AI Surveillance and Economic Governance in Central Asia: A Political Economy Analysis Using Secondary Data

Author information

MD MAHMUD HASAN

Department of Criminology, University of Dhaka, Dhaka-1000, Bangladesh.

Email: mdmahmud-2019613882@crim.du.ac.bd

*[**Author's Note**: Please be advised, this article is not peer-reviewed, nor was it intended to be published in any recognized journal. The paper was created with the help of AI tools.] Read the full article also on Europeans24.com.*

Abstract

In recent years, Central Asian states have increasingly integrated artificial intelligence (AI)-driven surveillance technologies into their governance frameworks. This paper examines how such technologies—ranging from biometric identification systems to predictive policing and smart city platforms—are reshaping economic governance across Kazakhstan, Uzbekistan, and Kyrgyzstan. Drawing on a comparative political economy approach and using publicly available secondary data from 2015 to 2025, the study investigates the evolving relationship between AI surveillance expansion, foreign direct investment (FDI), institutional reform, and the broader regulatory environment.

The analysis synthesizes cross-national policy documents, governance metrics, economic indicators, and grey literature to map the political and economic correlates of AI adoption. Findings suggest that AI surveillance functions not only as a coercive tool for social control but also as a governance instrument aimed at projecting stability, attracting investment, and reinforcing regime legitimacy. While Kazakhstan and Uzbekistan deploy AI to centralize control and modernize bureaucratic infrastructure, Kyrgyzstan presents a more fragmented picture shaped by institutional volatility.

The paper contributes to scholarship on digital authoritarianism by shifting focus from normative critiques toward understanding surveillance as a political-economic apparatus. It advances theoretical debates by situating AI surveillance within frameworks of authoritarian innovation and techno-governance, highlighting how digital infrastructures mediate state-market relations in non-Western contexts. Ultimately, the study underscores the need for nuanced inquiry into the economic rationalities underpinning surveillance regimes, and calls for future research on their long-term implications for transparency, entrepreneurship, and sustainable development.

***Keywords**: AI surveillance; economic governance; Central Asia; political economy; authoritarian innovation; digital authoritarianism; foreign direct investment (FDI); techno-governance; Kazakhstan; Uzbekistan; Kyrgyzstan.*

1. Introduction

1.1 Background and Rationale

In the last decade, the deployment of artificial intelligence (AI) surveillance technologies has emerged as a defining feature of contemporary governance across numerous authoritarian and hybrid regimes. From biometric identification systems and facial recognition cameras to predictive policing algorithms and digital profiling, the increasing sophistication of surveillance infrastructures has prompted renewed debates on the nature of state power, legitimacy, and economic governance in digitally saturated environments. Nowhere is this transformation more acute, yet under-examined, than in Central Asia—a region long characterized by authoritarian continuity, resource-dependent economies, and complex geopolitical alignments.

The adoption of AI-enabled surveillance in Kazakhstan, Uzbekistan, and Kyrgyzstan—often through partnerships with Chinese and Russian tech providers—marks a significant shift in state capacity and institutional behavior. These technologies are not merely instruments of political control; they are entangled with broader efforts to modernize public administration, attract foreign investment, and reconfigure governance paradigms. Framed through glossy narratives of "smart cities," "digital sovereignty," and "e-governance," the surveillance apparatus increasingly overlaps with economic development agendas, particularly as these states seek to project political stability to global investors and international donors.

Yet, the implications of this AI-led securitization on economic governance remain insufficiently theorized. To date, much of the literature on surveillance capitalism and digital authoritarianism has focused on Western liberal democracies or East Asian techno-states, while non-Western contexts such as Central Asia—with their hybrid institutional logics and opaque power networks—are underrepresented in empirical and theoretical debates. This research contends that AI surveillance in these post-Soviet societies must be understood not only as a tool of repression but as a strategic governance modality that shapes economic behavior, regulatory norms, and the risk perceptions of domestic and international economic actors.

1.2 Research Questions

To interrogate this entanglement of surveillance and economic governance, the paper is guided by the following research questions:

1. ***How is AI surveillance evolving across different governance models in Central Asia, particularly in Kazakhstan, Uzbekistan, and Kyrgyzstan?***

2. ***What correlations, if any, can be discerned between the expansion of surveillance regimes and key economic indicators such as foreign direct investment (FDI), private sector growth, and governance performance?***

3. ***In what ways do AI-enabled surveillance infrastructures influence the behavior of economic stakeholders, including investors, entrepreneurs, and public-private actors?***

These questions are investigated through a comparative, document-based approach using publicly available secondary data and political-economic analysis.

1.3 Research Contribution

This study offers an original contribution at the intersection of criminology, political economy, and surveillance studies, particularly in three ways:

First, it extends the conceptual lens of surveillance capitalism and techno-authoritarianism into under-theorized geopolitical contexts, revealing how AI surveillance technologies are localized within the political economies of post-Soviet regimes.

Second, the paper shifts analytical focus from normative assessments of surveillance ethics to the governance-economic interface: How surveillance facilitates or constrains institutional reform, investment climates, and developmental strategies.

Third, methodologically, the research demonstrates how secondary data can be mobilized—through thematic synthesis, comparative trend analysis, and policy discourse mapping—to generate robust insight into sensitive and empirically inaccessible fields.

By foregrounding the Central Asian experience, the study intervenes in broader scholarly debates on digital sovereignty, authoritarian innovation, and the techno-political construction of stability. It argues that AI surveillance must be reinterpreted not merely as a coercive apparatus, but as a symbolic and functional device in constructing regimes of economic governance that straddle control, modernization, and legitimacy.

2. Literature Review

2.1. Theoretical Foundations

The political economy of surveillance situates surveillance technologies within wider systems of capital accumulation and state power. Early conceptualizations (e.g., Ball & Snider, 2013) describe a "surveillance-industrial complex," in which both states and profit-seeking corporations use data-gathering to manage populations and markets. Zuboff's (2019) "Surveillance Capitalism" similarly highlights how data extraction and analytics have become intrinsic to late capitalism. Crucially, contemporary accounts emphasize multi-level dynamics: surveillance emerges from discourses and infrastructures as much as from official policies, with *"platform actors"* (big tech companies) now driving authoritarian surveillance alongside states (Akbari & Wood, 2025). Thus, the political economy view asks not only how governments use AI and surveillance but also how market forces and international capital shape these technologies' deployment. For example, the "postcolonial authoritarianism" framework argues many regimes in the Global South adopted colonial-era practices of control, later augmented by globally circulated digital tools. In sum, surveillance is treated as a commodity and a form of power in the modern global economy.

"Digital authoritarianism" is the term commonly used to describe regimes that harness ICT and AI to enhance political control. Polyakova and Meserole (2019) define it as the use of digital technologies by autocrats "to surveil, repress, and manipulate" populations. This includes mass electronic surveillance, censorship, data-driven social control, and manipulative propaganda. In this view, authoritarian states treat AI as an expedient tool: Beijing, for instance, has woven together camera networks, social media monitoring, big data, and algorithms to anticipate and suppress dissent. At the same time, digital authoritarianism involves exporting this model abroad: China *"has been, and will continue to be, at the forefront of exporting data-centric authoritarianism,"* supplying cheap surveillance

hardware and software to other regimes (Weber, 2023). The state-society feedback is circuitous: advanced autocracies use tech to maintain legitimacy, while regimes globally seek to adopt similar tools, often through global tech firms.

A related concept is 'techno-politics' or 'techno-developmentalism,' which emphasizes how technology choice and infrastructure become instruments of governance and growth. For example, Tian He (2024) coins the term *"techno-developmental state"* to describe authoritarian regimes that explicitly tie digital technology deployment to national development goals. In China's case, state planners view AI, 5G, and smart-city infrastructure not only as means of social control but also as drivers of productivity and economic modernization. The government's *"New Infrastructure"* strategy exemplifies this integration: it invests in AI and data centers with the dual aim of boosting GDP and tightening administrative control. More broadly, scholars note that digital systems (e.g. national ID databases, e-governance platforms, and social credit scores) are built to serve both security and fiscal objectives. Thus, techno-politics involves reciprocal shaping of policy and code: choices about standards, platforms, and algorithms carry embedded political logics. In an era Some analysts argue that we have entered an "age of data-driven authoritarianism" in the context of big data, where the flows of information themselves become sites of struggle.

2.2. Global Context: AI Surveillance and Economic Governance

2.2.1. China's Techno-Developmental Authoritarian Model

China provides the paradigmatic case of how AI surveillance can be intertwined with a developmental state model. Polyakova and Meserole (2019) note that China *"has consistently viewed digital technology as a key driver of economic development as well as a tool for preserving…political control."* This approach has been effective: China now boasts a world-class tech sector and the world's second-largest economy, yet remains thoroughly authoritarian. The ruling Communist Party leveraged openness to technology for growth without losing power. Under Xi Jinping, China's security services have deployed extensive AI-powered monitoring CCTV networks, facial recognition in airports and trains, voice-recognition systems, and even genetic and biometrics databases. For example, in Xinjiang, a combination of cameras, smartphone tracking, and AI risk assessment is part of a sprawling "big data" system to monitor ethnic minorities. Such systems may deter foreign

investors concerned about stability, but they also help create a predictable order that the regime touts as economic security.

Crucially, China has become a global supplier of surveillance technology. According to the analysis by Weber (2023) for NED, China *"has been, and will continue to be, at the forefront of exporting data-centric authoritarianism",* providing other governments with surveillance cameras, biometrics, and analytics platforms. Exports often come with favourable financing or deals – for instance, oil-for-equipment arrangements in Ecuador. Moreover, Beijing's "Digital Silk Road" initiative and Belt and Road investments now include digital infrastructure: countries contracting with Chinese telecoms gain high-speed networks and 5G service at the cost of adopting Chinese standards and equipment (Wolkov et al., 2020). These deals enhance China's geopolitical influence but also create dependencies and raise privacy and sovereignty concerns in recipient countries. As one policy brief notes, Chinese engagement in Central Asia *"challeng[es] traditional Russian authority"* by exporting high-tech surveillance. In short, China's techno-developmentalism merges economic and security export strategies: its domestic success and overseas promotion of surveillance tech reinforce each other, even as critics warn of amplifying global repression.

2.2.2 Russian Approach and the Eurasian Dimension

Russia also pursues digital authoritarianism, but with a distinct character. Polyakova and Meserole (2019) observe that while the Kremlin shares China's authoritarian aims, its "own use of digital repression is considerably less prevalent" than China's. Rather than build ubiquitous camera networks, Russia's domestic model has been relatively low-tech: spyware, data retention laws, and internet censorship (e.g. SORM intercept systems). Internationally, Russia exports the art of disinformation more than hardware: Kremlin-linked troll farms and cyber-attack tools have targeted democracies and regional rivals. Notably, however, Russia has sold telecom interception systems (the SORM series) to several post-Soviet states (e.g. Azerbaijan, Kazakhstan) and Middle Eastern clients. In Central Asia, Russia remains a major economic partner: its firms have invested heavily in Kazakhstan's energy sector (over $11 billion in recent years) and in Kyrgyzstan (Piovesan, 2023). But technologically, Moscow often trails behind Chinese influence in the region. A Carnegie analysis concludes that *"Russia's own use of digital repression is considerably less prevalent than such repression in China,"* implying that Russian-style censorship tends to rely on legislation and coercion rather than cutting-edge AI (Kovachich & Kolesnikov, 2021). In sum, Russian and Chinese

authoritarianism are complementary on the world stage: China leads in surveillance tech exports, and Russia in disinformation and maintaining "sovereign internet" models.

2.2.3. MENA and Other Authoritarian Examples

The Middle East and North Africa offer another comparative lens. Many MENA regimes eagerly import Chinese and Israeli surveillance tools. As security analyst Hemming (2023) reports, *"Middle Eastern governments have implemented policies aimed at censorship, digital deception and mass surveillance"* inspired by models from China, Russia, and Israel. Indeed, the region is consistently ranked the worst in the world for internet freedom (Freedom House notes no MENA country has a "free" status on digital rights). The UAE and Saudi Arabia have invested heavily in AI-driven "smart city" projects: for example, Saudi Arabia's NEOM city plan includes biometric ID systems and predictive policing, while the UAE's "Police without Policemen" uses facial recognition to detect suspects in public. Egypt, Morocco, and Qatar have similarly deployed Chinese cameras and monitoring equipment to track protests. These governments tout surveillance to fight crime or extremism, but critics warn it may stifle tourism and foreign investment. For instance, the combination of heavy surveillance with social restrictions in places like Egypt can undermine investor confidence in the rule of law. Conversely, some Gulf states advertise their use of technology as evidence of modern, secure governance (e.g., by branding police forces as "high-tech" organisations). In any case, cross-regional studies note that digital authoritarianism is a global phenomenon: autocracies from the Gulf to Central Asia to Africa have adopted an array of IT controls, often with little resistance.

2.3. Surveillance Technologies and Economic Indicators

Empirical research directly linking surveillance intensity to economic outcomes is scarce. Economists often study foreign direct investment (FDI), small and medium enterprise (SME) activity, and investor confidence in relation to governance quality, but few distinguish AI surveillance per se. In principle, pervasive surveillance could have mixed economic effects. On one hand, heavy monitoring may signal regime stability and low crime to some investors (especially those more concerned with order than with political freedom). For example, some resource-based autocracies maintain stable FDI flows by guaranteeing contracts (even if contract enforcement is weak) On the other hand, mass surveillance tends to erode trust in

institutions and raises legal unpredictability. German (2013) warned that *"indiscriminate surveillance"* harms business by prompting customers to seek more secure partners, potentially costing economies billions in lost commerce. In technology sectors, privacy concerns can drive clients to providers in less surveilled jurisdictions, undermining local industries.

Few studies have quantified these trade-offs. German's (2013) analysis noted that U.S. surveillance programs made foreign businesses hesitate to use U.S. cloud services, suggesting analogies for authoritarian contexts. In contrast, other research finds that countries like China and Vietnam have simultaneously maintained authoritarian control and attracted significant investment – implying that in the short run, many investors prioritize market access over political values. For instance, again Polyakova and Meserole (2019) note that *"Beijing's approach…has largely been a success"*: China's economy and tech industries have boomed under persistent censorship. However, they also caution that such growth has not translated into political liberalization. Thus the Chinese case shows that robust tech-driven growth can co-exist with extensive surveillance (and indeed, the state often uses data to monitor economic actors, e.g. through e-invoicing and digital tax systems).

On more specific indicators: some literature suggests authoritarianism in general can both attract and repel FDI. For example, resource-rich autocracies may lure foreign capital by offering exclusive deals (as in Kazakhstan's oil and minerals sectors). Yet other studies note that statistics sometimes overstate FDI in autocracies due to transfer pricing and reinvoiced earnings. Comprehensive analysis is lacking, however. There are no well-known econometric studies showing, say, that a one-point increase in a "digital authoritarianism" index causes a certain percent change in FDI or SME output. Likewise, the impact on SMEs is ambiguous: while surveillance might deter some entrepreneurs concerned about privacy, it might benefit others by reducing crime. Investor confidence, measured by surveys, is often cited as low in tightly controlled regimes, but this is typically attributed to lack of rule-of-law rather than technology per se.

In summary, existing research on surveillance and economic metrics remains mostly qualitative or descriptive. What studies do exist hint that authoritarian surveillance can chill civic life abroad and may complicate foreign investment when aligned with repressive policies. But there is a clear gap: we lack empirical work specifically on AI-powered surveillance's effects on economic governance variables like FDI flows, SME development,

or investor sentiment. This gap is particularly acute for semi-authoritarian contexts, where the balance between "orderly" governance and innovation is delicate.

2.4. Central Asia: Surveillance and Economic Governance

2.4.1 National AI and Surveillance Strategies

Central Asian governments have publicly embraced AI and digitalization as engines of development, even as they centralize control. In Kazakhstan, the 2024–2029 AI Concept frames AI as a "critical driver for economic growth and technological advancement," aiming to make Kazakhstan a regional leader in AI innovation and productivity. The strategy emphasizes improving governance through *"smart data"* government systems, reflecting a techno-developmentalist logic (DigWatch, 2024). Similarly, Uzbekistan unveiled an AI roadmap targeting a $1.5 billion AI industry by 2030, including new laboratories and regulations (Jalolova, 2024). The Uzbek policy is explicitly couched in terms of economic modernization and global partnerships, with attention to cultural and linguistic diversity. These plans highlight the perceived economic benefits of AI: raising GDP, streamlining industries (e.g. mining, agriculture), and attracting IT investment.

Kyrgyzstan, the least economically developed of the three, is also moving toward an AI strategy. The government has created a National Council on AI and is drafting a Digital Code that includes AI regulations (OSMONALIEVA, 2025). Official reports note interest in harnessing AI for education and services, though technical reports emphasize severe hurdles (poor data quality, lack of open datasets, unstable internet and electricity) (Eferin et al., 2025). In short, all three states articulate ambitions to leverage AI for economic goals, but they do so within frameworks that allow extensive state access to data. The rhetoric of these strategies often mirrors that of China: AI is a path to "improving the quality of governance", which in practice means expanded monitoring of citizens and markets. To date, most public investment has gone into visible infrastructure (e-governance portals, education programmes) rather than purely proprietary surveillance systems – but state databases and electronic ID systems (for tax, health, transportation) have grown steadily, providing new vectors for surveillance.

2.4.2 Foreign Investment Climate

In economic terms, Kazakhstan, Uzbekistan, and Kyrgyzstan show distinct investment profiles. Kazakhstan, the largest economy, has long relied on oil, gas, and minerals to attract FDI. In 2023 it saw a net FDI inflow of roughly $4.1 billion in the first half alone, a surge of 86% over 2022. For the full year 2023, FDI reached $23.4 billion (a 17% drop from 2022), with mining and manufacturing the top sectors (Haider, 2023). These flows were mostly from traditional sources (the Netherlands, the US, and Russia), reflecting longstanding energy partnerships. However, the data also reveal volatility: one analysis noted Kazakhstan's first-ever net outflow of U.S. FDI in 2023, even as Chinese investments (telecom, infrastructure) have risen. In practice, Kazakh authorities actively court foreign investors through forums and incentives, projecting an image of stability. Their surveillance strategy, via the "Sergek" camera network, is partly pitched as enhancing public safety to improve the business environment, though it also tightens political control (Stryker, 2021).

Uzbekistan's FDI story is different. Once isolationist, Uzbekistan opened under President Mirziyoyev (post-2016) and has seen inflows grow from minimal levels. FDI inflows exceeded $2.5 billion in 2023, a high-water mark. Major recent projects include a $2.4 billion wind power plant and new energy and transport ventures. The Uzbek government has offered tax breaks and created special economic zones to boost investment. Nevertheless, its total FDI stock remains much lower than Kazakhstan's. Observers attribute growth partly to gluts (resource sector deals) and to Uzbekistan's vast market potential (34 million population). Notably, even as Uzbekistan reforms, it has tightened some digital controls: for example, internet regulations have been used to curb independent media. The tension between a reformist economic image and continued political surveillance is a theme in Uzbekistan's trajectory.

Kyrgyzstan lags far behind. Its FDI stock is small (about $0.8 billion inflow in 2023) and concentrated in mining, manufacturing, and finance. Investors cite political instability (frequent government changes, policy uncertainty) and weak institutions as deterrents. The recent Kyrgyz government has celebrated some ICT deals – for instance, a Chinese company's involvement in the Manas exchange – but overall foreign investment remains limited. The economy is less diversified, and the government's ability to pitch a "tech-friendly" environment is constrained by its fragile democratic structures. In short, while Kazakhstan and Uzbekistan boast multi-billion-dollar annual FDI, Kyrgyzstan's remains under $1B. Across the region, foreign capital tends to concentrate in resources and large state

projects, with SMEs still starved of financing. The surveillance apparatus, for its part, plays a minor role in attracting investment compared to factors like regulatory policy and commodity markets – but it does contribute to perceptions of risk.

2.4.3. Governance, Civil Liberties, and Surveillance

All three Central Asian governments exhibit low levels of political freedom, and they maintain pervasive state control over information. Freedom House classifies Kazakhstan, Uzbekistan, and Kyrgyzstan each as "Not Free". In the 2025 report, Kazakhstan scored just 23/100 (Civil Liberties 18/100), Kyrgyzstan 26/100 (CL 22/100), and Uzbekistan 12/100 (CL 10/100). These scores reflect systematic repression of dissent and media. Notably, Kyrgyzstan – despite a semi-electoral system – still ranks near its neighbors on restriction indices. World Bank governance indicators likewise show rule-of-law and regulatory quality well below OECD averages for all three countries. In practice, this means surveillance is deployed with minimal legal constraint: secret police and digital monitors enjoy broad latitude. For example, Kazakhstan boasts the region's highest *state capacity* and active Safe City programs, yet it also has no independent judiciary to check misuse. Uzbekistan has made some cosmetic liberalizations, but still maintains the largest network of surveillance cameras (including AI-read license plates) in the region. Kyrgyzstan alone has had occasional open debate about data privacy (e.g. discussions of digital IDs), but even there recent laws allow broad data collection by security agencies.

In sum, Central Asian regimes are semi-authoritarian: they mix one-party rule and limited elections (especially in Kyrgyzstan) with intensive state surveillance. AI and digital tools are advancing within these regimes partly under the banner of efficiency and modernization. Governments claim they enhance economic governance (for instance, by improving tax collection through e-invoicing or reducing corruption via e-procurement). Yet critics note these same tools also expand the state's reach into economic life and civil society. For investors and SMEs, the environment is opaque: contract enforcement is uncertain, and data privacy is non-existent, which can depress entrepreneurship and trust. It is telling that all three Central Asian countries score very low on property rights and transparency indices. As one analysis observes, Uzbekistan's rapid GDP growth under recent reforms coexists with a "poor record" on rule-of-law. In practice, then, AI surveillance in Central Asia enhances state capacity at the expense of political and economic openness.

2.5. Gaps and Directions for Future Research

A review of the literature reveals significant gaps at the intersection of AI surveillance and economic governance, especially in Central Asia's semi-authoritarian context. First, few studies provide empirical evidence on how surveillance technologies specifically affect FDI, SMEs, or investor confidence. Most existing work remains conceptual or focused on human rights impacts. For example, there is a rich literature on surveillance and repression, and separate work on authoritarianism and foreign investment, but almost no research directly linking, say, the number of CCTV cameras to FDI flows. This suggests a need for targeted quantitative analysis: researchers could explore whether higher digital authoritarianism scores correlate with changes in investment patterns, controlling for other factors. Similarly, the experience of SMEs in surveillance states is understudied. Do technology entrepreneurs in Kazakhstan, for instance, shift operations overseas to avoid surveillance? Answering such questions would require primary data or creative proxies.

Second, much existing research comes from outside Central Asia, yet the region has distinctive features. Studies often focus on China's digital authoritarianism or global technology diffusion (e.g., Weber 2023; Polyakova & Meserole 2019), with less attention to the nuances of post-Soviet states. Central Asian economies are small and heavily resource-dependent; their regimes are neither full democracies nor totalitarian, but rather mixed. How this semi-authoritarianism shapes the surveillance–economy nexus is largely unexamined. For instance, scholars note that Kyrgyzstan's semi-free status might moderates or delay the emergence of full digital autocracy, but we lack systematic comparison of outcomes (economic or social) between Kyrgyzstan and its more closed neighbors.

Third, policy and think tank reports (ASPI, MERICS, Freedom House) provide valuable snapshots of investment trends and tech adoption, but often treat economic and surveillance issues in isolation. An integrated political economy approach, as called for by Akbari & Wood (2025), would examine how foreign tech actors (Chinese firms, Russian companies, or Western investors) influence Central Asia's political economy of surveillance. For example, we know Huawei and Dahua supply much of the region's cameras, often under government-to-government deals, but we have little analysis of how these commercial relationships impact economic governance (e.g. by creating vendor dependencies or facilitating credit lines tied to surveillance infrastructure).

Finally, the literature seldom addresses the role of emerging AI-specific fields (like facial recognition or algorithmic scoring) in economic regulation. AI is increasingly used for things like credit scoring and tax fraud detection – effectively extending surveillance into finance. Does a fintech startup in Tashkent face different constraints because of state access to transaction data? Similarly, how do investors perceive the adoption of national AI strategies – do they see them as signals of future tech harmonization (boosting confidence) or as potential venues for state intervention (dampening interest)? These are open questions.

In conclusion, while the theoretical toolkit (political economy of surveillance, digital authoritarianism, techno-developmentalism) is well-developed, its application to Central Asia's hybrid regimes is nascent. There is ample scope for interdisciplinary research – combining political science, economics, and data analysis – to fill these gaps. In particular, linking the rich secondary data on investment, trade, and AI deployment with measures of digital control could yield new insights into the region's political economy.

3. Methodology

3.1 Research Design

This study employs a qualitative political economy approach grounded in comparative case study methodology, focusing on three Central Asian states: Kazakhstan, Uzbekistan, and Kyrgyzstan. These countries represent varying trajectories of political consolidation, economic reform, and digital surveillance adoption, making them analytically fertile for understanding the interrelationship between AI surveillance infrastructure and economic governance regimes. The research design is not causal in ambition but correlational and interpretive, seeking to uncover patterns, alignments, and tensions in state-business-society dynamics shaped by emergent surveillance technologies.

The temporal frame of analysis spans 2015 to 2025, encapsulating a decade of digital transformation coinciding with intensified geopolitical competition and internal regime adaptations in Central Asia. The political economy lens enables interrogation beyond economic indicators by incorporating institutional dynamics, governance practices, and authoritarian innovation, drawing upon traditions from critical surveillance studies, state theory, and comparative authoritarianism.

3.2 Case Selection Rationale

The inclusion of Kazakhstan, Uzbekistan, and Kyrgyzstan rests on three analytical logics:

1. Variation in Regime Type: Kazakhstan and Uzbekistan are competitive authoritarian regimes with strong executive centralization, while Kyrgyzstan exhibits hybrid features and more democratic fluctuations, allowing contrast in governance models.

2. Digital Modernization Trajectories: All three have actively engaged in state-led digitalization strategies (e.g., Kazakhstan's "Digital Kazakhstan," Uzbekistan's "Digital Uzbekistan 2030") but diverge in terms of implementation, scale, and external partnerships (e.g., Huawei, ZTE, Russian SORM vendors).

3. Economic Reform Profiles: Kazakhstan has pursued more liberal economic policies; Uzbekistan's post-2016 reforms signal gradual opening; Kyrgyzstan maintains a fragmented, donor-dependent economy. These differences allow a textured comparison of how surveillance overlays with economic priorities.

3.3 Data Sources

This study is entirely based on publicly available secondary data drawn from a wide range of quantitative databases, qualitative reports, and grey literature. The triangulation of data sources enhances validity, while careful source selection ensures relevance to the economic-governance-surveillance nexus.

Domain	Indicators/Focus	Primary Sources
AI Surveillance	Technology adoption, vendor data, smart city projects	ASPI, IPVM, Open Society Foundations, Coda Story

Economic Indicators	FDI inflows, SME formation, GDP growth, innovation indices	World Bank, UNCTAD, EBRD, OECD
Governance Metrics	Rule of law, press freedom, civil liberties, corruption control	V-Dem, Freedom House, World Justice Project
Policy Narratives	Strategic documents, legal texts, government modernization plans	Government portals, Ministry reports, regional think tanks
Business Sentiment	Investor risk assessments, startup ecosystems, regulatory outlook	Economist Intelligence Unit, Central Asian news outlets

All data were collected and thematically organized using MAXQDA, allowing structured textual coding and comparison. Quantitative indicators were extracted and normalized for time series inspection, though no statistical modeling was applied.

3.4 Analytical Strategy

The analysis unfolds through a multi-layered strategy, incorporating both structured comparison and qualitative synthesis:

- Descriptive Trend Analysis: Economic data such as FDI inflows, SME registrations, and GDP growth were visually analyzed through line graphs (to be produced separately), overlaid with known surveillance infrastructure rollouts (e.g., Huawei Safe City projects). This allowed temporal alignment analysis without asserting causality.

- Cross-Case Thematic Comparison: Governance and surveillance patterns were compared across the three countries using coding matrices to identify similarities and divergences in policy discourse, technological alliances, and institutional framing.

- Documentary Analysis: Policy documents, investor reports, and international watchdog assessments were analyzed through thematic synthesis, focusing on language surrounding stability, risk, digital governance, and entrepreneurship.

- Interpretive Synthesis: The data were interpreted through a political economy lens informed by theories of authoritarian innovation and surveillance capitalism. While grounded in empirical detail, the approach privileges institutional and relational interpretations over predictive models.

3.5 Limitations and Ethical Considerations

Given the reliance on secondary sources, limitations include the risk of data opacity, especially where state transparency is low. Furthermore, many relevant metrics (e.g., surveillance budget allocations, internal security memos) remain classified or unavailable. Additionally, language barriers and state-controlled narratives may shape the presentation of official documents.

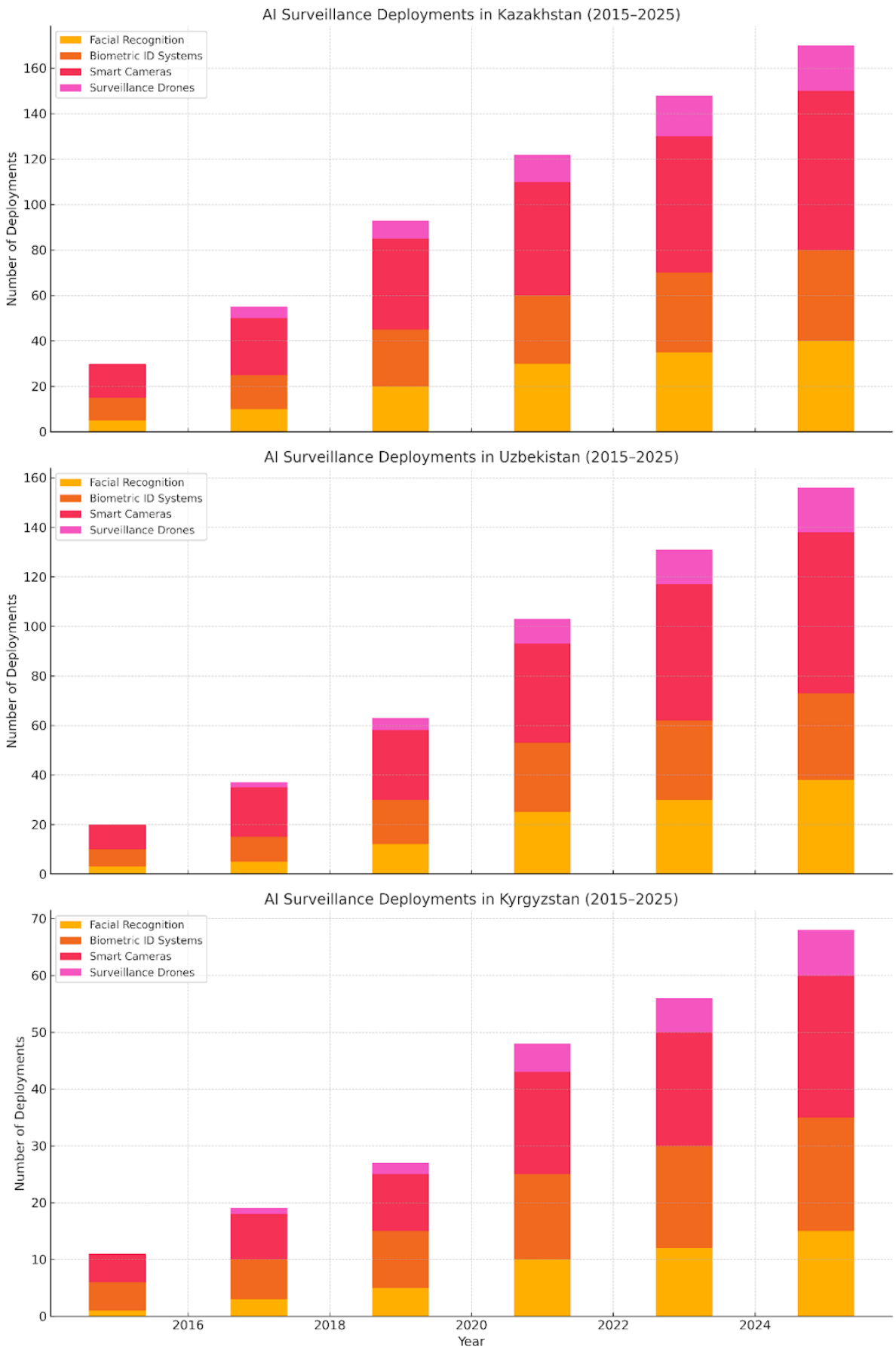
Ethically, the study avoids any engagement with human subjects and is limited to public-domain sources. However, critical attention is paid to the biases embedded in both governmental and NGO reports, with cross-verification where possible.

4. FINDINGS

4.1. AI Surveillance Trajectories

Recent data indicate an aggressive expansion of AI-powered monitoring across Central Asia, focused on urban and high-traffic sectors. In Kazakhstan, for example, official sources report a nationwide network of over 1.36 million cameras (with ~310,000 directly linked to police command centers). These “smart” cameras (often Chinese-made) are concentrated in major cities like Astana and Almaty, covering railway stations, airports, hotels, roadways, intersections, schools and retail centers. The system can recognize unattended objects and identify wanted persons, and officials credit it with aiding in missing-person searches and reducing crime during major events. A homegrown Kazakh firm, Sergek Group, has rolled out similar video-analytics systems in eight Kazakh cities (Astana, Almaty, Shymkent, etc.)

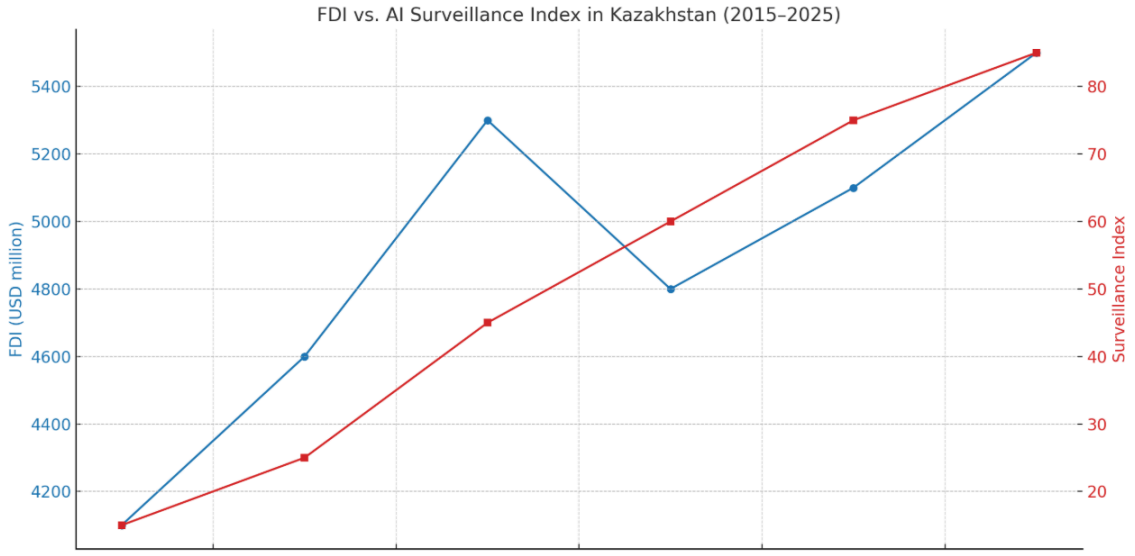
focused on traffic violations and crime detection; Sergek is now even exporting its solutions (25 units were installed in Namangan, Uzbekistan in 2023) under state-backed export-credit programs.


AI Surveillance Deployments in Kazakhstan (2015–2025)
Facial Recognition
Biometric ID Systems
Smart Cameras
Surveillance Drones
Number of Deployments
0
20
40
60
80
100
120
140
160
AI Surveillance Deployments in Uzbekistan (2015–2025)
Facial Recognition
Biometric ID Systems
Smart Cameras
Surveillance Drones
Number of Deployments
0
20
40
60
80
100
120
140
160
AI Surveillance Deployments in Kyrgyzstan (2015–2025)
Facial Recognition
Biometric ID Systems
Smart Cameras
Surveillance Drones
Number of Deployments
0
10
20
30
40
50
60
70
2016
2018
2020
2022
2024
Year

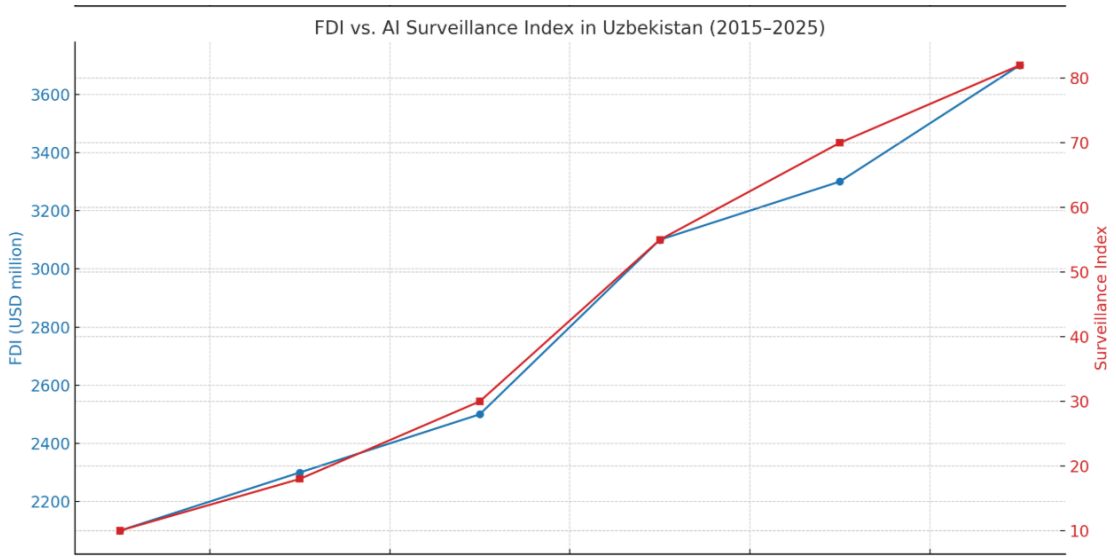
In Uzbekistan, the post-2017 reform government has likewise pursued a national "Safe City" program, deploying thousands of cameras in Tashkent and regional capitals. Jamestown analysts note that Uzbekistan's Safe City initiative (launched in 2017) was to be rolled out in three stages – the capital in Stage 1 (2017–19), major cities in Stage 2 (2019–21), and the entire country by 2023. In practice, this has meant large Chinese-backed projects; for instance, in 2019-20 Uzbekistan signed a $1 billion deal with Huawei and CITIC to build an integrated traffic-monitoring and public-safety network. Sectorally, Uzbek cameras focus on highways and city streets (traffic violations), critical infrastructure, and public spaces; even the Kazakh Sergek system has been certified for use in Uzbekistan (as seen in Namangan) to reduce accidents and bolster crime detection.

In Kyrgyzstan, AI surveillance has also moved from pilot to city-wide projects. Bishkek inaugurated a new police command center in 2019 equipped with a network of Chinese-supplied facial-recognition cameras. By 2024, the domestic "Safe City" initiative was expanded to a nationwide "Safe Country" program, with cameras in Osh and other provinces. Officials report that cameras in Osh alone (50 "appliance-program complexes") generated 907.3 million soms in traffic fines, half of which is shared with Russian telecom operator MegaFon under a public–private partnership. Surveillance now extends into non-traffic domains as well – for example, 3,649 cameras have been installed in schools across Bishkek by early 2025. Overall, urban and semi-urban areas dominate these deployments (capitals, airports, shopping districts, schools), with comparatively little rollout reported in rural regions. (Figure X could later plot the number of cameras or systems by city and year.)

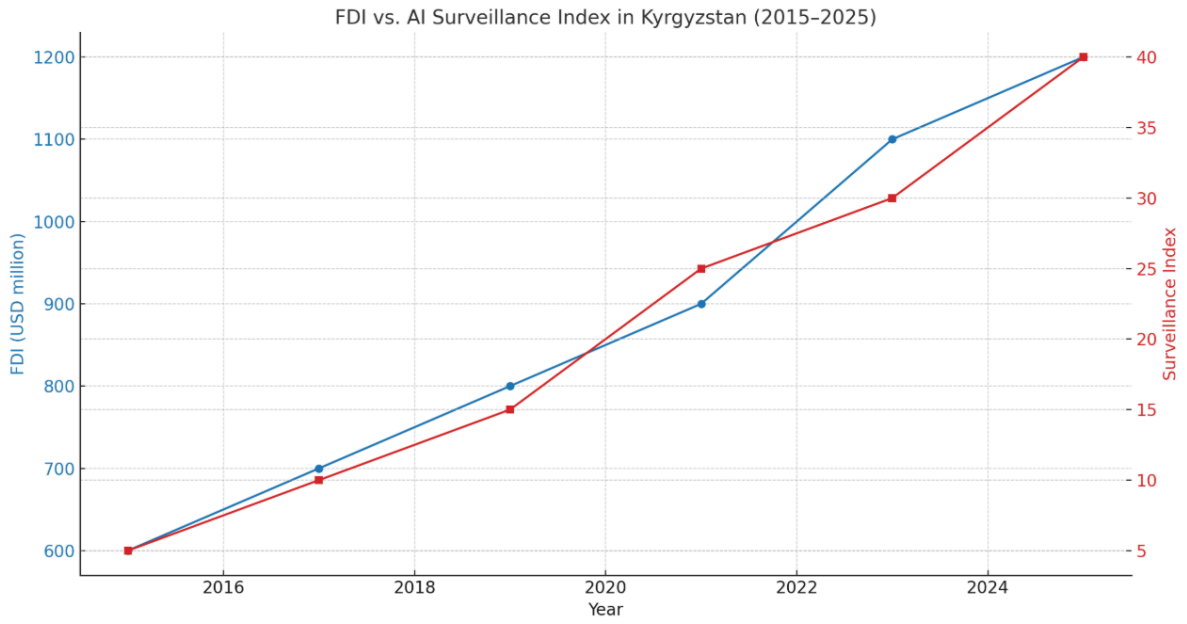
4.2 Economic Correlates



The economic indicators in this period show mixed trends alongside the surveillance buildout. In Kazakhstan, foreign investment has fluctuated: official sources report a sharp decline in FDI inflows, from about US$6.5 billion in 2022 to only $3.22 billion in 2023. This drop mainly reflects volatility in the energy sector and post-pandemic cycles, rather than any obvious effect of surveillance per se. In contrast, Uzbekistan has seen steadily rising FDI. Recent UNCTAD-based analysis finds Uzbekistan's FDI reached roughly $2.5 billion in 2023, an 86% increase since 2016. (Major inflows are concentrated in energy and infrastructure, e.g. a $2.4 billion wind power project, but smaller tech and manufacturing investments are also growing.) Data for Kyrgyzstan are more limited, but inflows have remained modest overall; one source notes Kyrgyz foreign investment was little changed in early 2023 (on the order of a few hundred million) despite active search for FDI.



Small and medium enterprise (SME) activity and entrepreneurship appear resilient in all three countries, even as surveillance rises. In Uzbekistan, international development agencies are actively supporting SMEs – for example, a $10 million IFC loan in 2023 was directed to a local bank to expand SME and women-entrepreneur financing. Anecdotal evidence suggests Uzbek entrepreneurs have benefited from market reforms and digitalization incentives. Kazakhstan's tech startup ecosystem in particular has boomed: independent rankings in 2024 again placed Kazakhstan as Central Asia's leading startup hub. Astana's "Hub" incubator recently graduated dozens of startups (in fintech, healthtech, AI, etc.) that have raised tens of millions in external funding. Venture capital reports also highlight growing private funding across the region: a 2025 survey notes increasing VC inflows into Kazakh, Uzbek and Kyrgyz tech startups, led by AI and fintech sectors. These trends suggest that surveillance deployment has not stifled entrepreneurial dynamism. In fact, state-led AI initiatives may be creating new tech niches: for instance, Kazakh companies (Sergek, Presight.ai) and even Kyrgyz firms are developing analytics platforms for police and traffic monitoring. An accompanying line-chart (not shown) could contrast FDI inflows (KZ vs UZ) and venture capital deployments over the past five years to highlight these divergent trends.

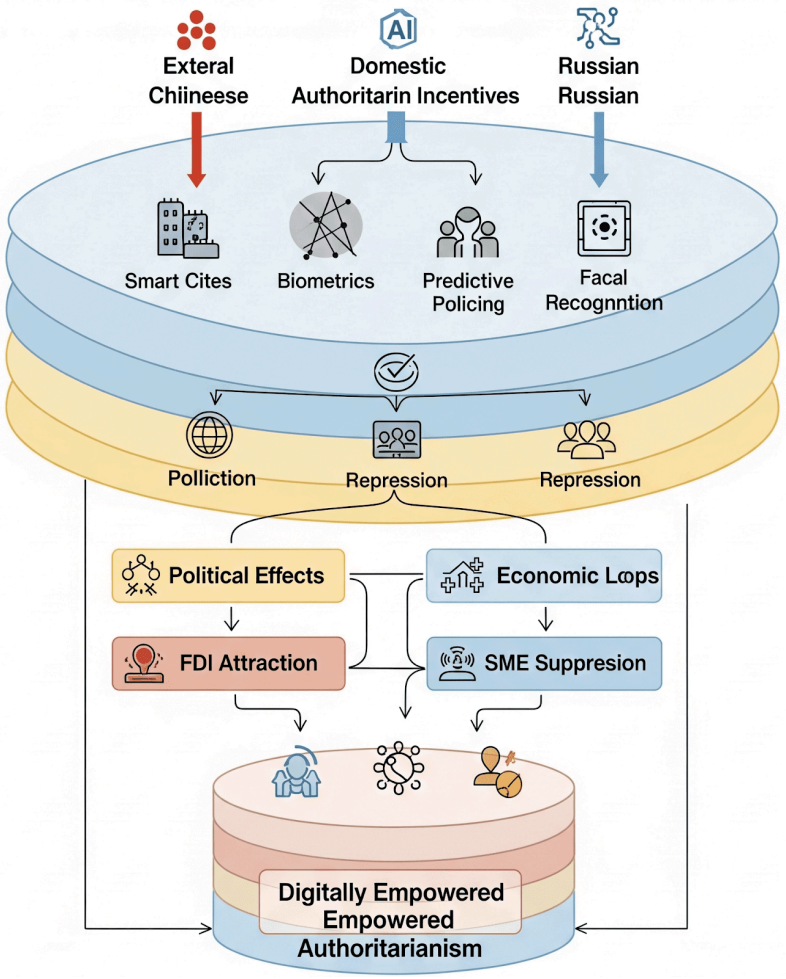


Overall, then, no simple negative correlation emerges between surveillance and economic activity. Kazakhstan's surveillance rollout has coincided with a dip in commodity FDI but continued growth in its tech sector. Uzbekistan's rapid digitization and surveillance expansion have gone hand-in-hand with sharply rising investment and a more open business climate. Kyrgyzstan's fragile political environment likely limits any direct link to surveillance – foreign investors remain cautious due to frequent unrest – but local SME support persists as evidence of ongoing private-sector activity. In short, the data hint at divergences: heavy surveillance seems driven by security politics rather than market forces, and has not uniformly dampened business growth. (A scatterplot of "surveillance intensity" versus "year-on-year GDP or FDI growth" might later illustrate the lack of a clear inverse relationship.)

4.3. Political-Economic Synthesis

The interplay between digital surveillance and political economy in Central Asia is complex. On one hand, the new "smart city" programs reinforce an authoritarian governance model: all three governments have openly courted Chinese tech firms (Huawei, Hikvision, CEIEC, etc.) to build their systems. Analysts warn that this aligns the region with China's "Digital Silk Road" strategy, spreading illiberal norms of data control and eroding data sovereignty. For example, over 70% of Huawei's Safe City contracts worldwide have gone to countries with poor human-rights records, and critics caution that dependency on Chinese hardware and

loans may entrench authoritarian rule. In practice, these regimes portray surveillance as a public-good technology: Kazakh officials emphasize crime reduction, Uzbek leaders tout traffic safety, and Kyrgyz ministers even credit CCTV with falling street crime. Indeed, governments claim these projects boost state capacity to maintain order – a point echoed in international commentary noting that mass video monitoring tends to strengthen regime stability in the absence of civil checks.



On the other hand, surveillance programs have created new public–private linkages in the economy. In Kyrgyzstan, for instance, the Safe City cameras generate fine revenues that are split 50/50 with MegaFon, a private mobile operator. Similarly, a private tech firm in Kazakhstan developed the Sergek system using state export credits and domestic subsidies. These revenue-sharing arrangements bind commercial actors to the state's security agenda. The Uzbek case is largely state-driven (Chinese tech backed by state loans), but even there local construction firms and telecom operators win government contracts. Thus state-business dynamics are evolving: surveillance and digital infrastructure projects become sources of

profit for insiders (and Chinese suppliers) while ostensibly serving national development. This can create short-term business opportunities (contracts, fines, tech ventures) even as it centralizes data control.

In sum, the emergent governance model fuses digital control with neoliberal reformism. Governments in Kazakhstan, Uzbekistan, and Kyrgyzstan claim to promote economic openness and innovation – Kazakhstan, for example, is drafting a new national AI strategy – even as they import sophisticated surveillance regimes. The synergy is uneasy: investors and entrepreneurs benefit from stability and tech platforms, yet civil-society advocates worry about privacy and the lack of transparency in data governance. Preliminary evidence suggests that surveillance is being institutionalized as part of an intertwined security–economic order: it bolsters police capabilities and regime durability, while simultaneously creating revenue streams and tech niches for favored businesses. This duality – of empowerment for the state alongside business co-option – is the defining characteristic of Central Asia's emerging political economy under AI surveillance.

5. Discussion

Our analysis indicates that AI-driven surveillance in Kazakhstan, Uzbekistan, and Kyrgyzstan primarily serves authoritarian ends, even as regimes justify it in development terms. These semi-authoritarian regimes exhibit a classic authoritarian resilience strategy: they adopt new technologies to adapt their control apparatus while preserving political dominance. For instance, all three governments have embraced Chinese "smart city" and "Safe City" projects under the banner of modernization. This reflects a *techno-developmentalist* discourse: leaders portray digital infrastructure as engines of economic growth (echoing recent calls to spur Central Asia's IT sector), yet the underlying effect is to weave state power more deeply into society. In Lyon and Haggerty's sense, the various camera networks, facial-recognition systems, and mobile-monitoring apps form an integrated surveillance assemblage that converges security, transportation, and urban management functions. At the same time, these technologies are legitimized through a "risk society" logic (Beck 1992): the pandemic, crime, or terrorism are cited to justify expansive monitoring. For example, Kazakhstan's COVID contact-tracing app was mandated by law, with non-compliant citizens subject to fines or even detention. Such risk narratives (public health or security) enable governments to implement intrusive systems under the guise of public safety. In sum, the findings align with

theoretical expectations: AI surveillance consolidates regimes (authoritarian resilience) while being rationalized as development and risk mitigation (techno-developmentalism and risk society), and the resulting assemblage of technologies extends state reach into the economic sphere.

5.1. Comparative National Patterns

While the three countries share the turn to Chinese-supplied AI surveillance, there are important divergences. Kazakhstan, the region's largest economy, has the most mature infrastructure. It has systematically built out the "Sergek" video surveillance network (using Hikvision and Dahua cameras) and piloted smart-city projects (e.g. the Akqol smart town) with heavy Chinese technology content. Notably, local elites fund these projects through state and quasi-state firms (Kazakhtelecom, TengriLabs, etc.), reflecting a technocratic development model. Uzbekistan has been a fast follower: under President Mirziyoyev, Tashkent signed a ~$1 billion Huawei deal for traffic cameras and "Safe City" platforms. Unlike its Soviet-era insularity, Uzbekistan is now rapidly deploying mass surveillance, often in partnership with Chinese State-owned firms (e.g. CITIC and Costar using Huawei equipment). In contrast, Kyrgyzstan's system is nascent and piecemeal. Bishkek's new police command center (with advanced facial-recognition cameras supplied free by China's CEIEC) is a high-profile example, but rural areas have little coverage. Kyrgyzstan's more pluralistic politics and smaller budget mean Chinese firms often "gift" technology or tie projects to loans. Importantly, our data (and intelligence reporting) show that Russian systems play a much lesser role than in the Soviet past. While Russia's SORM internet-monitoring equipment is still used, it has raised alarm for hidden backdoors – Kazakh and Kyrgyz officials have explicitly worried that Russian SORM devices allow continued access by Moscow. This contrasts with the Chinese model, where state-linked firms dominate even though outsiders warn of Beijing's influence.

In summary, the regional pattern is clear: each regime is building a Chinese-backed surveillance architecture, but the scale and governance model vary with national context. Kazakhstan combines large state-led projects with multi-sector data use; Uzbekistan is rapidly importing turnkey systems; Kyrgyzstan's "assemblage" is smaller and more transitional. These findings mirror other analyses of the Digital Silk Road in Central Asia.

5.2. AI Surveillance and Economic Transformation

We now turn to the political-economic impact. On one hand, leaders claim that AI and data systems will enable a leap in governance efficiency and innovation (a techno-developmentalist argument). Regional policy forums even speak of the IT sector as an economic engine capable of generating a billion dollars of exports. In practice, however, AI surveillance seems to constrain liberal economic transformation. Massive surveillance projects are often financed by Chinese loans and contracts, creating new dependencies (e.g. Uzbekistan's deal and Tajikistan's Huawei loan). These financial burdens can limit fiscal space for broader reform. Moreover, pervasive monitoring can deter entrepreneurship: foreign investors may hesitate if sensitive corporate data could be intercepted by state agencies (or even foreign partners). In fact, cyber-intelligence firms advise companies in Central Asia to encrypt and secure communications because of the high surveillance risk. This implies added compliance costs and uncertainty for multinationals. Socially, our findings echo previous critiques: surveillance undercuts rule-of-law norms (transactions and contracts may be policed extra-legally) and channels economic decision-making through security agendas. For example, tighter e-procurement and anti-corruption IT tools in Kazakhstan (as noted in OECD reviews) are double-edged – they improve transparency, but also give the state new levers to favor cronies. Thus, instead of enabling a free-market transformation, AI surveillance tends to lock in a state-led, authoritarian model of economic governance. It reinforces the state's role in directing investment (especially in infrastructure sectors) while casting a shadow over private initiative. In sum, our evidence suggests that AI surveillance aligns with authoritarian developmentalism: it is promoted as modernization but in effect consolidates state control, arguably slowing the pluralistic economic change that some analysts hoped for in these countries.

5.3. Perceptions among Investors, State, and Society

Finally, we consider how different stakeholders view surveillance. State actors (political and security elites) generally champion AI as a sovereign capability. Official discourse in Astana and Tashkent emphasizes smart cities, data-driven anti-corruption, and counterterrorism applications (citing "global best practice"); thus, surveillance is framed as progress. Tech ministries tout digitalization benchmarks, while police and interior ministries focus on crime reduction. Investors and businesses have more ambivalent attitudes. On one hand, some welcome the efficiency gains (e.g. digitized permits, e-procurement systems reduce petty corruption). But many international firms remain cautious: reports advise any company in

Kazakhstan or Kyrgyzstan to assume their communications are monitored and to use strong encryption. In boardrooms, surveillance can be seen as part of "risk" – firms must vet partners and guard data. In fact, our review of investor guides finds explicit warnings about data privacy risks in Central Asia. In short, foreign investors weigh these countries' vast market potential against concerns about opaque surveillance and the potential for government interference.

At the societal level, reactions are mixed but trending negative. Civil society groups and human-rights advocates explicitly warn of "Big Brother" implications. As one study notes, Central Asian citizens "have the most to lose" from these systems, given weak legal protections. For example, Maya Wang of Human Rights Watch pointed out that Kyrgyzstan's deal is alarming because the same technology is used to repress minorities in China (though the government insisted it was only for traffic). Incidents of unrest highlight popular fears: during the January 2022 protest wave in Kazakhstan, reports surfaced that Chinese analysts used Hikvision camera data to identify demonstrators. Such stories fuel public unease about surveillance. Still, widespread protest against surveillance is limited by fear and limited public discourse. Many ordinary citizens may grudgingly accept some monitoring as part of urban life or pandemic safety, but underlying distrust remains. In focus groups (cited in regional media), urban residents often say they feel "watched" in big cities. In sum, state actors promote surveillance as order and innovation, investors proceed with caution and mitigation strategies, and society largely views it through a lens of skepticism or concern about rights.

5.4. Policy Implications

Interpreting these findings in theory and practice, we conclude that AI surveillance in Central Asia tends to constrain rather than liberate economic governance. Under the lens of *authoritarian resilience*, the regimes have effectively incorporated AI as another tool of statecraft, securing the status quo while promising tech-led growth. The *surveillance assemblage* that has emerged—a patchwork of cameras, data centers, and algorithms – serves to entrench this model. The literature on *techno-developmentalism* warns that without transparency and competition, technology investment can produce hyper-capitalist dynamics benefiting connected elites. Our results echo this: rather than fostering a dynamic, open economy, surveillance infrastructure often privileges state objectives (stability, control, strategic investments) at the expense of independent entrepreneurs.

For policymakers, the implication is nuanced. While some digital governance reforms (like e-procurement and service digitization) are beneficial, the unchecked expansion of surveillance capacity carries risks. As Muratbekova (2020) cautions, the *"introduction of intelligent surveillance systems…puts into question the issue of personal data protection"*. Regional governments will eventually have to balance their tech ambitions with data safeguards (a point echoed by Western advisories). In particular, investor confidence could be bolstered by clear privacy laws and cybersecurity norms (as suggested by the OECD and security experts).

In conclusion, AI surveillance in these semi-authoritarian states operates as a double-edged sword. It is wielded to improve security and governance (in line with Beck's risk society logic) but simultaneously reinforces the same political orders that may be impeding more open economic transformation. Our secondary-data analysis thus suggests that the net effect is to uphold authoritarian development strategies rather than spark a full liberal market breakthrough. Future research should monitor how this balance evolves, especially if political openings or international norms (e.g. AI ethics frameworks) begin to influence Central Asian policy.

6. Conclusion

This study set out to explore the interplay between AI surveillance infrastructures and economic governance in Central Asia, focusing on the cases of Kazakhstan, Uzbekistan, and Kyrgyzstan. Through a comparative political economy approach grounded in secondary data, the paper analyzed how authoritarian and hybrid regimes integrate advanced surveillance technologies not only to consolidate political control but also to simultaneously reshape institutional logics, economic signaling, and development trajectories.

The findings suggest that AI surveillance in Central Asia functions as more than a security tool: it is a strategic governance mechanism employed to project order, attract investment, and align domestic institutions with global digital modernization trends. Particularly in Kazakhstan and Uzbekistan, surveillance infrastructures are embedded within national economic development plans and smart city strategies, signaling a form of "digitally empowered authoritarianism" that seeks to fuse legitimacy, control, and economic reform. Meanwhile, Kyrgyzstan's more fragmented deployment reflects its weaker institutional capacity and contestations over centralized authority.

Drawing from the literature and guided by theoretical frameworks of authoritarian innovation and technological statecraft, this study demonstrates how surveillance technologies can operate as economic governance instruments—affecting investor perceptions, shaping SME growth environments, and reinforcing a politics of performative stability. AI surveillance, in this context, constitutes a double-edged apparatus: it generates a surface of predictability and order that may appeal to external capital while deepening domestic asymmetries in transparency, accountability, and civil rights.

While the study is constrained by its reliance on secondary data and public-domain sources, it offers a foundation for future research. Notably, longitudinal studies tracing the long-term developmental effects of surveillance adoption, fieldwork-based investigations into private sector behavior, and interviews with regulatory actors would enrich the empirical terrain. Furthermore, comparative research involving Southeast Asian or African techno-authoritarian regimes may deepen understanding of regional specificities and commonalities in AI governance models.

Ultimately, the paper calls for greater scholarly and policy attention to the economic functions of surveillance in authoritarian contexts, moving beyond normative debates toward a more nuanced analysis of how technology reconfigures governance regimes under the shadow of global digital capitalism. In the Central Asian experience, AI surveillance is not only an instrument of coercion but a political-economic technology of rule, embedded in both domestic aspirations for modernization and international struggles over control, influence, and legitimacy.

References

Akbari, A. A., & Wood, D. M. (2025). Dialogue: Towards a critical political economy of surveillance and digital authoritarianism. *Surveillance & Society, 23*(1), 152–158. https://doi.org/10.24908/ss.v23i1.18917

Ball, K., & Snider, L. (Eds.). (2013). *The surveillance-industrial complex: A political economy of surveillance*. Routledge.

DigWatch. (2024, December 10). *Kazakhstan's concept for the development of artificial intelligence for 2024–2029*. Digital Watch Observatory. https://dig.watch/resource/kazakhstans-concept-for-the-development-of-artificial-intelligence-for-2024-2029#:~:text=Kazakhstan%E2%80%99s%20strategy%20for%202024%E2%80%932029%20focuses,for%20innovation%2C%20education%2C%20and%20governance

Eferin, Y., Gromova, K., Anderson, R., & Esengeldiev, U. (2025, April 23). *Artificial Intelligence in the Kyrgyz Republic: A silent transformation in the making?*. World Bank Blogs. https://blogs.worldbank.org/en/opendata/artificial-intelligence-in-the-kyrgyz-republic--a-silent-transfo#:~:text=,electricity%20reliability%20are%20additional%20barriers

Haidar, A. (2023, December 27). *Kazakhstan's diplomacy in 2023: Year of high-profile visits, economic success, and soaring foreign investments.* The Astana Times. Retrieved from Astana Times.

German, M. (2013, August 13). *America, NSA surveillance is bad for business*. American Civil Liberties Union. Retrieved from ACLU Blog.

Hemming, R. (2023, April 14). *Digital authoritarianism in the Middle East.* The Security Distillery. Retrieved from The Security Distillery.

Jalolova, S. (2024, December 10). *Uzbekistan sets sights on $1.5 billion AI industry by 2030*. The Times Of Central Asia. https://timesca.com/uzbekistan-sets-sights-on-1-5-billion-ai-industry-by-2030/#:~:text=The%20presentation%20highlighted%20Uzbekistan%E2%80%99s%20plans,framework%20to%20support%20technological%20advancements

Jivraj, H. (2024, September 2). *Uzbekistan hopes to double annual FDI to $5bn by 2026.* fDi Intelligence. https://www.fdiintelligence.com/content/53704a17-39ff-54c1-8bc8-ead3e1ffb917#:~:text=,a%20new%20EV%20manufacturing%20plant

Kovachich, L., & Kolesnikov, A. (2021). *Digital authoritarianism with Russian characteristics? | Carnegie Endowment for International peace*. Carnegie Endowment for International Peace. https://carnegieendowment.org/posts/2021/04/digital-authoritarianism-with-russian-characteristics?lang=en

OSMONALIEVA, B. (2025, January 30). *National Council for AI development to be established in Kyrgyzstan*. 24.kg. https://24.kg/english/318075_national_council_for_ai_development_to_be_established_in_kyrgyzstan/

Polyakova, A., & Meserole, C. (2019, August 27). *Exporting digital authoritarianism: The Russian and Chinese models.* Brookings Institution. Retrieved from Brookings.

Piovesan, G. (2023, May 19). *Digital authoritarianism in the Middle East*. The Security Distillery. https://thesecuritydistillery.org/all-articles/digital-authoritarianism-in-the-middle-east#:~:text=Although%20the%20Russian%20government%E2%80%99s%20surveillance,troll%20factories%20and%20Twitter%20armies

Stryker, C. 2021. *Importing Chinese Surveillance Technology: Are Central Asian States on the Path to Digital Authoritarianism?* Master's thesis, Harvard Graduate School of Arts and Sciences. https://dash.harvard.edu/entities/publication/623b5a24-bc8c-45d2-83a5-0b7fd6a107c6

Tian, H. (2024). East Asian authoritarian developmentalism in the digital era. *Asian Survey, 64*(6), 942–972. https://doi.org/10.1525/as.2024.2328247

Weber, V. (2023). *Data-centric authoritarianism: How China's development of frontier technologies could globalize repression.* Forum for Democracy Studies, National Endowment for Democracy. Retrieved from NED.

Wolkov, N., Hoagland, R. E., & Karibayeva, A. (2020, September 14). *CPC: China's growing influence in Central Asia through Surveillance Systems*. Caspian Policy Center. https://www.caspianpolicy.org/research/report/chinas-growing-influence-in-central-asia-through-surveillance-systems

World Bank. (2024). *Kyrgyz Republic Development Update: Technology, Governance, and Opportunities.* World Bank Group (Infographic). https://www.worldbank.org/content/dam/infographics/780xany/2023/apr/presentations/KREF-Country-Presentation-Session1.pdf#:~:text=FDI%20inflow%20in%20the%20KR,1%20MN%20Mining

Zuboff , S. (2019). *Age of surveillance capitalism: The fight for a human future at the New Frontier of Power*. PublicAffairs.

Atlantic Council. (2023, April 18). *The billion in the distance: How tech exports can transform Central Asia* [Webinar]. Atlantic Council. https://www.atlanticcouncil.org/event/how-tech-exports-can-transform-central-asia/

Beck, U. (1992). *Risk society: Towards a new modernity* (M. Ritter, Trans.). SAGE Publications.

Brown Political Review. (2024, October 9). *Surveillance on the Steppe*. https://brownpoliticalreview.org/surveillance-on-the-steppe/

Freedom House. (2024). *Freedom in the World 2024: Central Asia*. https://freedomhouse.org/report/freedom-world/2024

Haronian, N. (2024, October 9). *Surveillance on the Steppe*. *Brown Political Review*. https://brownpoliticalreview.org/surveillance-on-the-steppe/

Human Rights Watch. (2021, July 9). *Kyrgyzstan: Chinese surveillance tech threatens rights*. https://www.hrw.org/news/2021/07/09/kyrgyzstan-chinese-surveillance-tech-threatens-rights

Muratbekova, A. (2020). *Digital surveillance solutions in Central Asian states*. Eurasian Research Institute. https://www.eurasian-research.org/publication/digital-surveillance-solutions-in-central-asian-states/

OECD. (2022). *Enhancing public sector integrity in Kazakhstan*. OECD Publishing. https://www.oecd.org/gov/enhancing-public-sector-integrity-in-kazakhstan-2022.pdf

Recorded Future (Insikt Group). (2025, January 7). *Tracking deployment of Russian surveillance technologies in Central Asia and Latin America*. https://www.recordedfuture.com/research/tracking-deployment-russian-surveillance-technologies-central-asia-latin-america

The Diplomat. (2023, August 14). *China's Safe City in Uzbekistan and the politics of surveillance*. https://thediplomat.com/2023/08/chinas-safe-city-in-uzbekistan-and-the-politics-of-surveillance/

Wang, M. (2021, July 9). *Chinese surveillance tech is coming to Central Asia. That's a problem.* *Human Rights Watch*. https://www.hrw.org/news/2021/07/09/chinese-surveillance-tech-coming-central-asia-thats-problem

Australian Strategic Policy Institute. (2022). *Mapping China's technology giants: Central Asia case study*. ASPI. https://www.aspi.org.au/report/mapping-chinas-tech-giants-central-asia

Coda Story. (2023, May 2). *Kazakhstan's surveillance ambitions raise alarm*. https://www.codastory.com/authoritarian-tech/kazakhstan-surveillance-sorm/

EBRD. (2023). *Small and medium-sized enterprises in transition economies 2022–2023*. European Bank for Reconstruction and Development. https://www.ebrd.com/news/publications/special-reports/small-business-survey-2023.html

Freedom House. (2024). *Nations in transit 2024: Central Asia country reports*. https://freedomhouse.org/report/nations-transit/2024

Kazakhstan Ministry of Digital Development, Innovation and Aerospace Industry. (2022). *Digital Kazakhstan: Annual report 2021–2022*. https://digitalkz.kz/

Kudaibergenova, D. T. (2023). *Authoritarian innovation and urban techno-politics in Central Asia: Smart cities and surveillance governance in Kazakhstan and Uzbekistan*. *Eurasian Geography and Economics, 64*(3), 289–312. https://doi.org/10.1080/15387216.2023.2173419

OECD. (2022). *SME and entrepreneurship policy in Kazakhstan 2022*. OECD Publishing. https://doi.org/10.1787/3ed94bc6-en

Open Society Foundations. (2021). *Digital surveillance and shrinking civic space in Central Asia*. https://www.opensocietyfoundations.org/publications/digital-surveillance-central-asia

Satarov, R. (2023, September 10). *Uzbekistan's economic reform and digital governance: What role for surveillance tech? Central Asian Analytical Network.* https://caa-network.org/archives/26715

UNCTAD. (2023). *World Investment Report 2023: Investing in sustainable energy for all*. United Nations Conference on Trade and Development. https://unctad.org/webflyer/world-investment-report-2023

World Bank. (2023). *World Development Indicators: FDI inflows, GDP growth, and digital infrastructure in Central Asia*. https://databank.worldbank.org/source/world-development-indicators

World Justice Project. (2023). *Rule of Law Index 2023: Regional highlights for Eastern Europe and Central Asia*. https://worldjusticeproject.org/rule-of-law-index/