joint defense [a kind of grassroots unit where the CPP organizes groups of 10 households together into a defensive unit] and combine it with [the] 'Integrated' [Joint Operations] platform."[126] It shows how the government uses Grassroots Stability Maintenance Forces and Ten Household Joint Defense to feed data into the Integrated Joint Operations Platform (IJOP), an AI analytics system at the heart of mass surveillance in Xinjiang.

> When I swipe my ID card, they always arrest me. I was arrested three times. I left China in August 2015. After I got released, I had a psychological problem that I always feel that I'm under control, I'm under surveillance. I don't feel comfortable.[127]

120 Ayup.

121 Ayup, interview.

122 Dyani Lewis, "Unethical Studies on Chinese Minority Groups are Being Retracted—but not Fast Enough, Critics Say," *Nature,* January 24, 2024, https://www.nature.com/articles/d41586-024-00170-0.

123 Ayup, interview.

124 Ayup.

125 Megha Rajagopalan, "China Is Forcing People to Download an App That Tells Them to Delete 'Dangerous' Photos," BuzzFeed News (news site), April 10, 2018, https://www.buzzfeednews.com/article/meghara/china-surveillance-app.

126 ICIJ, "Read."

127 Ayup, interview.

Culture of Surveillance[128]

As Ramila Chanisheff, President of the Australian Uyghur Tangritagh Women's Association, explains:

> Surveillance is all across Xinjiang. Surveillance cameras were put up, whenever they stop you, they put a software on your mobile phone, so they can keep tabs on what you say, who you talk to, and what you search; it is a part of life. … It did not start there; the whole China has always been under surveillance. It has been happening since Mao Zedong's time. It's neighbourhood watching, listening and dobbing in.[129] Back then, you have these nosy grandmothers and grandpas, who come around and listen, ask questions, and report back to the local police. It was tighter during Mao Zedong's time, because they wanted to get rid of capitalism or any kind of freedom. It's over a billion people, that's how they surveil them back then, it's word of mouth. … They ask children, what did you talk about, what did you do, are your parents praying, or your parents fasting. Children don't know, they tell them, and the whole family is subjected to investigation. It's in Chinese culture to do this kind of things, Chinese are heavily surveilled people, people report neighbors and friends to save themselves. … During the Cultural Revolution in the 60's and 70's, people live[d] through this. People spent a long time in jail, without any trial or evidence, simply because someone accused them of something. My grandmother spent two years in jail because she shared the same name of someone that they called a separatist. My grandfather spent 17 years in jail because he could speak Russian, and they thought he was a Russian spy. It's not just my family, it happened to everyone. … People disappear and are held in re-education camps. Some people are never found again; millions of Tibetan and Uyghur children are in forced orphanages.[130]

The UN Office of the High Commissioner for Human Rights (OHCHR) has expressed serious concern about the forced separation of a million children from ethnic minority backgrounds. These children have been forcibly taken from their families and placed in state-run boarding schools as part of the Chinese government's mandatory cultural assimilation program.[131] Chanisheff's account shows that China has always been a tightly controlled society, emphasizing the vast surveillance capabilities required to maintain such a draconian system of social control. Advances in AI, big data, and machine learning have now understandably enhanced this system of comprehensive social control.

128 The following account is based on a consented Zoom interview with Ramila Chanisheff, President, Australian Uyghur Tangritagh Women's Association, August 28, 2024.

129 *To dob [someone] in*: British/Australian slang, meaning to inform, tell, snitch, or rat on someone.

130 Chanisheff, interview.

131 United Nations Office of the High Commissioner for Human Rights (OHCHR), "China: UN Experts Alarmed by Separation of 1 Million Tibetan Children from Families and Forced Assimilation at Residential Schools," UN OHCHR, February 6, 2023, https://www.ohchr.org/en/press-releases/2023/02/china-un-experts-alarmed-separation-1-million-tibetan-children-families-and.

FIGURE 3: This photo is from an original video that made headlines in 2019.[132] It shows the transfer of prisoners in Xinjiang.[133]

Falun Gong (Falun Dafa) Incarcerations[134]

Adherents of the Taoist-Buddhist fusion religious movement known as Falun Gong in China face the brunt of mass surveillance and consequent incarceration. An independent China Tribunal held two sessions in London to gather evidence on forced organ harvesting in China in 2018 and 2019. The tribunal investigated witness testimonies, interviewed witnesses, and systematically examined evidence. As the tribunal's judgment states, the tribunal is convinced "beyond reasonable doubt" that the alleged crimes against humanity against Falun Gong practitioners and Uyghurs in China have indeed occurred.[135] According to Rogers, "The Tribunal's findings are significant as those resulted from an independent and rigorous process and involved individuals with impeccable credentials, such as Sir Geoffrey Nice."[136]

The collection of bio-identifiers for AI analytics serves many purposes. Rogers said, "A person testified to the tribunal, who believes that the blood samples from prisoners were added to a database; that expert thought that given the speed in which they can match recipients with organs, they must have databases to manage that information."[137] Providing evidence to the China Tribunal, Maya Mitalipova,

132 BBC, *Andrew Marr Show*, July 20, 2020, https://www.bbc.com/news/uk-politics-53463403.

133 War on Fear, "新疆：新讲 Xinjiang：a New Explanation," War on Fear战斗恐惧 YouTube channel, September 17, 2019, https://www.youtube.com/watch?v=gGYoeJ5U7cQ.

134 The following account is based on the consented informal personal discussion with Wendy Rogers, distinguished professor of clinical ethics at Macquarie University, August 16, 2024. Rogers is an expert in AI in healthcare and an eminent transplant ethicist who was recognized as one of the "Ten people who helped shape science" in the journal *Nature*'s top 10 list in 2019. She is the chair of the International Advisory Board of the International Coalition to End Transplant Abuse in China (ETAC).

135 The Independent Tribunal into Forced Organ Harvesting from Prisoners of Conscience in China, *Judgment* (London: The China Tribunal, March 1, 2020), 156, https://chinatribunal.com/final-judgment.

136 Rogers, personal discussion.

137 Rogers, discussion.

the Director of the Human Stem Cell Laboratory at the Massachusetts Institute of Technology (MIT), noted in her testimony to the China Tribunal:

> What for the Chinese government is using a million people's DNA-sequenced data? … State-approved DNA sequencing of the entire Muslim population of Xinjiang without informed consent is another proof of evidence that the knowledge obtained from genomic data analysis will be used to determine if a patient and a potential donor are a better match for the long-term success of transplantation.[138]

An evidence-based account published by the International Coalition to End Transplant Abuse in China, which became widely known as *The Update*, reveals the horrific details of forced organ harvesting.[139] A witness explains how prisoners signed counterfeit voluntary donation forms without their consent.[140] An estimated 65,000 Falun Gong members were killed for their organs,[141] and most prisoners' organs were removed while they were still alive.[142] Based on his work, one of the authors, Ethan Gutmann, received a nomination for the Nobel Peace Prize in 2017.[143] "There's a surgeon who was involved and is now living in the West, Enver Tohti, who removed organs from someone who was not dead at the time. It was someone who had been shot, a prisoner."[144] The China Tribunal heard the testimony of Tohti as an eyewitness to forced organ harvesting in China.[145] The *British Medical Journal* (BMJ) reported the findings of the China Tribunal.[146]

Dolkun Isa, whose elderly mother Ia Memet died in a camp, testified to the tribunal: "Since 2017, the government took blood samples and DNA from 11 million people."[147] In an earlier testimony to the UK Parliament, Isa also underlined the "dual use" of the AI-managed databases:

> Collecting blood samples allowed the Chinese government to establish a genetic database of the Uyghur people to further monitor, control, and repress them. This genetic information also facilitates organ harvesting, making it easier to compare blood types and compatibility of potential Uyghur victims.[148]

These practices were mostly enabled by mass surveillance and AI big data analytics. Is this a problem specific to China, affecting only the people living there?

---

138 China Tribunal, 486, 488.

139 David Kilgour et al., *Bloody Harvest / The Slaughter: An Update*, International Coalition to End Transplant Abuse in China, April 2017, p. 361, 364, https://endtransplantabuse.org/an-update.

140 Kilgour et al., *The Update*, 401.

141 Kilgour et al., 10.

142 Kilgour et al., 100.

143 End Transplant Abuse in China, "Ethan Gutmann Receives Nomination for the 2017 Nobel Peace Prize," https://endtransplantabuse.org/ethan-gutmann-nomination-2017-nobel-prize.

144 Rogers, discussion.

145 China Tribunal, *Judgment*, 52.

146 Richard Hurley, "China's Forced Organ Harvesting Constitutes Crimes against Humanity, Informal London Tribunal Finds," *British Medical Journal* 365 (June 18, 2019), 4287, https://doi.org/10.1136/bmj.l4287.

147 China Tribunal, *Judgment*, 517.

148 World Uyghur Congress, "WUC President Speaks on Organ Harvesting at Roundtable in the UK Parliament," World Uyghur Congress website, December 14, 2017, https://www.uyghurcongress.org/en/WUC, -president-speaks-on-organ-harvesting-and-uyghurs-at-hearing-in-the-uk-parliament/.

China follows a uniquely original model of geopolitical expansion. As Bradford notes, China transfers its "digital authoritarianism through infrastructure."[149] Its Belt and Road Initiative (BRI) is the largest infrastructure development project in the world, expanding into over 146 countries.[150] BRI is at the heart of a new world being built by China for Chinese primacy. As Xi Jinping asserts, "We will work to build a new type of international relations" through BRI.[151] The Digital Silk Road (DSR) expands digital connectivity along the colossal infrastructure route of the BRI. DSR builds smart cities, wiring the BRI landscape through Chinese digital technologies. The DSR is a vital element of China's global ambitions; it implements technological infrastructure along with the BRI, rewriting global norms that govern such technologies.[152] The DSR promotes political illiberalism, as digital technology plays a pivotal role in suppressing liberal values.[153] The BRI and DSR are original models of geopolitical expansion, in which AI plays a major role in enhancing authoritarian governance and exerting social control. Alibaba's city brain has already been implemented in 23 Asian cities.[154] Huawei alone provides safe city solutions to more than 700 cities in 100 countries and regions.[155] Huawei is part of China's AI National Team, leading the CCP's aim for global AI leadership by 2030.[156] As Huawei asserts, "A magnificent, intelligent world is fast approaching";[157] it is the "intelligent world of 2030."[158]

China has the world's largest mass surveillance network. Chinese surveillance technology replicates its impact abroad. Uyghurs are being extradited back to China. According to Ayup, "China sold surveillance technology to the United Arab Emirates (UAE),"[159] and "In Turkey, they use Chinese Huawei 5G; Turkey is a dangerous place to Uyghurs because those surveillance cameras are already installed there."[160] Freedom House has uncovered repression against Uyghurs in Turkey.[161] Amnesty International collected information from "approximately 400 Uyghurs, Kazakhs,

149 Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 290, https://doi.org/10.1093/oso/9780197649268.003.0009.

150 Green Finance & Development Center, "Countries of the Belt and Road Initiative (BRI)," GreenFDC.org, December 2023, https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri.

151 Xi Jingping, Speech Marking the 100th Anniversary of the CCP, July 1, 2021, http://www.xinhuanet.com/english/special/2021-07/01/c_1310038244.htm.

152 Article 19, *The Digital Silk Road* (London: Article 19, March 2024), 6, https://www.article19.org/wp-content/uploads/2024/04/DSR_final.pdf.

153 Clayton Cheney, "China's Digital Silk Road," *Pacific Forum* vol. 19, working paper no. 8 (July 2019), 1, https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf.

154 Alibaba Clouder, "City Brain Now in 23 Cities in Asia," Alibaba Cloud blog, October 28, 2019, https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479.

155 Huawei, *2018 Annual Report*, Huawei website, 30, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en.pdf?la=zh.

156 Sarah Dai, "China Adds Huawei, Hikvision to Expanded 'National Team' Spearheading Country's AI Efforts," *South China Morning Post*, August 30, 2019, https://www.scmp.com/tech/big-tech/article/3024966/china-adds-huawei-hikvision-expanded-national-team-spearheading.

157 Huawei, *Intelligent World 2030* (Shenzhen: Huawei. 2021), 13, https://www-file.huawei.com/-/media/corp2020/pdf/giv/intelligent_world_2030_en.pdf.

158 Huawei, *Intelligent World 2030*, 12.

159 Ayup, interview.

160 Ayup.

161 Freedom House, "Turkey: Transnational Repression Host Country Case Study," Freedom House special report, 2022, https://freedomhouse.org/report/transnational-repression/turkey-host.

Uzbeks," and other Chinese minorities living in 22 countries, revealing China's intimidation of them and coercion of their families back home.[162]

The Uyghur Human Rights Project (UHRP) and the Oxus Society for Central Asian Affairs, based on their China's Transnational Repression of the Uyghurs Database, have produced several rare and comprehensive assessments on China's repression of Uyghurs and Chinese minorities living in the Arab world.[163] As Freedom House notes, there is a "much broader system of surveillance" behind the repression against Chinese exiles overseas.[164] In Southeast Asia and the Middle East, Chinese surveillance is in full swing as China works with authoritarian regimes to track down Uyghurs. Chinese tech companies are behind the "Saudi smart city projects, Morocco Digital 2025, Digital Egypt, Smart Dubai 2021, etc., which are national strategies to transform digital applications."[165] Saudi Arabia, Egypt, and the UAE are dangerous places for Chinese minorities.

The Shanghai Security Files, a database from the Shanghai National Police Database leaked in July 2022, included the personal information of more than one billion people.[166] This leak showed how prominent international figures, such as former Australian Ambassador Geoff Miller, had been flagged once they visited China.[167] The surveillance system flags people for further monitoring. Cyber security expert Robert Potter explains the leaked files as "a piece of a larger database feeding into a burgeoning mass surveillance system."[168] China uses the BRICS organization, the Belt and Road Initiative, the Forum for China-Africa Cooperation (FOCAC), and the China-Africa Defense Forum to promote Chinese surveillance systems on the pretext of counterterrorism and safe city projects in the Global South.[169] Poireault delves into the I-Soon hack that occurred in 2024 and the lengths to which China goes to obtain data through cyber espionage, targeting countries worldwide.[170] The I-Soon hack compromised the data of the Chinese security company of the same name, which serves as a contractor to China's Ministry of Public Security (MPS), shedding light on the inner workings of the commercial cyber espionage industry in China.[171]

---

162 Amnesty International, "Nowhere Feels Safe," Amnesty.org, Feb 21, 2020, https://www.amnesty.org/en/latest/research/2020/02/china-uyghurs-abroad-living-in-fear.

163 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, "Beyond Silence: Collaboration between Arab States and China in the Transnational Repression of Uyghurs" (Washington, DC: UHRP, March 24, 2022), https://uhrp.org/report/beyond-silence-collaboration-between-arab-states-and-china-in-the-transnational-repression-of-uyghurs/.

164 Freedom House, "Out of Sight, not out of Reach" (Washington D.C., FH, Feb 2021), 15, https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.

165 Dale Aluf, "China's Digital Footprint Grows in the Middle East & North Africa," Mapping Global China (website), https://mapglobalchina.com/chinas-digital-footprint-grows-in-the-middle-east-north-africa/.

166 Yiwen Lu, "Hackers Claim They Breached Data on 1 Billion Chinese Citizens," *Washington Post*, Business section, July 6, 2022, https://www.washingtonpost.com/business/2022/07/06/china-hack-police/.

167 Sean Rubinsztein-Dunlop and Echo Hui, "Australians Flagged in Shanghai Security Files Which Shed Light on China's Surveillance State and Monitoring of Uyghurs," ABC News (Australia), April 1, 2021, https://www.abc.net.au/news/2021-04-01/shanghai-files-shed-light-on-china-surveillance-state/100040896.

168 Rubinsztein-Dunlop and Hui, "Australians Flagged in Shanghai Security Files Which Shed Light on China's Surveillance State and Monitoring of Uyghurs."

169 Bulelani Jili, "China's Surveillance Ecosystem & The Global Spread of Its Tools," Atlantic Council, Digital Forensic Research Laboratory, October 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/.

170 Kevin Poireault, "I-Soon GitHub Leak: What Cyber Experts Learned about Chinese Cyber Espionage," *Infosecurity Magazine*, Feb 27, 2024, https://www.infosecurity-magazine.com/news-features/isoon-github-leak-chinese-cyber/.

171 Poireault, "I-Soon."

UHRP and Oxus have recorded 7,078 cases of Chinese repression abroad since 1997.[172]

The tech companies responsible for the algorithmic repression of Uyghurs in China are involved in "smart-city programs along the Digital Silk Road, including in Central Asia and Pakistan—significant hubs for transnational repression of Uyghurs."[173] UHRP and Oxus reveal how Ahmad Talip was imprisoned in Dubai in 2018 and forced to give a blood sample as part of China's surveillance of Uyghurs abroad.[174] Chinese repression overseas has become widespread since 2017 due to "algorithmic surveillance," in which data is fed into the massive IJOP database.[175] The IJOP algorithms-based flagging of people results in the Chinese state doing what UHRP and Oxus call "internationalizing algorithmic surveillance systems used in the Uyghur region."[176] "Transnational digital surveillance" is at the heart of monitoring Uyghurs living overseas.[177] Egyptian authorities tracked down and detained Uyghurs in Egypt at the request of the Chinese state in 2017.[178] Human Rights Watch issued a plea not to deport Uyghurs to China, witnessing one such mass detention in Jul7 2017.[179]

In an alarming development, Huawei's role in building Hajj and Umrah digital services in Saudi Arabia resulted in the surveillance of Uyghur pilgrims.[180] Uyghurs living in Europe faced risks when they visited Saudi Arabia for Hajj. The Chinese Security Services held Norway-based Omer Rozi's mother during the latter's Hajj pilgrimage in Saudi Arabia in 2008. The Chinese wanted Omer but failed to lure him into Saudi Arabia using his mother.[181] Students Abdusalam Mamat and Yasinjan were ordered back to China from Egypt and were detained and later died under suspicious circumstances in Chinese police custody in 2015.[182] Chinese police were present in Dubai in 2017, tracking down Uyghurs, showing how China cracks down on people across many countries.[183] China is effectively surpassing the world in repressive technology, such as AI surveillance, which it deploys along the BRI corridors, creating digital topographies such as smart cities. All this evidence proves how Chinese smart cities proliferate repressive algorithms in China and beyond.

The Chinese surveillance state and its resulting internment camps are gross violations of the Universal Declaration of Human Rights,[184] of which China is a signatory.

172 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, " 'Your Family Will Suffer': How China Is Hacking, Surveilling, and Intimidating Uyghurs in Liberal Democracies," (Washington DC: UHRP, 2021), 4, https://uhrp.org/wp-content/uploads/2021/11/UHRP-Your-Family-Will-Suffer-Report.pdf.

173 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, " 'Your Family Will Suffer,' " 44.

174 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 45.

175 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 46.

176 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 11.

177 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 3.

178 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 2.

179 Human Rights Watch, "Egypt: Don't Deport Uyghurs to China," HRW.org, July 7, 2017, https://www.hrw.org/news/2017/07/08/egypt-dont-deport-uyghurs-china.

180 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, "Beyond Silence," 3.

181 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 31.

182 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 13; Middle East Monitor, "2 Uyghur Students Returned from Egypt, Dead in China Police Custody," MEMO (news site), December 22, 2017, https://www.middleeastmonitor.com/20171222-2-uyghur-students-returned-from-egypt-dead-in-china-police-custody/

183 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 24–25.

184 United Nations, *Universal Declaration of Human Rights*, UN.org, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Assessing the situation in Xinjiang, the UN Office of the High Commissioner for Human Rights concedes that the "Allegations of patterns of torture, or ill-treatment, including forced medical treatment and adverse conditions of detention, are credible."[185] It noted the large-scale arbitrary deprivation of liberty for members of Uyghur and other Muslim minorities in Xinjiang in the so-called Vocational Education and Training Centers (VETC) and other facilities.[186] Alarmingly, China tries to alter international human rights norms and procedures, leveraging its influence over the UN human rights bodies:[187]

> the evidence considered by Tribunal members overall left them certain that throughout the last 20 years, the PRC has been in substantial breach of at least Articles 2, 3, 5, 6, 7, 8, 9, 10, 11, and 13 of the Declaration, and of Articles 6, 7, 9, 10, 12 and 14 of the International Covenant on Civil and Political Rights of 16 December 1966.[188]

Indiscriminate DNA collection, even from children, and "genomic surveillance" grossly violate "the UN Universal Declaration on the Human Genome and Human Rights, the UN International Declaration on Human Genetic Data, the International Covenant on Civil and Political Rights, and the UN Convention on the Rights of the Child."[189] The evidence of the technological prowess involved, its application for draconian surveillance, and China's mass incarceration of ethnic minorities show how algorithmic surveillance tracks down people in China and beyond. The UN human rights mechanisms need an urgent overhaul of how they deal with AI, algorithms, big data collection, and the resulting mass bio-identifier monitoring in Chinese smart cities in China and abroad.

Critique: Western Technology

Western technology companies supply products to enable the Chinese surveillance state. The American firm Thermo Fisher Scientific provides technology to China's national DNA database, which is used for mass surveillance.[190] The French firm Morpho has supplied face recognition products to the Shanghai Public Security Bureau, while Sweden's AXis Communications and the Dutch company Noldus Information Technology have supplied equipment to enable Chinese surveillance.[191] Chinese companies such as Semptian, with links to Google and IBM, have been scrutinized for enabling the Chinese surveillance state.[192] With the rise of the CCP's

185 United Nations, "OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China, OHCHR.org, August 31, 2022, p. 43, https://www.ohchr.org/en/documents/country-reports/ohchr-assessment-human-rights-concerns-xinjiang-uyghur-autonomous-region.

186 United Nations, "OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China," 32.

187 Sophie Richardson, "China's Influence on the Global Human Rights System," Human Rights Watch, September 14, 2020, https://www.hrw.org/news/2020/09/14/chinas-influence-global-human-rights-system.

188 China Tribunal, *Judgment*, 26.

189 Australian Strategic Policy Institute, "Genomic Surveillance Inside China's DNA Dragnet," ASPI.org, https://xjdp.aspi.org.au/explainers/genomic-surveillance.

190 Australian Strategic Policy Institute, "Genomic Surveillance Inside China's DNA Dragnet."

191 Amnesty International, "EU Companies Selling Surveillance Tools to China's Human Rights Abusers," Amnesty.org, September 21, 2020, https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers.

192 Ryan Gallagher, "How US Tech Giants Are Helping to Build China's Surveillance State," The Intercept (news site), July 11, 2019, https://theintercept.com/2019/07/11/china-surveillance-google-ibm-semptian/.

coercion, intellectual property theft, Chinese reverse-engineering of technologies, Western sanctions, and allegations of human rights abuses, many tech companies ceased doing business in China.[193] However, China acquired market-leading Intel and Nvidia chips made in the US, as well as Dutch chip-maker Advanced Semiconductor Materials Lithography (ASML) machines.[194]

Despite Feldstein's argument that illiberal regimes have a high probability for abusive use of AI,[195] Western liberal democracies are major suppliers of AI surveillance technologies. As critics such as Majerowicz and Carvalho argue, associating only Chinese AI technologies with "digital authoritarianism" does not fully reveal the reality of AI surveillance.[196] Migliano and Woodhams note that Chinese AI surveillance technologies operate in many Western countries, including the US, Canada, the UK, and France, despite Western anti-China rhetoric on digital authoritarianism.[197] Researchers such as Woodhams,[198] Lugt,[199] Pisanu et al.,[200] Feldstein,[201] and Beraja et al.[202] indicate the actual scenario is one of AI surveillance being exported worldwide by autocracies like China and democracies such as the US in a race to dominate frontier technologies and achieve the market lead. Evidence of how these technologies are implemented and their impact on civil liberties is hard to come by. Seonae and Velasco suggest that "a more situated and differentiated approach" is needed to analyze AI surveillance projects.[203] Branding Chinese AI surveillance as digital authoritarianism without substantial evidence becomes rhetorical, especially in the current context of great-power rivalry and the competition between China and the West to dominate cutting-edge technologies. More research is required to examine how Western and Chinese AI surveillance technologies impact civil liberties. General references to mass AI surveillance do not help us understand AI surveillance architectures or their impact. Research must focus on real impacts with evidence on AI surveillance systems at work.

193 Dean DeBiase, "Why Companies Are Exiting China and What Leaders Can Do about It," *Forbes*, August 30, 2024, https://www.forbes.com/sites/deandebiase/2024/08/30/why-companies-are-exiting-china-and-what-leaders-can-do-about-it.

194 Bloomberg News, "Chinese Imports of Chip Gear Hit Record $26 Billion This Year," *Bloomberg News*, August 22, 2024, https://www.envoy.cirrus.bloomberg.com/news/articles/2024-08-22/chinese-imports-of-chip-gear-hit-record-26-billion-this-year.

195 Feldstein, "The Global Expansion of AI Surveillance," 351.

196 Esther Majerowicz and Miguel Henriques de Carvalho, *China's Expansion into Brazilian Digital Surveillance Markets* (Manchester, UK: University of Manchester, 2023), 5, https://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/di/dd_wp100.pdf.

197 Simon Migliano and Samuel Woodhams, "Hikvision and Dahua Surveillance Cameras: Global Locations Report," Top10VPN.com, 2021, https://www.top10vpn.com/research/hikvision-dahua-surveillance-cameras-global-locations.

198 Samuel Woodhams, "China, Africa, and the Private Surveillance Industry," *Georgetown Journal of International Affairs* vol. 21 (Fall 2020), 158, https://doi.org/10.1353/gia.2020.0002.

199 Sanne van der Lugt, "Exploring the Political, Economic, and Social Implications of the Digital Silk Road into East Africa: The Case of Ethiopia," in *Global Perspectives on China's Belt and Road Initiative: Asserting Agency through Regional Connectivity*, ed. Florian Schneider (Amsterdam: Amsterdam University Press, 2021), 315, https://doi.org/10.1515/9789048553952-014.

200 Gaspar Pisanu and Verónica Arroyo, "Surveillance Tech in Latin America Made Abroad, Deployed at Home," AccessNow.org, August 9, 2021, https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home.

201 Feldstein, "The Global Expansion of AI Surveillance," 1.

202 Beraja et al., "AI-tocracy," 1349.

203 Maximiliano Seoane and Carla Velasco, "The Chinese Surveillance State in Latin America? Evidence from Argentina and Ecuador," *The Information Society* 40, no. 2 (March–April 2024): 154, https://doi.org/10.1080/01972243.2024.2317057.

Conclusion

This study reveals how AI eliminates the technical bottlenecks previously facing efforts at mass surveillance and its trajectory toward achieving the pinnacle of authoritarian control in its all-embracing home ecosystem: smart city. AI not only upgrades mass surveillance in China but produces algorithmic rules, replicating repressive AI surveillance in China and beyond. The above evidence proves that China's AI dream extends beyond mass AI surveillance towards building its surveillance home in smart city. China does not export mere AI surveillance; it exports smart city surveillance technologies. A new form of governance is emerging in Chinese-built smart cities, which is smart authoritarianism. Akin to the early Greek city-states, which gave birth to democracy, smart cities are rapidly emerging along the DSR and BRI corridors in defiance of democracy and conquering lands to offer the Chinese model for the world, which is none other than smart authoritarianism, touted for its stability and prosperity in an uncertain world. This phenomenon highlights the ability of opposing forms of governance, such as democracy and authoritarianism, to utilize the same city-based model (smart city vs. city-state) to proliferate and compete with one another. Unlike the early democratic origins in city-states, the contemporary emergence of intelligent authoritarianism in smart cities is characterized by its distinctive total social control, effectively enforced by pervasive AI.

The rise of AI is eradicating efficiency bottlenecks just like how the rise of industrial machines was essential in the building of the modern world, working beyond human abilities and at a whole new level of precision. With AI surveillance, individual freedoms are squeezed out of any loopholes. China continues to widen its smart city ecosystem, built with a formidable eye on every aspect of people's lives. Western-style freedoms and democratic values remain alien in many places in the world. The CCP understands this, seizing the opportunity to export its surveillance technology mainly in the Global South. Chinese AI is the backbone of ubiquitous intelligence with worldwide connectivity, a world China has aimed to achieve by 2030. However, as a limit of this study, the Chinese smart city ecosystem is still expanding, aiming to connect across countries and regions, creating a behemoth of AI city brains to gather precision governance and surveillance under its wings. Future studies should follow the Chinese smart city ecosystem to chart its expansion, connectivity, and control, focusing on the metapolitical cultural battle confronting freedom of the world.

Smart city upgrades Chinese mass AI surveillance. Chinese mass surveillance itself is no longer the end of the researchers' focus. Instead, mass surveillance is the means to achieving the end goal of smart authoritarianism. China has moved on, upgrading to a smart city with a vision of achieving an intelligent, smart, authoritarian world by 2030. The rise of technological illiberalism in China alone is no longer the question. The question is how China seeks to conquer the world with its smart authoritarianism pushed forward through its Digital Silk Road and Belt and Road Initiative, rolling out smart cities. Chinese smart city is a technological advancement and a form of governance—smart authoritarianism that embodies the essence of illiberalism. Chinese smart city is the modern-day city-state of next-generation authoritarianism, envisioned to expand and connect the world, absorbing the Global South in particular and making China's vision for a smart authoritarian world a reality.