

# China-Central Asia Research Initiative 2025:

## Digital Sovereignty and Infrastructure



# Kazakhstan–China Cooperation in the Field of Digitalization: Achievements and Prospects

Danila Bekturganov, “Civil Expertise”, Eurasian Digital Foundation

## Abstract

*The study Kazakhstan–China Cooperation in the Field of Digitalization: Achievements and Prospects examines the positive and negative aspects of cooperation between China and Kazakhstan in the field of digitalization.*

*Relevance: Cooperation with China in the field of digitalization is relevant for Kazakhstan, especially in the context of turbulence caused by serious geopolitical changes; this cooperation needs to be monitored and evaluated in order to develop prospects and mitigate possible risks.*

*Objective: To study the latest achievements of Kazakhstan-China cooperation in digital sphere, identify the strengths and weaknesses of this cooperation, and formulate recommendations for its mutually beneficial development.*

*Methods: For the purposes of the study, a desk research format was used using the Digital Stack methodology.*

*Results: The achievements of Kazakhstan-China digital cooperation in recent years are described, successes and risks are analyzed, and recommendations are formulated.*

*Conclusions: China continues to actively participate in projects to build physical and data infrastructure in Kazakhstan, occupies a significant share of the consumer and business electronics market, shows strong growth in the application and content market, and significantly influences Kazakhstan’s Internet governance.*

## Introduction

Cooperation between Kazakhstan and China in the sphere of digital technologies and the development of digital infrastructure—both physical and data-related—emerged at the turn of the 20th and 21st centuries and has continued to evolve dynamically. Beyond the overarching framework of collaboration within the Belt and Road Initiative (BRI) and the Digital Silk Road (DSR)—both actively supported by the two governments—numerous memoranda have been signed between IT companies, including Kazakhstan’s state-owned Kazakhtelecom and Chinese corporations such as Huawei, China Telecom, and others, both public and private.

The growth of Kazakh–Chinese cooperation in the IT sector contributes, on the one hand, to the expansion of digitalization and to overcoming barriers to further digital development, particularly in terms of physical and data infrastructure. Furthermore, current turbulence in the global political landscape compels Kazakhstan to seek cost-effective technological solutions with shorter logistical routes. In this regard, cooperation with China and Chinese technology companies appears to be both a natural and logical choice. On the other hand, the growing dominance of Chinese vendors of hardware, software, and digital applications has raised valid concerns among Kazakhstani experts regarding the risk of digital dependency on China.

This study examines the achievements, opportunities, risks, and potential threats associated with the evolving digital cooperation between the Republic of Kazakhstan and the People’s Republic of China. The analysis covers the period up to August 2025.

## **Literature review**

Digital cooperation between China and Kazakhstan, as well as Central Asian countries, has repeatedly become the subject of research. Several scientific papers should be noted, in particular, the work “Prospects for Chinese-Kazakh Economic Cooperation in the Post-Covid Period”<sup>1</sup>, which notes international cooperation in building DSR: “China and Kazakhstan need to create a joint innovation community, deepen innovation and scientific and technological cooperation, build an integrated

---

<sup>1</sup> [Zhang Wanting, Problems of Modern Economy, No. 3 \(79\), 2021 UDC 339.92; BBK 65.011 pp: 139–142](#)

model of innovative cooperation in the field of production, teaching and research, focused on the needs of both sides. It is necessary to actively develop big data technology, artificial intelligence and “intelligence +” industries, and actively develop the industrial Internet”<sup>2</sup>.

In the study “The Digital Silk Road as a Form of Conjugation of the Eurasian Economic Union and the One Belt, One Road Project”<sup>3</sup>, the authors indicate the main areas of development of cooperation between the EAEU countries and China for the successful construction of the DSR: this is an increase in the level of digital integration of the EAEU member countries in order to reduce the digital inequality between them, improving the digital infrastructure of the EAEU member countries and developing new proprietary ICT technologies, expanding research and development in the field of modern next-generation technologies, including Big Data, cloud technologies, smart cities and AI. The authors also draw attention to the problems of training personnel for the knowledge-intensive industry, the need to use the common resources of the Eurasian market, and the need for institutional changes - harmonization of the legislation of the participating countries in the field of regulation of the digital economy, cybersecurity, etc.<sup>4</sup>

In the work “Regional Integration Projects and New Technologies: Digital Silk Road”<sup>5</sup>, the author emphasizes the existing gap in the technological development of China and most BRI countries; as a result, China occupies a leading position in building digital infrastructure. Central Asian countries are taking advantage of the opportunities provided by cooperation within the DSR for digitalization.<sup>6</sup>

---

<sup>2</sup> [Zhang, Wanting. “Prospects for Chinese-Kazakh Economic Cooperation in the Post-Covid Period.” Problems of Modern Economy, no. 3 \(79\), 2021: 139–142.](#)

<sup>3</sup> [Zhang Wanting, Selishcheva T.A., Dyatlov S.A., Problems of Modern Economy, N 1 \(77\), 2021 UDC 339.92; BBK 65.011 pp: 14–20](#)

<sup>4</sup> [Zhang, Wanting, T. A. Selishcheva, and S. A. Dyatlov. “The Digital Silk Road as a Form of Conjugation of the Eurasian Economic Union and the One Belt, One Road Project.” Problems of Modern Economy, no. 1 \(77\), 2021: 14–20.](#)

<sup>5</sup> [Tsvetkova N.N., Eastern Analytics, No. 1, 2019 ISSN 2227-5568](#)

<sup>6</sup> [Tsvetkova, N. N. “Regional Integration Projects and New Technologies: Digital Silk Road.” Eastern Analytics, no. 1, 2019.](#)

In the study “Cooperation between Kazakhstan, Russia and China in the Development of the Digital Silk Road: New Challenges and Prospects”<sup>7</sup>, the author analyzes the opportunities that open up for the BRI countries as a result of the implementation of the DSR, which is especially relevant in the context of trade wars and sanctions. Kazakhstan needs cooperation with neighboring countries within the framework of various agreements - BRI, SCO, EAEU, CSTO, to build the DSR and interaction in the field of cybersecurity, trade development and training of personnel for digitalization. The development of the DSR creates a sustainable environment for effective cooperation between countries.<sup>8</sup>

In addition to the aforementioned scientific works, there are other materials devoted to the analysis of the innovative component of the BRI, for example, “Formation of the Foundations of the “Digital Silk Road”<sup>9</sup>, “The Role of China as the Main Conductor of Digitalization in the Context of the Formation of Technological Sovereignty of the SCO Countries”<sup>10</sup>, and many others.

In addition to scientific articles, the topic of digital cooperation between Kazakhstan and China is regularly updated at official meetings of the leadership of the two countries in various formats, is reflected in numerous declarations, memoranda and other documents of international meetings, and is already deeply embedded in

---

<sup>7</sup> [Beisenbayev O.T., Proceedings of the 7th International Conference “East Asia: Past, Present, Future”, Institute of Far Eastern Studies of the Russian Academy of Sciences, 2020 UDC 908\(5-012\) BBK 26.89\(55\) B78](#)

<sup>8</sup> [Beisenbayev, O. T. “Sotrudnichestvo Kazakhstana, Rossii i Kitaya v razvitii Tsifrovogo Shelkovogo Puti: novye vyzovy i perspektivy” \[Cooperation between Kazakhstan, Russia, and China in the Development of the Digital Silk Road: New Challenges and Prospects\]. In Proceedings of the 7th International Conference “East Asia: Past, Present, Future”. Moscow: Institute of Far Eastern Studies RAS, 2020](#)

<sup>9</sup> [Liu, Yizhu, and E. F. Avdokushin. “Formirovanie osnov ‘Tsifrovogo Shelkovogo Puti’” \[Formation of the Foundations of the “Digital Silk Road”\]. The World of the New Economy 13, no. 3 \(2019\): 62–71.](#)

<sup>10</sup> [Fadeeva, I. A. “Rol’ Kitaya kak osnovnogo provodnika tsifrovizatsii v kontekste formirovaniya tekhnologicheskogo suvereniteta stran ShOS” \[The Role of China as the Main Conductor of Digitalization in the Context of the Formation of Technological Sovereignty of the SCO Countries\]. Fundamental Research, no. 11 \(2024\): 40–47.](#)

program documents on the development of digitalization in Kazakhstan. Also, this topic is often covered in media.

## **Methodology**

The research applies the Digital Technology Stack methodology<sup>11</sup>, under which cooperation between Kazakhstan and China in the digital domain is analyzed across five primary layers:

- Infrastructure layer: both physical infrastructure (fiber-optic communication lines, mobile internet stations, technical support centers, etc.) and digital infrastructure (data processing and storage centers, supercomputers, AI solutions, cloud services, etc.).
- Device layer: user devices such as smartphones, tablets, laptops, desktop computers, communication equipment, various smart devices, IoT tools, webcams, etc.
- Application layer: digital platforms and applications such as marketplaces, social networks, messengers, etc.
- Content layer: analysis of publications in digital media related to Kazakh-Chinese cooperation in the digital domain, including their tonality, reach, and dissemination.
- Internet governance layer: agreements signed between China and Kazakhstan on digital cooperation, as well as Chinese educational and informational initiatives that influence internet regulation and set future trends in internet governance in Kazakhstan.

Each layer of the digital stack is analyzed using open-source data derived from international agreements, company reports, press releases, and expert discussions

---

<sup>11</sup> ["China and Digital Information Stack in the Global South" by Bryce Barros, Nathan Kohlenberg and Etienne Soula 2022 The Alliance for Securing Democracy](#)

and opinions in media. The study is desk-based and relies exclusively on publicly available information, without recourse to focus groups or expert interviews.

### **Infrastructure layer**

The infrastructure layer is considered the base layer in the digital technology stack. An accessible and developed digital infrastructure determines the possibilities for digitalization, and makes other layers to a certain extent dependent on the development of the infrastructure layer. For the purposes of the study, it seems possible to combine the physical infrastructure and data infrastructure into a single layer in the analysis, since the main actors, both from the Kazakh and Chinese sides, adhere to a similar approach and consider the development of Kazakhstan's digital infrastructure as a single process.

This approach is largely determined by the geographical features of Kazakhstan and the difficulties associated with them – long distances, low population density, underdevelopment of the existing digital infrastructure network, and related economic problems, such as long payback periods and the associated unattractiveness of investments in infrastructure projects. In addition, traditionally, most fiber-optic cable routes connecting Kazakhstan and other Central Asian countries to the global Internet pass through Russian territory, which imposes its own restrictions on the development of Kazakhstan's digital infrastructure. This applies to both the limitations on the volume of transmitted traffic and the scaling capabilities, which are determined by the performance of data processing and storage centers.

#### *Trans-Caspian fiber-optic communication line*

The main project for the development of digital infrastructure in Kazakhstan is currently the work on laying the Trans-Caspian fiber-optic communication line (FOCL), which will connect the digital communication lines of Kazakhstan and other Central Asian countries with the global Internet through the South Caucasus countries. This project is also one of the key ones for the organization of the Middle Corridor,

connecting China with Europe bypassing the territory of Russia, and itself, in turn, is part of the East-West Digital Highway.<sup>12</sup>

It should be noted that the Trans-Caspian FOCL project was first considered in the mid-2000s; back in 2008 in Baku, at the Bakutel-2008 international exhibition and conference, was adopted the “Baku Declaration on the Transnational Eurasian Information Highway”, which envisaged the possibility of laying a FOCL along the bottom of the Caspian Sea<sup>13</sup>. However, at that time, a number of factors prevented the detailed development and implementation of this project. The large-scale project to build the Trans-Caspian FOCL was launched in 2019,<sup>14</sup> after the signing of the Interstate Agreement of March 19, 2019 between Azerbaijan and Kazakhstan<sup>15</sup>. In 2022, it became known that the Trans-Caspian FOCL would be built by two telecom operators: Kazakhstan’s Kazakhtelecom JSC and Azerbaijan’s AzerTelecom International. In the summer of 2023, these structures signed documents on the establishment of a joint venture for the construction and operation of the line, which was expected to become a full-fledged part of the large-scale DSR project, ensuring data transit between Europe and Asia, and would also give Kazakhstan the opportunity to reserve existing routes and create an international digital hub on its territory.<sup>16</sup> Started in 2022, the FOCL project began to be declared as part of the DSR, which in turn is a digital part of the Chinese global BRI. Related infrastructure projects, including the construction of the largest data processing centers (DPC) in Central Asia, in particular, the Freedom Cloud data center in the special economic zone “Alatau Innovation Technology Park”, which will become an alternative transit point for data transmission between Europe and China through the territory of Kazakhstan, as well

---

<sup>12</sup> [The Silk Road Reimagined: Connecting Hong Kong and Kazakhstan's Tech Ecosystems, Jackee Wong, Astana Hub](#)

<sup>13</sup> Azerbaijan State News Agency Ali Abbasov, 07.01.2009

<sup>14</sup> [Journalist's Investigations Center, Dmitri Shishkin, 18.09.2024](#)

<sup>15</sup> [Resolution of the Government of the Republic of Kazakhstan dated March 19, 2019 No. 119](#)

<sup>16</sup> [International Information Agency Kazinform, Digital Silk Way will connect Asia and Europe along the bottom of the Caspian Sea, 23.08.2023](#)



as the promising largest Tier IV data center in Central Asia in Astana, the construction of which was the subject of a memorandum signed in July 2025 between Kazakhstan's Akashi Data Center and the Chinese telecom giant China Mobile, are also part of the DSR.

In May 2025, it became known that the technical partner and contractor for the direct laying of the 380-kilometer cable between Aktau in Kazakhstan and Sumgait in Azerbaijan becomes HMN Technologies Co., Ltd., previously known as Huawei Marine Networks. The cable laying work is estimated at approximately 45-60 million USD, more precise data on the cost of the project is not publicly available.<sup>17</sup>

HMN Technologies Co., Ltd<sup>18</sup>, is a provider of submarine cable services based in Tianjin, China. The company specializes in turnkey submarine cable system services incorporating system design, installation, training and maintenance of submarine cables and provides equipment for network operators. The cable itself will most likely be supplied to HMN Technologies by its partner company Hengtong Optic-Electric Co Ltd.<sup>19</sup> based in Suzhou, China, which provides fiber optic communication products in China and internationally. The fact that the cable being laid will most likely be of Chinese manufacture was emphasized in an interview by Alibek Indykbayev, member of the board of JSC Kazakhtelecom and general director of the corporate business division: "As for the cable itself, which is over 300 kilometers long, there are several manufacturers on the world market... I cannot name specific companies, but in terms of logistics, if we consider the land route, Chinese manufacturers will have an advantage."<sup>20</sup>

---

<sup>17</sup> [BES.media portal, Prokladkoy-transkaspiskoy-vols-za-45-mln-dollarov-zaymyotsya-kitayskaya-kompaniya-hmn-tech, 30.05.2025](#)

<sup>18</sup> [HMN Technologies Co., Limited.](#)

<sup>19</sup> [Hengtong Optic-Electric Co Ltd](#)

<sup>20</sup> [Kursiv Media Agency, Alibek Indykbayev, The Trans-Caspian fiber-optic communication line will be operational as early as 2026, 26.10.2023](#)

In August 2025, information appeared in open sources that work on laying the FOCL had begun.<sup>21</sup> The Trans-Caspian FOCL construction project is the largest digital infrastructure project involving Chinese technology companies in Kazakhstan. Implementation of this project has given impetus to the construction of the largest data centers in Kazakhstan and Central Asia. However, this is not the only infrastructure project in which Chinese partners are involved.

#### *Huawei projects in Kazakhstan*

Projects to develop wireless Internet access for rural residents, develop 5G networks, cloud technologies and artificial intelligence continue to be relevant areas for Kazakh-Chinese cooperation in the field of digital infrastructure. Huawei Technologies is the leader in the implementation of these technologies and the creation of the corresponding infrastructure.

At the annual Huawei Technologies Partner Conference in April 2025, the company declared the launch of a project announced in 2023 to implement its cloud technologies for Kazakhstan's national railway carrier Kazakhstan Temir Zholy (KTZ);<sup>22</sup> Huawei has introduced SD-WAN technology, which has replaced outdated communications equipment and improved the speed and security of data transmission.<sup>23</sup> Digitalization of railway infrastructure is one of the priorities for the development of Kazakhstan's transit potential, and cooperation with a leading Chinese technology company is an important factor in the modernization of the railway transportation industry.

Another important infrastructure project of Huawei in Kazakhstan is the implementation of Fixed Wireless Access (FWA) technology for digitalization and increasing the speed of mobile data transmission in rural areas. In 2021, Huawei

---

<sup>21</sup> [Caspian Life Portal, Bagdat Mussin, From shore to shore: Kazakhstan and Azerbaijan launch joint project in the Caspian Sea, 06.08.2025](#)

<sup>22</sup> Huawei Technologies Co., Ltd. Huawei Partners Conference 2025: New Horizons for Digitalization and Growth in Kazakhstan

<sup>23</sup> Huawei Technologies Co., Ltd. KTZ and Huawei: How Kazakhstan's Railways Are Digitally Transforming

announced the launch of FWA in rural areas and suburbs of Shymkent; in 2025, in partnership with Auyt Telecom (a subsidiary of Kazakhtelecom JSC), Huawei began the testing in the Almaty region.<sup>24</sup> As part of the technology testing, more than 200 households were connected, and by the end of 2025 the company plans to increase the number of connected households to 10,000 in 100 settlements.

Huawei Technologies continues to cooperate with Kazakhstani companies providing mobile Internet access services. All major Kazakhstani mobile companies use Huawei equipment and technologies. For example, according to Beeline, “by May 2025, the average speed of Beeline mobile Internet in Almaty increased by 11% compared to April and by more than 40% compared to February 2024. Overall, an annual speed increase reached to 18.2% in the first half of 2025.”<sup>25</sup> This was achieved by the modernization of more than 300 base stations using Huawei Massive MIMO technology. In addition, Huawei modernizes and services the equipment of Kazakhtelecom JSC, as well as mobile operators Kcell/Activ and Tele2, so in 2024, contracts for equipment maintenance and modernization amounted to about 5.7 billion tenge.<sup>26</sup>

The company plans to conduct a pilot project to demonstrate Huawei's 10G broadband network in Astana,<sup>27</sup> development of Wi-Fi 7 technology, and participation in the construction of national data centers capable of supporting machine learning tasks and working with big data at the level of state infrastructure.<sup>28</sup>

---

<sup>24</sup> [International news agency "DKnews.kz" High-speed internet comes to Kazakhstan's villages, 21.01.2025](#)

<sup>25</sup> [Zakon.kz portal, Beeline and Huawei: A Partnership That Speeds Up Mobile Communications in Almaty – Speeds Increased by Over 40%, 22.07.2025](#)

<sup>26</sup> [Factcheck.kz, Million-Dollar Contracts: Huawei Selected in Kazakhstan Without Competitive Bid, 10.12.2024](#)

<sup>27</sup> [International news agency "DKnews.kz" Huawei and Astana Innovations launch a new phase of digital transformation in Kazakhstan, 16.06.2025](#)

<sup>28</sup> Huawei Technologies Co., Ltd.

Thus, Chinese technology companies are actively involved in the construction of Kazakhstan's digital infrastructure, thereby contributing to the strengthening of Kazakh-Chinese cooperation in the field of digitalization. Chinese companies act not only as contractors in the implementation of Kazakh infrastructure projects, but are also active participants in joint projects and collaborations with government agencies and quasi-state companies in Kazakhstan.

## **Device layer**

The device level covers consumer electronics that have Internet access functions, including communication, control, and content transfer. This category includes user devices and gadgets, telecommunications equipment, and IoT devices. This also includes control and video surveillance systems, access control systems, and a wide range of automotive electronics, including geo-positioning and traffic control systems.

### *Consumer Electronics and Smartphones*

In general, the dynamics of the consumer electronics market in Kazakhstan is stable, as is the stable prevalence of Chinese manufacturers in this market. And, if, according to Kapital.kz,<sup>29</sup> the share of Chinese-made smartphones is about 35-40%, then in the video surveillance systems market the share of Chinese vendors can reach more than 50%, and for user telecommunications equipment (modems, Wi-Fi amplifiers, fiberoptic adapters, etc.) up to 80%. This trend has been going on for a long time, and the only change that could affect the market dynamics in 2025 is the legislatively approved requirement to register IMEI codes of smartphones imported into Kazakhstan.<sup>30</sup> However, this innovation has not yet had a significant impact on the share of Chinese smartphones on the Kazakhstani market.

### *Devices for Smart cities*

---

<sup>29</sup> [Business Information Center Kapital.kz, Which smartphones are popular among Kazakhstanis? 14.01.2025](#)

<sup>30</sup> [Order of the Acting Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated January 13, 2025 No. 8/HK](#)

As for video surveillance systems and other smart city elements, this sector is currently developing rapidly. Thus, the Kazakhstani company Sergek received the prestigious Digital Almaty Award 2025 for the implementation of an intelligent video surveillance and analytics system for ensuring public safety Sergek VMS. This system is used by police in 14 cities of Kazakhstan to improve public safety, solve crimes, monitor emergency situations and other tasks; the system uses AI-based video analytics tools, including facial recognition. These technologies significantly speed up the response of security services and help in conducting operational investigations.<sup>31</sup> It should be noted that the Sergek company uses cameras manufactured by the Chinese company Dahua (Zhejiang Dahua Technology Co., Ltd) in its system.

In Almaty, as part of the implementation of the Safe City program, a unified video monitoring system project was launched in 2022, which has become the largest urban video analytics system in the country. It is planned that by the end of 2025, the number of centralized cameras will reach 70,000 (currently 45,000), of which 9,000 video cameras with a video analytics function, currently 1,165 cameras with a facial recognition system are operating in Almaty<sup>32</sup>. These are mainly Chinese-made cameras from Hikvision and Dahua, which have long been actively used by law enforcement agencies in Kazakhstan.<sup>33</sup>

Modern technologies for monitoring traffic conditions and public safety are also being actively introduced in the regions of Kazakhstan. Chinese vendors play an active role in this process, cameras from Hikvision, Dahua and other Chinese manufacturers provide high quality and reliability at a relatively low price, which is an important competitive advantage. In general, according to Kazinform, about 1,36

---

<sup>31</sup> [International news agency "DKnews.kz", Digital Almaty Awards 2025: Sergek VMS Recognized as the Best AI System, 14.01.2025](#)

<sup>32</sup> [Vlast Media Portal, Tamara Vaal, More than 7,800 cameras with facial recognition functionality will be installed in Almaty by the end of 2025, 13.12.2024](#)

<sup>33</sup> [Azattyq.kz, Kazakhstani edition of Radio Liberty/Radio Free Europe, Joldas Orisbay, Astana's video surveillance system will be modernized with the introduction of AI, 27.02.2025](#)

million cameras are operating in Kazakhstan, 310,000 of which are connected to various police command centers.<sup>34</sup>

#### *Internet of Things (IoT) Devices*

Chinese IoT companies are successfully promoting AI-based solutions for industry, automotive systems, fintech solutions, and many more.<sup>35</sup> For example, Xiaomi is actively implementing its key operating strategy “double focus on scale and profitability” in Kazakhstan. In 2023 was launched the strategy Smart Ecosystem Human-Car-Home, which includes scaling the Xiaomi AIoT platform to all IoT devices; Xiaomi launched its own car brand, and integrated all automotive, home and personal smart devices into a single network.<sup>36</sup> Such comprehensive solutions create serious competitive advantages and contribute to strengthening the leadership of Chinese IT companies in the IoT market in Kazakhstan.

Thus, Chinese technology companies have firmly established themselves in the Kazakhstan market as vendors of electronic equipment, and continue to strengthen their positions, including the market of consumer electronics and IoT systems; relatively low prices with fairly high quality, convenient logistics and the availability of service centers make Chinese electronics accessible to Kazakhstani buyers. New technologies, especially automotive electronics using AI, are becoming increasingly popular in the Kazakhstan market, and this further strengthens the position of Chinese vendors offering comprehensive solutions. The presence of Chinese companies at the device layer in Kazakhstan stays constant.

#### **Application layer**

---

<sup>34</sup> [“Kazinform” News Agency, Diana Bizhanova, Kazakhstan implements AI-powered video monitoring system, 20.11.2024](#)

<sup>35</sup> [South China Morning Post, Mia Nurmat, Belt and robot: Chinese start-up to open first robotics facility in Central Asia, 05.02.2025](#)

<sup>36</sup> [Alfa.kz portal of Multimedia Club LTD, Xiaomi's net profit for 2023 increased by 126.3%, 21.03.2024](#)

The application layer includes Chinese-developed software and applications that are present in the Kazakhstani Internet space and are used by Kazakhstani users for both personal and commercial purposes.

#### *TikTok Social Network*

Chinese social network TikTok has become the most popular social network in Kazakhstan, with the number of active TikTok users in the country reaching 10 million in 2024; about 60% of Kazakhstani users are young people aged 16 to 24.<sup>37</sup>

TikTok has an official representative office in Kazakhstan, opened in 2023. Kazakhstan's legislation regulating the activities of digital platforms and online advertising requires that owners of online platforms, the average daily access to which during the month is more than 100,000 users located in the Kazakhstani territory, appoint their legal representative to interact with regulators in accordance with the legal requirements of Kazakhstan.<sup>38</sup> TikTok's representative office in Kazakhstan actively cooperates with authorized bodies; in the Q1 2025 alone, more than 1,4 million videos were removed in Kazakhstan for violating Community Guidelines. The company emphasizes that 99% of them were removed proactively, before users complained about inappropriate content. For the whole of 2024, about 6,5 million videos were removed on TikTok in Kazakhstan. The main reason for removing videos is the spread of hate speech, pornography, calls for suicide, and other inappropriate content. TikTok indicates that 87% of the total volume of removed content was removed through automatic moderation technologies.<sup>39</sup> Thus, TikTok officially admits that it censors content using automatic moderation technologies. There is no publicly available information on the number of contested cases of content removal and the consequences of resolving such disputes. In

---

<sup>37</sup> [Check-point.kz Kazakhstani online information portal, Kazakhstani youth choose TikTok, 06.08.2024](#)

<sup>38</sup> [Law of the Republic of Kazakhstan dated July 10, 2023 No. 18-VIII 3PK About online platforms and online advertising](#)

<sup>39</sup> [TikTok website, TikTok Community Safety: The platform removed 1.4 million videos in Kazakhstan in the first quarter of 2025, 17.07.2025](#)

general, censoring content using automated moderation systems is a controversial concept, but the use of such moderation is supported by TikTok globally: in the Q1 2025, more than 211 million videos were removed from TikTok worldwide due to violation of community rules, and about 99% of video content was removed proactively. However, despite the work of the Kazakhstan representative office of TikTok, and the presence of systems for moderating unwanted content, the Kazakh authorities from time to time announce the possibility of banning the platform in Kazakhstan.<sup>40</sup>

Kazakhstan is a country where public debates about blocking or restricting the use of TikTok regularly arise in the public space. Thus, in the winter of 2025, Majilis Deputy Zhanarbek Ashimzhanov proposed restricting access to TikTok for minors in Kazakhstan;<sup>41</sup> earlier, in the fall of 2024, Senate Deputy Gennady Shipovskikh made a similar call.<sup>42</sup> However, TikTok is not restricted or blocked in Kazakhstan, unlike most neighboring countries.<sup>43</sup>

#### *Temu (Pinduoduo) Marketplace*

The Chinese marketplace Temu, which is an online store of the e-commerce company PDD Holdings (Pinduoduo), is actively operating in Kazakhstan. Temu, legally, is an international company registered in the Cayman Islands, but is positioned as a company trading Chinese goods directly from China. In China itself, the company operates through the internal marketplace Pinduoduo<sup>44</sup>.

---

<sup>40</sup> [Central Asian Bureau for Analytical Reporting, a project of the Institute For War & Peace Reporting, Fariza Ospan, Kazakhstan Discusses TikTok Blocking. What Is The Risk For Other Social Media? 08.05.2024](#)

<sup>41</sup> [Tengrinews.kz information portal, Aruzhan Daribay, "Like an atomic bomb." A deputy proposed restricting TikTok in Kazakhstan, 19.02.2025](#)

<sup>42</sup> [Tengrinews.kz information portal, Azamat Syzdykbayev, A deputy has demanded that TikTok be blocked in Kazakhstan, 03.10.2024](#)

<sup>43</sup> [Tengrinews.kz information portal, Which countries have banned TikTok? 20.01.2025](#)

<sup>44</sup> [Forbes Media LLC, Conor Murray, What to Know About Temu, 17.02.2023](#)



According to Netpeak Kazakhstan, the Temu app averaged 130,000 to 150,000 downloads per month during Q1 2025.<sup>45</sup> In order to make purchases on the marketplace, Kazakhstani users must provide their personal data - region, residential address, telephone number, full name, and Individual Identification Number (IIN).<sup>46</sup> According to the Personal Data Processing Policy, in addition to this data, user must also provide an email address.<sup>47</sup> When installing a mobile application, it requests many permissions, including access to the camera, microphone, contacts and other functions of the device, including geolocation, device data, IP address and interaction with other users. If the user refuses to provide data, the marketplace is unavailable (No Data No Service). In accordance with the Payment Policy, the marketplace does not collect bank card data and uses a third-party secure service Robokassa, which does not transfer bank card data to the online store or third parties.

The company's business model is based on advertising in social media. Temu encourages the creation of its communities in social networks; users who repost ads receive certain privileges in additional discounts, participation in competitions, and attract new users with their "success stories with Temu". The marketplace buys large volumes of advertising traffic in social networks to occupy the highest positions in the search results of Google, Yandex and other search engines in Kazakhstan. Such an aggressive approach to advertising the marketplace, coupled with low prices of the products sold, creates certain competitive advantages, and is the subject of criticism from Kazakhstani e-commerce experts. Temu uses the same approach in all markets where the marketplace is present, including the US and Europe.<sup>48</sup>

The quality of the products and the use of intellectual property also leave a lot of questions. According to the US-China Economic and Security Review Commission (USCC), "Temu's lack of affiliation with established brands has brought concerns of

---

<sup>45</sup> [Tribune.kz, a website of Central Asian Advertising Association, What mobile apps did Kazakhstanis install in the first quarter of 2025, 17.07.2025](#)

<sup>46</sup> [Website of Temu marketplace](#)

<sup>47</sup> [Privacy Policy of Temu marketplace](#)

<sup>48</sup> Profit Online news portal, Temu – on topic or not? 14.02.2025

product quality as well as accusations of copyright infringement.” The marketplace does not check the quality and compliance of the products sold, uses forced labor in supply chains, and neglects the security of customer data.<sup>49</sup>

Temu’s operations in Kazakhstan have also been criticized for being unregulated and lacking an official representative. The website [temu.com.kz](http://temu.com.kz) is registered to a private individual and can be removed at any time;<sup>50</sup> 92 more sites are registered on the server’s IP address.<sup>51</sup> In addition, the site is not registered and does not pay taxes.

There are no publicly available statistics on the marketplace’s sales volumes in Kazakhstan, but judging by the aggressive advertising and app download statistics, Temu is one of the most popular marketplaces. The low price of the goods presented on the marketplace plays a major role and attracts Kazakhstani consumers; they often do not pay attention to problems with the security of personal data, counterfeit use of brands and overly aggressive advertising.

Thus, Chinese influence at the application layer in Kazakhstan is growing, despite the existing problems. The most popular public apps are TikTok and Temu, whose audiences are constantly growing and have already made them leaders in the social media and e-commerce app market. It should be noted that Chinese app market leaders, such as WeChat, Baidu, QQ, etc, almost not represented in Kazakhstan.

### **Content layer**

The content layer covers the promotion of messages and narratives in the digital environment by the Chinese government and state-affiliated and state-supported media outlets, with the aim of improving China’s image around the world.

#### *Traditional media*

---

<sup>49</sup> [Issue brief by the research staff of US-China Economic and Security Review Commission, Nicholas Kaufman, Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes, 14.04.2023](#)

<sup>50</sup> [Whois domain check portal, Whois Record for Temu.com.kz](#)

<sup>51</sup> [DomainTools Reverse IP Lookup, 213.130.74.19 Reverse IP Lookup](#)

There are Chinese media outlets in Kazakhstan, including news agencies, TV channels and print media covering events in China and bilateral relations. However, their number and coverage are relatively limited. For example, some TV channels (CGTN, CCTV and others) are included in cable operators' broadcasting networks, but are not included in basic packages. News agencies, such as Xinhua, have offices in Kazakhstan and mainly cover events that take place within the framework of Kazakh-Chinese cooperation and domestic Chinese topics.

Chinese media attach great importance to collaboration with local media, and are often participants in joint media projects. For example, in June 2025, the Xinhua agency initiated and held the China-Central Asia News Agency Forum, in which participated representatives of the state-owned media agencies from Central Asia. Speaking at the forum, Fu Hua, Director General of Xinhua News Agency, said, "China and Central Asian news agencies have the responsibility to spread the Central Asia-China Spirit and jointly tell the stories of China-Central Asia cooperation, promote China-Central Asia people-to-people exchanges and mutual learning between civilizations, advance innovation and cooperation in media technology, deepen exchanges and cooperation between news agencies, and contribute to promoting the building of a community with a shared future for China and Central Asia."<sup>52</sup> The CGTN (China Global Television Network) television channel and the Kazakhstani state-owned Silk Way television channel, launched a joint long-term project in 2024 to strengthen friendship and cooperation between the countries.<sup>53</sup> As part of this joint project, a number of events will be organized in 2025, including televised debates, joint news broadcasts, joint press tours, etc.<sup>54</sup> In addition to the Silk Way TV

---

<sup>52</sup> [Xinhua News Agency, The China-Central Asia News Agency Forum was held in Astana, 22.06.2022](#)

<sup>53</sup> [Television and Radio Complex of the Presidential Administration of the Republic of Kazakhstan, Silk Way TV and China Global Television Network \(CGTN\) have launched a joint project, 01.07.2024](#)

<sup>54</sup> [International Information Agency "Kazinform", Muratbek Makulbekov, Silk Way and CGTN: International TV project to air in Kazakhstan and China, 16.06.2025](#)

channel, the collaboration also includes the Kazakh Atameken Business TV channel, which belongs to the Atameken National Chamber of Entrepreneurs. Thus, in addition to state-owned media, Kazakh private TV channels are also ready to collaborate with Chinese media and promote the agenda of Kazakh-Chinese cooperation.<sup>55</sup>

### *Social Media*

The presence of Chinese media in social networks and Telegram channels in Kazakhstan is relatively small. For example, the Xinhua agency has a profile on Facebook, but only about 14,000 subscribers, which is a small number for a news portal. The content promoted by the account includes news, photos and videos, and contains information about cooperation between China and countries included in the BRI initiative.<sup>56</sup>

Among Telegram channels, it is worth noting the work of the Kazakhstani channel AB Silk Way, which has about 4,000 subscribers. The channel belongs to the Atameken Business TV channel. The channel initially, in 2023, had about 50% of the content in Russian, and 50% in Kazakh, currently almost 100% of the channel's content is in Kazakh. The channel provides positive information about China, including both economic and cultural news, and is aimed at creating a positive image of China for the Kazakh-speaking audience.<sup>57</sup>

An example of an analytical Telegram channel is the channel of the Kazakh sinologist Adil Kaukenov about China in Central Asia and around the world, "Notes of a Kazakh Sinologist".<sup>58</sup> The channel has about 5,000 subscribers. The channel publishes analytical materials on a wide range of topics of Kazakh-Chinese cooperation. The owner of the channel, Sinologist Adil Kaukenov, is the head of the Scientific and

---

<sup>55</sup> [Media Holding Atameken Business, Sayan Abayev, The best Chinese programs and films are shown in Kazakhstan, 03.07.2024](#)

<sup>56</sup> [Xinhua News Facebook account](#)

<sup>57</sup> Atameken Business Telegram Channel

<sup>58</sup> Adil Kaukenov Telegram Channel

Educational Center “Belt and Road”, opened under the auspices of the Institute of Philosophy, Political Science and Religious Studies. The publications are in Russian. Currently, the number of publications about China and news related to Chinese initiatives is increasing, and their tone is invariably positive. The growth of content on Kazakh-Chinese cooperation is recorded both in traditional and social media. This indicates an increase in interest in information about China, and leads to positive changes in the perception of Kazakh-Chinese cooperation in Kazakh society.

### **Internet Governance layer**

The Internet Governance layer examines international agreements related to the digitalization of Kazakhstan with the participation of Chinese partners, as well as initiatives of the largest Chinese technology companies that influence the legal environment and form, or significantly influence, the rules of the game for the development of internet in Kazakhstan. In addition, this layer also considers Kazakh-Chinese initiatives in the educational sphere, concerning the improvement of the quality of human capital in Kazakhstan, which is necessary for further digitalization.

#### *Second China-Central Asia Summit*

The second China-Central Asia Summit, held on June 17, 2025 in Astana, brought together the leaders of China and the five Central Asian states, built on the agreements reached during the first meeting in Xi'an, China, in May 2023. The summit aimed to deepen economic, security and cultural cooperation, and institutionalize and strengthen the China-Central Asia mechanism as a platform for mutually beneficial economic cooperation and regional stability.<sup>59</sup>

During the summit, the speech of Chairman Xi Jinping also voiced the prospects for digital cooperation between the Central Asian countries and China: “We are ready to share development experience and the latest technological achievements with the Central Asian states, promote digital infrastructure communications, expand cooperation in the field of artificial intelligence, and cultivate productive forces of a

---

<sup>59</sup> [News Central Asia, Report – Second China-Central Asia Summit, 18.06.2025](#)

new quality.”<sup>60</sup> Thus, China confirms its participation in the digitalization of Kazakhstan and expresses its readiness to cooperate in this area in the future.

At the summit, a wide range of documents were signed on cooperation between Kazakhstan and China in various economic spheres. In particular, a Memorandum was signed between Samruk-Kazyna JSC and Huawei Kazakhstan on cooperation in the field of digital transformation of energy and cybersecurity. The memorandum includes a number of key areas of cooperation, including the development and implementation of digital platforms and cloud solutions, the creation and development of 5G networks and smart cities, support for educational initiatives aimed at developing skills in the field of digital technologies.<sup>61</sup> Also, a Memorandum of Understanding was signed between the Ministry of Energy and Huawei Technologies Kazakhstan, aimed at the digital transformation of the energy sector and strengthening its cybersecurity. The document provides for the implementation of joint innovative projects on digitalization in the oil and gas, mining and electric power industries of Kazakhstan, using AI and big data technologies to improve energy efficiency, environmental friendliness and reliability of the energy system.<sup>62</sup> Adopted at the Summit the Astana Declaration also includes provisions important for Internet governance. This concerns both strengthening cybersecurity in the face of new threats, and the regular exchange of information for support the development of a peaceful, open, secure, cooperative and orderly cyberspace within the framework of the Global Data Security Initiative.<sup>63</sup>

Speaking at the summit, President of Kazakhstan K-Zh. Tokayev emphasized Kazakhstan’s interest in implementing joint projects with China in the field of artificial

---

<sup>60</sup> [CGTN web portal, Xi Jinping's keynote speech at the 2nd China-Central Asia Summit, 17.06.2025](#)

<sup>61</sup> Huawei Technologies Co., Ltd, Huawei and Samruk-Kazyna signed a memorandum of understanding on digital transformation, 19.06.2025

<sup>62</sup> [ICT Magazine, The Ministry of Energy of Kazakhstan and Huawei signed a memorandum on digitalization of the energy sector, 25.06.2025](#)

<sup>63</sup> [Xinhua News Agency, Astana Declaration of the Second Central Asia-China Summit, 18.06.2025](#)

intelligence: “China’s impressive achievements in the development of cosmonautics and quantum technologies have confirmed its status as a global technological power. Therefore, Kazakhstan is interested in implementing joint projects in the field of artificial intelligence, biotechnology, quantum computing, as well as in the creation of research centers and technologies.” The President also announced the opening of the Alem AI artificial intelligence center in Astana in the fall of 2025 on the basis of Astana Hub, and invited foreign partners to cooperate: “We propose using the Astana Hub platform to promote smart innovations within the framework of the Central Asia-China format. All foreign partners could also take part in this promising project.”<sup>64</sup>

#### *China’s Digital Education Initiatives*

Chinese educational initiatives can be roughly divided into two main categories. First, these are Chinese state educational initiatives, including Confucius Institutes, Lu Ban Workshops, and the activities of Kazakh branches of Chinese universities in Kazakhstan. Secondly, there are schools, trainings and workshops initiated by Chinese tech companies such as Huawei and TikTok, which help users and experts to effectively use these companies’ products.

Currently, there are five Confucius Institutes in Kazakhstan: Astana (based on the Eurasian National University), Almaty (based on the Kazakh National University and the Kazakh University of International Relations and World Languages), Karaganda (based on the Karaganda State Technical University) and Aktobe (based on the Aktobe State Pedagogical Institute). Students who attend classes at Confucius Institutes have the opportunity to participate in exchange programs with Chinese universities and subsequently get jobs in Chinese companies, including technology companies.

Lu Ban’s workshops are educational institutions at universities where students gain practical knowledge in the technical field by working with Chinese machines on

---

<sup>64</sup> [International Information Agency "Kazinform", Karina Kuschanova, Kazakhstan is interested in joint AI projects with China, 17.06.2025](#)

Chinese equipment. The first Lu Ban workshop opened in 2023 at the East Kazakhstan Technical University in Ust-Kamenogorsk, and specializes in training specialists in the repair and maintenance of Chinese electric vehicles, hybrid vehicles, and the use of artificial intelligence in car control and traffic management.<sup>65</sup> Lu Ban's second workshop will be opened in Astana at the Eurasian National University in fall 2025. It is planned that the main focus of the workshop will be the development of human resources in the field of digital technologies and AI.<sup>66</sup>

Chinese universities are opening their branches in collaboration with Kazakh universities. The first example of such collaboration is the opening of a branch of the Northwestern Polytechnical University of China at the Kazakh National University in 2023; the branch trains students from Kazakhstan and Central Asia in bachelor's and master's programs in engineering, electronic science and technology, IT, etc.<sup>67</sup> In 2024, a branch of Beijing Language and Culture University (BLCU) opened in Astana in cooperation with Astana International University (AIU). In 2025, the Atyrau University of Oil and Gas officially opened the Chinese Jingshi Institute (specializing in petroleum engineering technologies), which trains highly qualified specialists in oil and gas.<sup>68</sup>

Chinese technology companies are also actively involved in training Kazakhstani personnel for the IT sector. For example, Huawei Technologies is developing a network of ICT Academies throughout Kazakhstan to train students in technical specialties and support domestic personnel, as part of the state strategy to train

---

<sup>65</sup> [International Academy of Cultural and Economic Cooperation "New Silk Road", Lu Ban's workshop in Kazakhstan](#)

<sup>66</sup> [Website of Eurasian National University, Lu Ban Workshop to be established at ENU, 22.11.2024](#)

<sup>67</sup> [State Electronic Government Portal eGov, A branch of the Chinese University will open at KazNU, 18.05.2023](#)

<sup>68</sup> [Website of Atyrau Oil and Gas University, Strategic agreement with Liaoning University of Petroleum and Chemical Technology](#)



100,000 Kazakhstani IT specialists by 2025.<sup>69</sup> In addition to Huawei ICT Academies, the company is also developing other educational projects. For example, since 2008, the Seeds of the Future program for the development of young talents has been operating around the world. In Kazakhstan, in 2021, 30 students from 7 leading universities in the country participated in it.<sup>70</sup>

TikTok is also actively involved in educational and outreach activities in Kazakhstan. TikTok has opened a Startup Academy at the Astana Hub platform, where it plans to train users and entrepreneurs who want to use TikTok to develop their startups.<sup>71</sup> In 2022, TikTok organized the TikTok Film Academy competition, in which users tried to participate in the filming of short feature films,<sup>72</sup> the Learn on TikTok competition, where contestants make short popular science films, and other similar competitions.<sup>73</sup>

In addition to educational events, Chinese IT companies actively organize their own IT events, for example, the annual Huawei Partner Conference in 2025 brought together more than 200 IT industry specialists and business partners.<sup>74</sup> Huawei, Hikvision, CITIC Group, TikTok and other Chinese companies act as co-sponsors of major IT events in Kazakhstan, such as Digital Bridge, which brings together a large number of IT specialists not only from Kazakhstan, but also from the entire Central Asian region.

Thus, cooperation with China in the digital sphere has a serious impact on Internet governance in Kazakhstan. Taking into account all the memorandums already

---

<sup>69</sup> [Huawei Technologies Co., Ltd. Kazakhstani students won three prizes at the Huawei ICT Competition 2024–2025 international finals in China, 27.05.2025](#)

<sup>70</sup> [Tengrinews.kz information portal, New directions for digital development offered by Huawei in Kazakhstan, 03.11.2021](#)

<sup>71</sup> [Astana Hub, TikTok Startup Academy](#)

<sup>72</sup> [Blue Screen Technological Media Portal, TikTok launches a competition with the support of leading Kazakh filmmakers, 09.11.2022](#)

<sup>73</sup> [Profit Online news portal, TikTok launches "Learn on TikTok Kazakhstan" initiative, 25.05.2022](#)

<sup>74</sup> Huawei Technologies Co., Ltd. Huawei Partners Conference 2025

concluded, it is clear that the influence of Chinese technologies and Chinese approaches to digitalization, including AI regulations, will increase. The conclusion of memorandums and agreements forms the technological environment and contributes to changes in legislation and law enforcement practices. The large number of students and young professionals who have received technical education through Chinese educational initiatives also influence the technological environment of Kazakhstan, bringing and integrating Chinese approaches and standards.

## **Conclusion**

Kazakh-Chinese cooperation in the digital environment is developing at record high rates at all layers of the Digital Stack. Chinese companies are actively involved in the construction of Kazakhstan's digital infrastructure, Chinese vendors are steadily increasing sales of consumer and business electronics, Chinese applications are actively used by Kazakhstani users, the amount of positive content related to China is increasing, and a favorable environment is being created for the development of the Internet using Chinese technologies, including AI, cloud services and big data tools.

Such deep involvement of Chinese companies in the digitalization of Kazakhstan is due not only to a large number of intergovernmental agreements and a favorable business climate for Chinese companies in Kazakhstan. The new geopolitical reality, including the consequences of COVID 19 pandemic, the war in Ukraine and the Middle East, serious obstacles to international shipping, make the Middle Corridor increasingly important for world trade. China's role in the development of this corridor has always been key, as has Kazakhstan's participation in its implementation. In addition, disruptions to the international supply chain caused by geopolitical changes have played into the hands of Chinese high-tech equipment manufacturers, since China's logistics to Central Asian countries and Kazakhstan are not affected by these changes. The cost of Chinese technological solutions was previously relatively low, but now the prices of competitors – companies from the USA and Europe – have increased even more due to difficulties with logistics. Thus, this situation benefits

both Kazakhstan, which can relatively inexpensively expand its digital infrastructure and ensure digitalization, and Chinese companies, which do not experience competitive pressure from other manufacturers. All these factors contribute to further strengthening of cooperation between Kazakhstan and China in the field of digitalization.

However, this situation, in addition to obvious advantages, also carries certain risks and threats. As for the risks for the infrastructure and the device layers, Kazakhstan does not have its own production of electronic components and optical fiber, does not produce or localize on its territory the production of full-cycle electronic devices, does not produce microchips and other electronic devices necessary for digitalization. This seriously limits the participation of Kazakhstani companies in electronic equipment supplies for digitalization needs. Those Kazakhstani companies that produce computers in Kazakhstan (LogiCom, ALSI, etc.) actually carry out large-unit assembly from completely imported components, and are dependent on the supply of these components; the vendors of these components are predominantly Chinese companies, which further increases the dependence of the Kazakhstani market on Chinese suppliers.<sup>75</sup>

In terms of the layer of programs and applications, Kazakhstan has shown some progress. Thus, in the UN E-Government Rating in 2024<sup>76</sup> the country took 24th place, moving up 4 positions compared to the previous 2022 ranking.<sup>77</sup> This rating focuses more on software for government services eGov and related platforms, and it does not cover the broad consumer market. Kazakhstani IT company BTS Digital, the affiliate of mining company ERG, has developed its own messenger, Aitu, but it is not

---

<sup>75</sup> [Russia and China in Central Asia's Technology Stack: An analysis of Kazakhstan, Kyrgyzstan and Uzbekistan by Dylan Welch, 05.06.2025](#)

<sup>76</sup> [UN E-Government Survey 2024 Accelerating Digital Transformation for Sustainable Development](#)

<sup>77</sup> [State Electronic Government Portal eGov, Kazakhstan ranked 24th in the UN e-government global ranking, 18.09.2024](#)

popular among users. The Kazakh authorities are now forcing state bodies to use this messenger, citing its “high level of security.”<sup>78</sup> It is obvious that Kazakhstani users prefer widely known products that allow global communication and have a large number of services, but in Kazakhstan there are objectively no opportunities for the development and distribution of such products. Therefore, dependence on international platforms, including Russian and Chinese ones, remains.

At the content level, the prevalence of positive news and messages can also play a cruel joke on Kazakhstani consumers. The absence of criticism quietly turns into a ban on criticism: many reports of poor quality or design flaws in Chinese machines, equipment, components, etc. are kept under wraps. The desire to create a positive image of China and to muffle critical statements, which is de facto state policy in Kazakhstan, unties hands for the use of repression against critics, using the available tools, including initiating cases for disseminating false information.

All these factors cannot but have a negative impact on Internet governance. The established dominance of China at the levels of infrastructure, devices and applications, and rapid growth at the level of content, critically affect the digital environment and dictate changes that adapt the digital environment to Chinese requirements. Legislative restrictions imposed on freedom of expression lead to self-censorship, de facto existing censorship strengthens restrictions, which leads to less freedom and limits development. Thus, to the already existing negative factors - geographical remoteness, weak infrastructure, no access to the sea, low population density, and, as a result, a small domestic market - are added artificial restrictions on freedom of speech, expression, and exchange of information, hindering the development of an industry that is developing dynamically in other regions of the world. The associated technological lag and increasing dependence on Chinese suppliers lead to dependence in the sphere of Internet governance, which can be overcome by broad diversification of the market of equipment and software vendors,

---

<sup>78</sup> [Tengrinews.kz information portal, Alina Shashkina, The Kazakh government will switch to a national messenger, 11.08.2025](https://tengrinews.kz/information-portal/Alina-Shashkina-The-Kazakh-government-will-switch-to-a-national-messenger-11.08.2025)

which will not allow any one country to become the main supplier of technological solutions. And, if a multi-vector approach is applied in Kazakhstan's foreign policy, the same approach should be applied to the country's technological development. Good-neighborly relations and developing technological cooperation between Kazakhstan and China should not lead to Kazakhstan's technological dependence on China.

## **Recommendations**

### *For Infrastructure and Device Layers*

It is essential to continue collaborating with Chinese and other international partners to strengthen and develop Kazakhstan's digital infrastructure, shifting focus to domestic production of electronic components for Kazakhstan's digitalization needs. Strategic areas of domestic production should include the creation of high-cycle silicon processing plants for the production of domestic semiconductor products, the production of fiber-optic cables, and the acquisition of licenses for the production of electronic equipment in Kazakhstan, which will ultimately allow us to avoid technological dependence on foreign manufacturers.

### *For Application Layer*

It is necessary to continue developing and implementing domestic software, both for general civilian and specialized tasks, and to utilize existing international experience, including Chinese experience, to promote domestic applications both domestically and abroad.

### *For Content Layer*

Continue and deepen efforts to disseminate information about technological advances, emphasizing domestic developments, success stories, and the promotion of Kazakhstani digital products, including those using AI technologies. Promoting Kazakhstan's technological achievements should become one of Kazakhstani soft power tools, fostering a positive image of the country and attracting investment into the economy.

### *For Internet Governance Layer*

It is necessary to continue efforts to improve the quality of human capital for digitalization and create conditions for internet development. This includes creating special tax regimes for manufacturers of hardware and software, ensuring maximum favorable conditions for domestic manufacturers in public procurement of hardware and software, as well as requirements to protect the rights and interests of citizens, including the right to privacy and the protection of personal and biometric data when using programs and gadgets. The harmonious development of the Internet industry should become one of the priorities of the country's state policy.

## Bibliography

- Abayev, S. (2024, July 3). The best Chinese programs and films are shown in Kazakhstan. *Atameken Business*. <https://www.inbusiness.kz/ru/news/luchshie-programmy-i-filmy-kitaya-pokazyvayut-v-kazahstane>
- Abbasov, A. (2009, January 7). *Azerbaijan State News Agency*.
- Alfa.kz. (2024, March 21). Xiaomi's net profit for 2023 increased by 126.3%. *Alfa.kz*. [https://alfa.kz/node/12397/chistaya\\_pribil\\_xiaomi\\_za\\_2023\\_god\\_uvelichilas\\_a\\_na\\_126\\_3](https://alfa.kz/node/12397/chistaya_pribil_xiaomi_za_2023_god_uvelichilas_a_na_126_3)
- Astana Hub. (n.d.). *TikTok Startup Academy*. <https://astanahub.com/en/ITikTokStartupAcademy>
- Atameken Business [@atameken\_business]. (n.d.). *Telegram channel*. Telegram.
- Atyrau Oil and Gas University. (2025). *Strategic agreement with Liaoning University of Petroleum and Chemical Technology*. <https://aogu.edu.kz/news/03092025/>
- Barros, B., Kohlenberg, N., & Soula, E. (2022). *China and digital information stack in the Global South. Alliance for Securing Democracy*. <https://securingdemocracy.gmfus.org/wp-content/uploads/2022/06/China-Digital-Stack.pdf>
- Beisenbayev, O. T. (2020). Sotrudnichestvo Kazakhstana, Rossii i Kitaya v razvitii Tsifrovogo Shelkovogo Puti: novye vyzovy i perspektivy [Cooperation between Kazakhstan, Russia, and China in the development of the Digital Silk Road: New challenges and prospects]. In *Proceedings of the 7th International Conference 'East Asia: Past, Present, Future'*. Institute of Far Eastern Studies RAS. <https://cyberleninka.ru/article/n/sotrudnichestvo-kazahstana-rossii-i-kitaya-v-razvitii-tsifrovogo-shelkovogo-puti-novye-vyzovy-i-perspektivy/viewer>
- BES.media. (2025, May 30). Китайская HMN Tech проложит интернет-кабель по дну Каспия за 45 млн долларов [Chinese company HMN Tech will lay the Trans-Caspian fiber-optic line for \$45 million]. *BES.media*. <https://bes.media/news/prokladkoy-transkaspiskoy-vols-za-45-mln-dollarov-zaymyotsya-kitayskaya-kompaniya-hmn-tech/>
- Bizhanova, D. (2024, November 20). Kazakhstan implements AI-powered video monitoring system. *Kazinform*. [https://www.inform.kz/ru/cifrovoy-shelkovyy-put-ob-edinit-aziyu-i-evropu-po-dnu-kaspiya\\_a4104525](https://www.inform.kz/ru/cifrovoy-shelkovyy-put-ob-edinit-aziyu-i-evropu-po-dnu-kaspiya_a4104525)
- Blue Screen. (2022, November 9). TikTok launches a competition with the support of leading Kazakh filmmakers. *Blue Screen*. <https://soroskz.sharepoint.com/sites/CentralAsia-ChinaRoundtable10-11November/Shared%20Documents/For%20Interns/Original%20Papers/blue-screen.kz/news/12203/tiktok-zapuskaiet-konkurs-pri-poddierzhkie-viedushchikh-dieiateliei-kino-kazahstana>
- Business Information Center Kapital.kz. (2025, January 14). Which smartphones are popular among Kazakhstanis? *Kapital.kz*. <https://kapital.kz/economic/133381/kakiye-smartfony-populyarny-u-kazakhstantsev.html>



- Caspian Life Portal. (2025, August 6). From shore to shore: Kazakhstan and Azerbaijan launch joint project in the Caspian Sea [B. Mussin]. *Caspian Life*. <https://rus.caspianlife.kz/32391>
- Central Asian Bureau for Analytical Reporting. (2024, May 8). Kazakhstan discusses TikTok blocking. What is the risk for other social media? [F. Ospan]. *Institute For War & Peace Reporting*. <https://cabar.asia/en/kazakhstan-discusses-tiktok-blocking-what-is-the-risk-for-other-social-media>
- CGTN. (2025, June 17). Xi Jinping's keynote speech at the 2nd China-Central Asia Summit. CGTN. <https://russian.cgtn.com/news/2025-06-17/1934935699277127681/index.html>
- Check-point.kz. (2024, August 6). Kazakhstani youth choose TikTok. *Check-point.kz*. <https://check-point.kz/publication?id=1710>
- Daribay, A. (2025, February 19). 'Like an atomic bomb.' A deputy proposed restricting TikTok in Kazakhstan. *Tengrinews.kz*. [https://tengrinews.kz/kazakhstan\\_news/kak-atomnaya-bomba-deputat-predlozil-ogranichit-tiktok-562967/](https://tengrinews.kz/kazakhstan_news/kak-atomnaya-bomba-deputat-predlozil-ogranichit-tiktok-562967/)
- DKnews.kz. (2025, January 21). High-speed internet comes to Kazakhstan's villages. *DKnews.kz*. <https://dknews.kz/ru/dk-it/350138-vysokoskorostnoy-internet-prihodit-v-sela-kazahstana>
- DKnews.kz. (2025, January 14). Digital Almaty Awards 2025: Sergek VMS recognized as the best AI system. *DKnews.kz*. <https://dknews.kz/ru/dk-it/351146-digital-almaty-awards-2025-sergek-vms-priznana>
- DKnews.kz. (2025, June 16). Huawei and Astana Innovations launch a new phase of digital transformation in Kazakhstan. *DKnews.kz*. <https://dknews.kz/ru/dk-it/362526-huawei-i-astana-innovations-zapuskayut-novyy-etap>
- DomainTools. (n.d.). 213.130.74.19 Reverse IP lookup. <https://reverseip.domaintools.com/search/?q=temu.com.kz>
- eGov. (2023, May 18). A branch of the Chinese University will open at KazNU. *State Electronic Government Portal*. <https://www.gov.kz/memleket/entities/sci/press/news/details/556921?lang=ru>
- eGov. (2024, September 18). Kazakhstan ranked 24th in the UN e-government global ranking. *State Electronic Government Portal*. <https://www.gov.kz/memleket/entities/maidd/press/news/details/847800>
- Eurasian National University. (2024, November 22). Lu Ban Workshop to be established at ENU. *Eurasian National University*. <https://enu.kz/ru/news/3444>
- Factcheck.kz. (2024, December 10). Million-dollar contracts: Huawei selected in Kazakhstan without competitive bid. *Factcheck.kz*. <https://factcheck.kz/vestnik-goszakupok/kontrakty-na-millions-dollarov-huawei-vybirayut-v-kazahstane-vne-konkursa/>
- Fadeeva, I. A. (2024). Rol' Kitaya kak osnovnogo provodnika tsifrovizatsii v kontekste formirovaniya tekhnologicheskogo suvereniteta stran ShOS [The role of China as the main conductor of digitalization in the context of the formation of



- technological sovereignty of the SCO countries]. *Fundamental Research*(11), 40–47. <https://fundamental-research.ru/ru/article/view?id=43712>
- Forbes Media LLC. (2023, February 17). What to know about Temu [C. Murray]. *Forbes*. [forbes.com/sites/conormurray/2023/02/17/what-to-know-about-temu-new-chinese-owned-fast-fashion-app-draws-comparisons-good-and-bad-to-shein](https://forbes.com/sites/conormurray/2023/02/17/what-to-know-about-temu-new-chinese-owned-fast-fashion-app-draws-comparisons-good-and-bad-to-shein)
- Hengtong Optic-Electric Co Ltd. (n.d.). *Company information*. <https://www.hengtongglobal.com/our-company>
- HMN Technologies Co., Limited. (n.d.). *Company information*. <https://www.hmntech.com/front/en>
- Huawei Technologies Co., Ltd.. (2025, May 19). Huawei Partners Conference 2025: New horizons for digitalization and growth in Kazakhstan. *Huawei*.
- — —. (n.d.-c). KTZ and Huawei: How Kazakhstan's railways are digitally transforming. *Huawei*. <https://e.huawei.com/en/case-studies/solutions/enterprise-network/ktz>
- — —. (2025, May 27). Kazakhstani students won three prizes at the Huawei ICT Competition 2024–2025 international finals in China. *Huawei*.
- — —. (2025, June 19). Huawei and Samruk-Kazyna signed a memorandum of understanding on digital transformation. *Huawei*.
- ICT Magazine. (2025, June 25). The Ministry of Energy of Kazakhstan and Huawei signed a memorandum on digitalization of the energy sector. *ICT Magazine*. <https://ictmagazine.kz/ministerstvo-energetiki-kazahstana-i-huawei-podpisali-memorandum-o-czifrovizaczii-energetiki/>
- Indykbayev, A. (2023, October 26). The Trans-Caspian fiber-optic communication line will be operational as early as 2026. *Kursiv Media Agency*. <https://kz.kursiv.media/2023-10-26/skvr-indikb/>
- International Academy of Cultural and Economic Cooperation 'New Silk Road.' (n.d.). *Lu Ban's workshop in Kazakhstan*. <https://silk-road-today.kz/news/1977-masterskaya-lu-ban-v-kazahstane.html>
- Journalist's Investigations Center. (2024, September 18). [Article by D. Shishkin]. *Journalist's Investigations Center*. <https://www.czhr.kz/post/%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BA%D0%B0%D1%81%D0%BF%D0%B8%D0%B9%D1%81%D0%BA%D0%B0%D1%8F-%D0%B2%D0%BE%D0%BB%D1%81-%D0%B8%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F-%D0%BE%D0%B1%D0%B5%D1%89%D0%B0%D0%BD%D0%B8%D0%B9>
- Kaukenov, A. [@adilkaukenov]. (n.d.). *Telegram channel*. Telegram.
- Kaufman, N. (2023, April 14). *Shein, Temu, and Chinese e-commerce: Data risks, sourcing violations, and trade loopholes* (Issue Brief). US-China Economic and Security Review Commission. [https://www.uscc.gov/sites/default/files/2023-04/Issue\\_Brief-Shein\\_Temu\\_and\\_Chinese\\_E-Commerce.pdf](https://www.uscc.gov/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf)
- Kazinform. (2023, August 23). Digital Silk Way will connect Asia and Europe along the bottom of the Caspian Sea. *Kazinform*. <https://www.inform.kz/ru/silk-way-i>

- [cgtn-mezhdunarodniy-teleproekt-budet-pokazan-v-kazahstane-i-kitae-66b54b](#)
- Kuschanova, K. (2025, June 17). Kazakhstan is interested in joint AI projects with China. *Kazinform*.
- Law of the Republic of Kazakhstan No. 18-VIII ZRK. (2023, July 10). *About online platforms and online advertising*. <https://www.inform.kz/ru/kazahstan-zainteresovan-v-sovmestnih-proektah-s-kitaem-v-sfere-ii-tokaev-753e05>
- Liu, Y., & Avdokushin, E. F. (2019). Formirovanie osnov 'Tsifrovogo Shelkovogo Puti' [Formation of the foundations of the 'Digital Silk Road']. *The World of the New Economy*, 13(3), 62–71. <https://cyberleninka.ru/article/n/formirovanie-osnov-tsifrovogo-shelkovogo-puti/viewer>
- Makulbekov, M. (2025, June 16). Silk Way and CGTN: International TV project to air in Kazakhstan and China. *Kazinform*.
- News Central Asia. (2025, June 18). Report—Second China-Central Asia Summit. *News Central Asia*. <https://www.newscentralasia.net/2025/06/18/otchet-vtoroy-sammit-kitay-tsentralnaya-aziya>
- Nurmamat, M. (2025, February 5). Belt and robot: Chinese start-up to open first robotics facility in Central Asia. *South China Morning Post*. <https://www.scmp.com/economy/china-economy/article/3297469/belt-and-robot-chinese-start-open-first-robotics-facility-central-asia>
- Order of the Acting Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan No. 8/HK. (2025, January 13). <https://adilet.zan.kz/rus/docs/V2500035656#z6>
- Orisbay, J. (2025, February 27). Astana's video surveillance system will be modernized with the introduction of AI. *Azattyq.kz*. <https://rus.azattyq.org/a/sistemu-videonablyudeniya-v-astane-obeschayut-modernizirovat-vnedriv-ii-est-li-v-etom-riski-33330110.html>
- Profit Online. (2025, February 14). Temu—On topic or not? *Profit Online*.
- Profit Online. (2022, May 25). TikTok launches 'Learn on TikTok Kazakhstan' initiative. *Profit Online*. <https://profit.kz/news/62589/TikTok-zapuskaet-inicativu-UchisvTikTokKazakhstan>
- Resolution of the Government of the Republic of Kazakhstan No. 119. (2019, March 19). <https://adilet.zan.kz/rus/docs/P1900000119>
- Shashkina, A. (2025, August 11). The Kazakh government will switch to a national messenger. *Tengrinews.kz*. [https://tengrinews.kz/kazakhstan\\_news/pravitelstvo-kazahstana-pereydt-na-natsionalnyiy-messendjer-577785/](https://tengrinews.kz/kazakhstan_news/pravitelstvo-kazahstana-pereydt-na-natsionalnyiy-messendjer-577785/)
- Syzdykbayev, A. (2024, October 3). A deputy has demanded that TikTok be blocked in Kazakhstan. *Tengrinews.kz*. [https://tengrinews.kz/kazakhstan\\_news/zablokirovat-tiktok-v-kazahstane-potreboval-deputat-549804/](https://tengrinews.kz/kazakhstan_news/zablokirovat-tiktok-v-kazahstane-potreboval-deputat-549804/)

- Television and Radio Complex of the Presidential Administration of the Republic of Kazakhstan. (2024, July 1). Silk Way TV and China Global Television Network (CGTN) have launched a joint project. *Presidential Administration*.
- Temu. (n.d.-a). *Website of Temu marketplace*. <https://temu.com.kz/>
- Temu. (n.d.-b). *Privacy policy of Temu marketplace*. <https://project5662217.tilda.ws/privacypolicy>
- Tengrinews.kz. (2025, January 20). Which countries have banned TikTok? *Tengrinews.kz*. <https://tengrinews.kz/curious/kakie-stranyi-zapretili-ispolzovat-tiktok-560150/>
- Tengrinews.kz. (2021, November 3). New directions for digital development offered by Huawei in Kazakhstan. *Tengrinews.kz*. <https://tengrinews.kz/conference/novye-napravleniia-cifrovogo-razvitiia-kotorye-predlagaet-415/>
- TikTok. (2025, July 17). TikTok Community Safety: The platform removed 1.4 million videos in Kazakhstan in the first quarter of 2025. *TikTok*. <https://newsroom.tiktok.com/tiktok-removed-more-then-million-videos-in-kazakhstan-in-q-1-2025?lang=ru-KZ>
- Tribune.kz. (2025, July 17). What mobile apps did Kazakhstanis install in the first quarter of 2025. *Tribune.kz*. <https://tribune.kz/kakie-mobilnye-prilozheniya-ustanavlivali-kazahstantsy-v-i-kvartale-2025-goda>
- Tsvetkova, N. N. (2019). Regional integration projects and new technologies: Digital Silk Road. *Eastern Analytics*(1). <https://cyberleninka.ru/article/n/proekty-regionalnoy-integratsii-i-novye-tehnologii-tsifrovoy-shelkovyy-put/viewer>
- United Nations. (2024). *UN e-government survey 2024: Accelerating digital transformation for sustainable development*. <https://desapublications.un.org/sites/default/files/publications/2024-09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf>
- Vaal, T. (2024, December 13). More than 7,800 cameras with facial recognition functionality will be installed in Almaty by the end of 2025. *Vlast Media Portal*. <https://vlast.kz/novosti/63077-bolee-78-tys-kamer-s-funkciej-raspoznavali-lic-ustanovat-v-almaty-do-konca-2025-goda.html>
- Welch, D. (2025, June 5). *Russia and China in Central Asia's technology stack: An analysis of Kazakhstan, Kyrgyzstan and Uzbekistan*. <https://www.gmfus.org/news/russia-and-china-central-asias-technology-stack>
- Whols. (n.d.). *Whois record for Temu.com.kz*. <https://whois.domaintools.com/temu.com.kz>
- Wong, J. (n.d.). *The Silk Road reimagined: Connecting Hong Kong and Kazakhstan's tech ecosystems*. Astana Hub. <https://mobile.astanahub.com/en/blog/the-silk-road-reimagined-connecting-hong-kong-and-kazakhstan-s-tech-ecosystems>
- Xinhua News Agency. (2022, June 22). The China-Central Asia News Agency Forum was held in Astana. *Xinhua*.

- <https://russian.news.cn/20250622/386c02747b53473898765b2688d826e0/c.html>
- Xinhua News Agency. (2025, June 18). Astana Declaration of the Second Central Asia-China Summit. *Xinhua*. <https://russian.news.cn/20250618/e9057e91c41a4c2f99c4c4b17a7a2b79/c.html>
- Xinhua News [@xinhua]. (n.d.). *Facebook account*. Facebook. <https://www.facebook.com/xinhuanewsruusia>
- Zakon.kz. (2025, July 22). Beeline and Huawei: A partnership that speeds up mobile communications in Almaty—Speeds increased by over 40%. *Zakon.kz*. <https://www.zakon.kz/tekhnno/6484948-Beeline-i-Huawei-partnerstvo-kotoroe-uskoryaet-mobilnuyu-svyaz-v-almaty--rost-skorosti-bolee-chem-na-40.html>
- Zhang, W. (2021a). Prospects for Chinese-Kazakh economic cooperation in the post-Covid period. *Problems of Modern Economy*(3), 139–142. <https://www.m-economy.ru/art.php?nArtId=7166>
- Zhang, W., Selishcheva, T. A., & Dyatlov, S. A. (2021). The Digital Silk Road as a form of conjugation of the Eurasian Economic Union and the One Belt, One Road Project. *Problems of Modern Economy*(1), 14–20. <https://www.m-economy.ru/art.php?nArtId=7035>

## **Analytical report: Technological and Digital Cooperation between China and Central Asia: Opportunities, Challenges and Trends**

Aida Kumarbayeva, Nazarbayev University

### **Abstract**

*This report examines the scope, dynamics, and implications of technological and digital cooperation between China and Central Asian states, with a particular focus on Kazakhstan, Uzbekistan, and Kyrgyzstan. Framed within the development of China's Digital Silk Road under the Belt and Road Initiative, the study explores how digital partnerships have expanded across key sectors, including telecommunications infrastructure, e-governance, smart city systems, and emerging technologies such as artificial intelligence.*

*Adopting a qualitative methodology combining documentary analysis, content analysis, and comparative case studies, the research identifies both the opportunities and challenges associated with this cooperation. On the one hand, Chinese investments and technologies provide Central Asian countries with cost-effective solutions to accelerate digital transformation, enhance connectivity, and modernize governance. On the other hand, these partnerships raise significant concerns related to data security, technological dependency, regulatory capacity, and digital sovereignty.*

*The findings highlight uneven levels of digital development across the region, with Kazakhstan emerging as a frontrunner, Uzbekistan demonstrating rapid advancement alongside growing reliance on Chinese infrastructure, and Kyrgyzstan progressing more gradually. The report concludes that while digital cooperation offers substantial developmental benefits, its long-term sustainability will depend on the ability of Central Asian states to strengthen institutional frameworks, diversify technological partnerships, and ensure that digital transformation aligns with broader societal and governance objectives.*

## **Preface**

### **Acknowledgements**

My sincere gratitude to Central Asian Policy Studies for providing the grant opportunity and dissemination platform that enabled the successful completion and publication of this report. I also extend special thanks to Research Associate Oyuna Baldakova for sharing her expert insights on the topic.

### **Methodology**

This study will adopt a qualitative research approach to explore the nature, scope, and implications of technological and digital cooperation between China and Central Asian countries. It will rely on documentary analysis of official policy papers, cooperation agreements, national digital strategies, and reports.

To examine the narratives, priorities, and framing of cooperation, the research will employ content analysis of media reports, speeches, and public communications.

Additionally, a comparative case study method will be used to analyze Kazakhstan, Uzbekistan and Kyrgyzstan as primary examples, given their more advanced digital engagements with China.

To evaluate the impact of cooperation, the study will apply a result-chain model, linking inputs to outputs, outcomes, and potential long-term impacts.

The study will also incorporate a semi-structured interview with an expert in the field of digital cooperation between China and Central Asia. This interview will provide valuable, in-depth insights into the motivations, challenges, and perspectives surrounding technological and digital cooperation, complementing the documentary and media analyses.

## **Introduction**

In recent years, Chinese technology has made significant inroads into digital and technological sectors throughout Central Asia. The launch of the Belt and Road Initiative (BRI) by President Xi Jinping in 2013 marked a pivotal moment in the relationship between China and Central Asia. In 2015, the Digital Silk Road (DSR) was introduced as a vital component of the BRI, emphasizing the development of a shared digital future.

Central Asian countries, including Kazakhstan, Kyrgyzstan, and Uzbekistan, have increasingly relied on Chinese ICT companies to build extensive digital infrastructure projects, such as Safe City initiatives that use facial recognition, biometric technologies, and centralized management systems. At the same time, these governments have launched national digitalization strategies aimed at modernizing their economies and improving governance frameworks. Notable examples are Kazakhstan's 2023-2029 digital transformation strategy, Uzbekistan's "Digital Uzbekistan 2030," and Kyrgyzstan's "Digital Kyrgyzstan 2024-2028" program. These efforts, alongside China's growing digital influence, provide



a crucial context for investigating the interplay of technology, governance, and international cooperation in Central Asia.

This research aims to investigate the scope, dynamics, and impacts of technological and digital collaboration between China and Central Asian states. The specific objectives are to identify key areas of digital and technological partnership and analyze the motivating opportunities and challenges of such cooperation.

## **Literature Review**

The advancing technological and digital collaboration between China and Central Asia has increasingly become a focus of academic research, highlighting a multifaceted relationship influenced by economic, political, and security considerations. Researchers stress the intricate nature of this dynamic and explore how China's strategic digital goals align with the needs and developmental challenges of Central Asian countries.

A key element of China's digital involvement in the region is the Digital Silk Road (DSR), which forms part of the wider Belt and Road Initiative (BRI). Yang and Jiang (2015) identify the roots of the DSR in China's awareness of the economic and political opportunities presented by the digital domain. Expanding on this, Ly (2020) contends that the DSR embodies China's goal to influence global technological standards, especially in fields like 5G, artificial intelligence (AI), and e-commerce platforms.

Building on these theoretical discussions, empirical studies provide insights into the goals and execution of the Digital Silk Road (DSR). The World Bank (2020) notes that the DSR aims to expand broadband access, implement 5G technology, update broadcasting infrastructure, and develop large-scale data centers. These initiatives are designed to strengthen regional digital capabilities and promote synchronized digital development strategies. Knight (2014) supports this perspective by highlighting the DSR's potential to reduce economic inequalities and stimulate growth. He suggests that creating an integrated digital ecosystem could help Central Asian nations resolve conflicts and establish conditions conducive to economic collaboration. However, he warns that realizing this potential requires coordinated, people-focused planning that develops digital skills and guarantees fair access.

Other researchers emphasize the political and security aspects of digital collaboration. Sukhanin (2021) examines the bilateral ties between China and Central Asian countries, especially Kazakhstan and Uzbekistan, concentrating on surveillance technologies and cybersecurity. His study highlights the political and security implications of digital cooperation, drawing attention to the crucial role played by Chinese ICT companies in extending China's digital presence throughout the region.

Complementing the security-focused viewpoint, other studies emphasize digitalization's potential to promote regional collaboration. Kassenova and Duprey (2021) view digital technologies as instruments to strengthen multilateral efforts addressing cross-border issues like climate change and migration. This aligns with Gabarró (2020), who supports establishing a common digital space in Central Asia through institutional, legal, regulatory, and investment measures. He highlights the crucial role of public-private partnerships, shared infrastructure, and international cooperation in bridging connectivity gaps and enhancing overall welfare.

From a developmental perspective, the conceptual shift from digitalization to digital transformation is essential to understanding the trajectory of China–Central Asia cooperation. While digitalization has focused on improving business operations, digital transformation represents a broader paradigm characterized by disruptive technologies such as AI, the Internet of Things (IoT), and expansive digital networks.

The region is presently in the initial phase of this digital transformation. According to Zakiyeva (2021), Central Asian nations vary in their speed of digital progress, with Kazakhstan standing out as a regional frontrunner, while countries like Kyrgyzstan and Uzbekistan continue to develop their basic digital infrastructure. Disruptive technologies are altering competitiveness, governance, and economic development, and the extent to which states can capitalize on these changes depends not only on infrastructure but also on institutional capabilities and the quality of human capital.

The COVID-19 pandemic has further accelerated this transition, opening up new areas for cooperation. Liyun (2022) observes that collaboration has expanded beyond economic and energy sectors to include digital health, epidemic control, the mutual recognition of health codes, and joint public health research. Similarly, the International Monetary Fund and World Bank emphasize that regional integration through shared digital platforms and cross-border data sharing is essential for tackling global challenges and promoting sustainable development. Tazhiyev (2021) highlights that these approaches could help Central Asian countries overcome stagnation and advance in economic, political, and sociocultural fields by enabling more intelligent governance and improved service delivery.

Building on emerging trends, Rezapour (2025) offers important perspectives on China's comprehensive digital strategy, especially regarding artificial intelligence (AI). She points out China's goal to achieve global leadership by combining AI with other transformative technologies and integrating them into its overseas investments. Zakiyeva (2021) emphasizes that improving digital connectivity is essential for boosting competitiveness and fostering inclusive growth. The Digital Silk Road's five strategic objectives—resolving industrial overcapacity, supporting the global expansion of Chinese technology companies, promoting the



international use of the renminbi, developing China-centered infrastructure, and advancing globalization driven by cyberspace—illustrate China's broader ambitions to lead global digital development. Cheney (2019) further highlights this cooperation as not only a diplomatic instrument but also a domestic strategy for China to secure its status as a top technological power.

China's increasing focus on digital partnerships mirrors its broader industrial shift. Tukumov (2023) points to the alignment between Chinese investments and global trends in AI, electric vehicles, and mobile technologies. He observes that domestic industrial growth, fueled by supportive policies and tax incentives, has strengthened China's international role, especially through high-tech exports like AI-powered solutions and vehicles gaining global traction.

However, the implementation of digital transformation strategies in the region is not without tension. The DSR is expected to manifest differently across national contexts, depending on infrastructure, political will, and existing digital ecosystems (Radjabovich 2025). Understanding the DSR, therefore, requires a nuanced analysis of how Chinese investments intersect with local needs, regulatory frameworks, and development priorities.

Concerns about data governance and state surveillance further complicate this picture. Bokhoronov and Bekturganov (2023) examine Chinese technology companies in Kazakhstan and Uzbekistan, highlighting risks arising from these firms' access to sensitive user data and questioning the regulatory capacity of host countries. Their findings underscore the need for stronger oversight at national, regional, and international levels to safeguard privacy and uphold digital rights.

These concerns resonate with Gussarova's (2021) critique of Kazakhstan's digitalization strategy. She argues that it places disproportionate emphasis on ICT performance metrics—such as e-government indices and Smart City rankings—while neglecting societal, cultural, and ethical dimensions of transformation. Moreover, Kazakhstan's reliance on foreign technology and expertise, particularly from China, limits its autonomy in shaping long-term digital policies aligned with public interests.

At the governance level, Yang and Ping (2021) emphasize that for the DSR to advance effectively, China and Kazakhstan must jointly establish standards in areas such as e-commerce payments, customs electronic ports, tax regulation, and data flow security. Yet both countries still lack clear and unified coordination mechanisms in these domains, which creates obstacles to cross-border trade and investment. Liyun (2022) similarly observes that the pace of regulatory development in the digital economy lags behind the rapid globalization of digital activities, creating a structural imbalance between technological innovation and institutional adaptation.

Finally, Gao (2022) cautions that while the DSR holds considerable promise, it must navigate the contested terrain of digital geopolitics, where issues of data privacy, technological sovereignty, and dependence on China remain unresolved.

Taken together, the scholarly debate underscores that the trajectory of China–Central Asia digital cooperation will hinge not only on infrastructure investments and market expansion but also on the ability of both sides to develop robust institutional frameworks, safeguard digital rights, and ensure that digital transformation serves broader developmental and societal goals.

### **Institutional, legal, and capacity readiness prerequisites for digital and technological cooperation in central Asia**

The growing emphasis on the digitalization of national economies and public administration systems in Central Asian countries has created a strategic opportunity for China to strengthen its position within these markets. This development aligns closely with Beijing’s broader geopolitical and economic ambitions, particularly in securing roles for Chinese technology companies in the region. Xi Jinping, China’s current leader, had already begun articulating these priorities when he launched the Belt and Road Initiative (BRI) at Nazarbayev University in Astana, Kazakhstan, in September 2013 (Vlast.kz 2023).

Within this broader framework, the Digital Silk Road (DSR) emerged in 2015 as the BRI’s dedicated digital component (International Institute for Strategic Studies 2022). Officially introduced by Xi Jinping at the first Belt and Road Forum in 2017, the DSR was presented as a cooperative platform designed to advance digital infrastructure, encompassing big data technologies, cloud computing, cross-border e-commerce, and smart city projects. The initiative has been welcomed by Central Asian leaders, many of whom view it as a source of essential investment for upgrading digital capabilities and modernizing information technology sectors. Over the last decade, governments in the region have introduced ambitious national strategies to accelerate digital transformation. Kazakhstan’s first major digitalization plan, Information Kazakhstan, was launched in 2013, followed by the more comprehensive “Digital Kazakhstan” initiative in 2018. Kyrgyzstan adopted its Digital Transformation plan in 2019, while Uzbekistan unveiled its national digital strategy, “Digital Uzbekistan – 2030,” in 2020. These programs have contributed to significant increases in internet penetration and mobile connectivity, while also laying the foundation for diversified, technology-driven economies. They envision the deployment of advanced technologies such as fifth generation (5G) telecommunications networks and artificial intelligence (AI) to support smart applications in sectors ranging from e-commerce and logistics to public services. In urban centers such as Almaty, Bishkek, and Tashkent, an emerging ecosystem of startups—particularly in Fintech, Edtech, and Healthtech—is benefiting from government-backed innovation hubs, incubation centers, and targeted entrepreneurship support programs (Bokhoronov, Bekturganov 2023).

Kazakhstan’s digital transformation agenda has recently been codified in the “Concept of Digital Transformation, Development of the Information and

Communication Technology Industry, and Cybersecurity for 2023–2029,” approved by the government on March 28, 2023. This strategic document sets out the vision, guiding principles, and target metrics for advancing digitalization, expanding the ICT industry, and strengthening cybersecurity. (Adilet 2023).

Kazakhstan’s approach to digital development is underpinned by a comprehensive legislative framework. Key laws include the Law “On Informatization,” (Adilet 2015) the Law “On Personal Data and Their Protection, (Adilet 2013), and the Law “On Fingerprint and Genomic Registration. (Adilet 2016). The Law on Personal Data, enacted in 2013 and modeled closely on the European Union’s General Data Protection Regulation (GDPR), grants individuals a range of privacy rights. A 2016 amendment (Adilet 2016) introduced strict data localization provisions, requiring that databases containing personal data of Kazakh citizens be stored on servers physically located within the country. Similarly, the Law on Informatization (2015) mandates that personal data processing be carried out domestically.

Concerns around data privacy, surveillance, and information security have become increasingly salient in Kazakhstan’s digital transformation discourse. Public debate has grown more active around issues of potential government overreach, censorship, and the balance between national security and individual rights. Recognizing these sensitivities, on March 20, 2023, the President signed a decree approving the Information Doctrine, which sets out a framework for developing the information sphere in ways that enhance transparency, foster competitiveness, and promote content security (Akorda 2023).

In Uzbekistan, the “Digital Uzbekistan – 2030” Strategy forms part of the broader “New Uzbekistan” development agenda. This strategy seeks to accelerate the country’s digital transformation by expanding high-speed broadband coverage, developing a robust national digital services ecosystem, and integrating ICT solutions into both public and private sectors. Key priorities include fostering innovation, supporting digital entrepreneurship, and modernizing governance systems to improve transparency and efficiency. The Uzbek government has placed particular emphasis on e-government initiatives, which aim to streamline public administration and improve citizens’ access to government services (Strategy.uz 2023).

A Presidential Decree has set the “Digital Government” and “Digital Region” programs for 2023–2024 in motion. These programs comprise 300 major projects: 112 aimed at digitizing public administration processes, 51 targeting digitalization in industrial sectors, and 137 dedicated to advancing regional digital transformation (Khakimov 2024).

Uzbekistan’s digitalization is supported by key laws and regulations, including the 2019 Law “On Personal Data” (cis-legislation 2019) with 2021 data localization requirements, Cabinet Resolution No. 570 (2022) on personal data processing, Presidential Decree UP-76 (2023) setting digital development priorities like e-

government and AI, and Resolution PP-162 (2023) focused on expanding digital services and infrastructure. Together, these create a solid legal and strategic foundation for Uzbekistan's digital transformation (DLA Piper 2025).

Kyrgyzstan's path to digitalization is guided by long-term strategic visions, including the National Development Strategy for 2018–2040 and the Concept of Digital Transformation "Digital Kyrgyzstan 2024–2028." These documents outline a national commitment to integrating digital technologies into economic and social systems, with a focus on expanding ICT infrastructure, optimizing state administrative processes, and fostering an enabling environment for digital entrepreneurship. The government's policy seeks to ensure that the benefits of technological progress extend to citizens and businesses alike, promoting inclusive growth and reducing the digital divide (Digitalgov.kg 2024).

From a legal standpoint, Kyrgyzstan's Law on Personal Data, enacted in 2008, stipulates that state consent must be obtained before personal data is collected, while corporations must secure state approval before transferring such data abroad. Transfers are prohibited to countries that do not provide an "adequate level of protection," although the law does not clearly define the criteria for adequacy. This creates some uncertainty for cross-border data flows, potentially complicating international business operations and cloud service provision (DLA Piper 2025).

Taken together, the digitalization strategies of Kazakhstan, Uzbekistan, and Kyrgyzstan illustrate a common regional trajectory toward deeper integration of digital technologies in governance, commerce, and daily life. While each country has tailored its policies to its specific political and economic contexts, all three are investing heavily in infrastructure, regulatory frameworks, and human capital to position themselves as competitive players in the global digital economy. The Digital Silk Road offers a platform for these ambitions to intersect with China's technological outreach, fostering both opportunities and challenges.

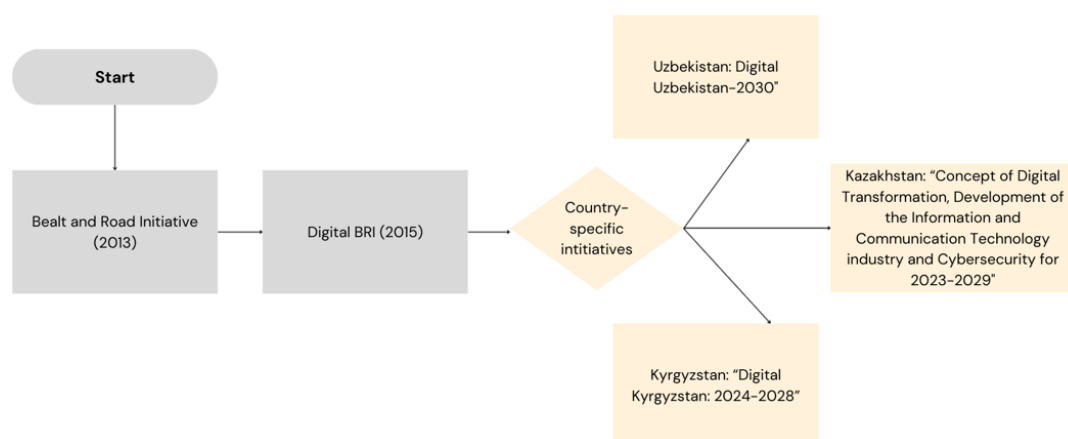


Figure 1 – Digital Silk Road: From BRI to National Strategies in Central Asia  
Source: Compiled by the author

Building on the legislative and institutional foundations, the level of digital development in Central Asia can be further illustrated through international indexes. The UN E-Government Development Index, which includes several key components, highlights the progress achieved by Kazakhstan, Uzbekistan, and Kyrgyzstan in comparison with global and regional benchmarks. In terms of the Telecommunication Infrastructure Index, Kazakhstan performs strongest with a score of 0.9235, significantly above both the Asian average of 0.7740 and the global average of 0.6896. Kyrgyzstan (0.8815) and Uzbekistan (0.8769) also surpass these averages, though they remain slightly behind Kazakhstan, pointing to remaining challenges in areas such as broadband penetration and equitable digital access (World Bank 2024).

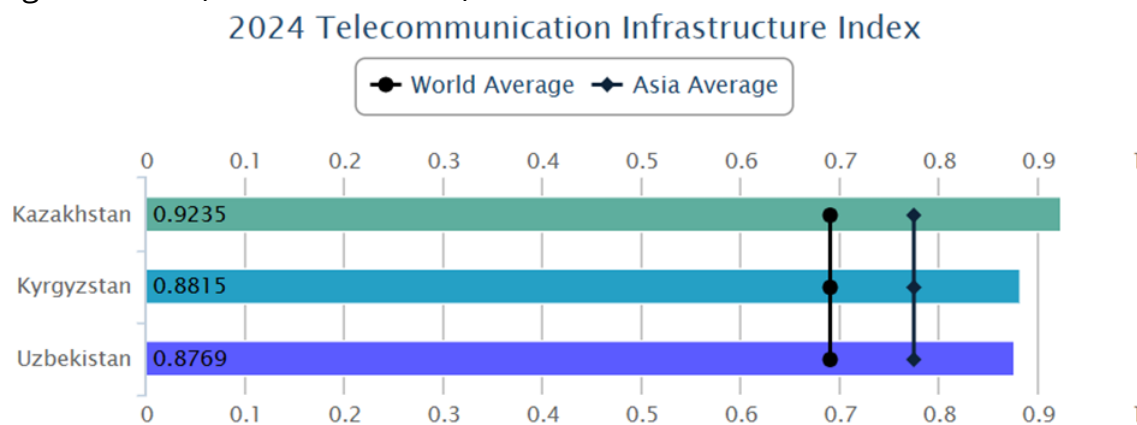


Figure 2 – Telecommunication Infrastructure Index (World Bank, 2024)

Kazakhstan again takes the lead in the Technology Index, scoring 0.7500, which is well above both the world average of 0.55 and the Asian average of 0.60. This strong performance reflects a more advanced adoption of emerging technologies, higher R&D capabilities, and a more vibrant innovation ecosystem. Uzbekistan follows with 0.6875, also above global and regional averages, underscoring steady progress in digital adoption, startup development, and joint research platforms. Kyrgyzstan, however, trails at 0.5625, only slightly above the global average but falling short of the Asian benchmark, indicating the need for stronger investment in technological infrastructure and innovation capacity (World Bank 2024).

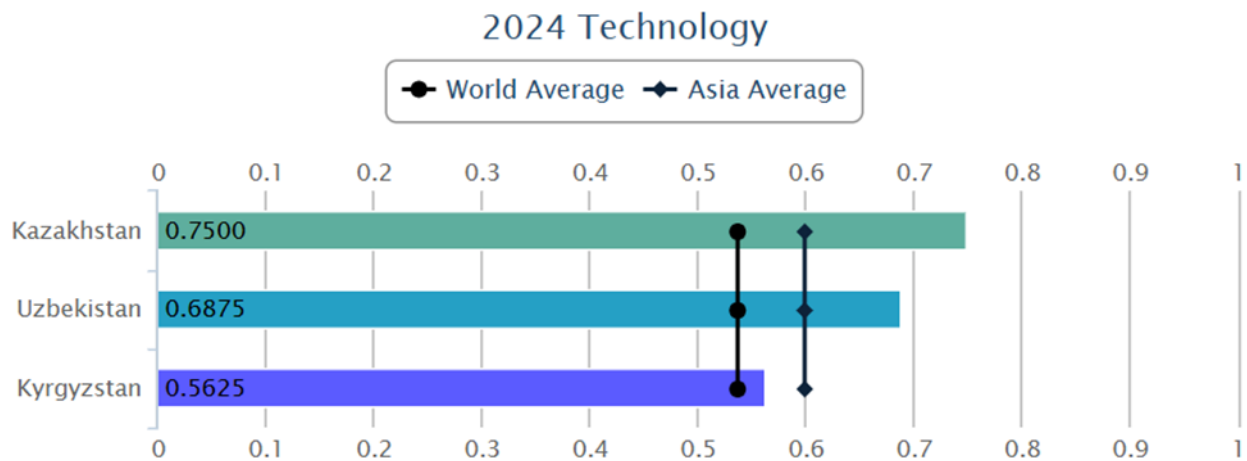


Figure 3 – Technology index (World Bank, 2024)

In the Institutional Development Index, Kazakhstan achieves a perfect score of 1.0000, the highest possible, which highlights the country's robust policies, governance structures, and comprehensive regulatory support for digital transformation. Uzbekistan and Kyrgyzstan both score 0.9200, performing strongly and surpassing global and Asian averages. These results demonstrate significant progress in developing institutional and legal frameworks for ICT and e-government across the region (World Bank 2024).

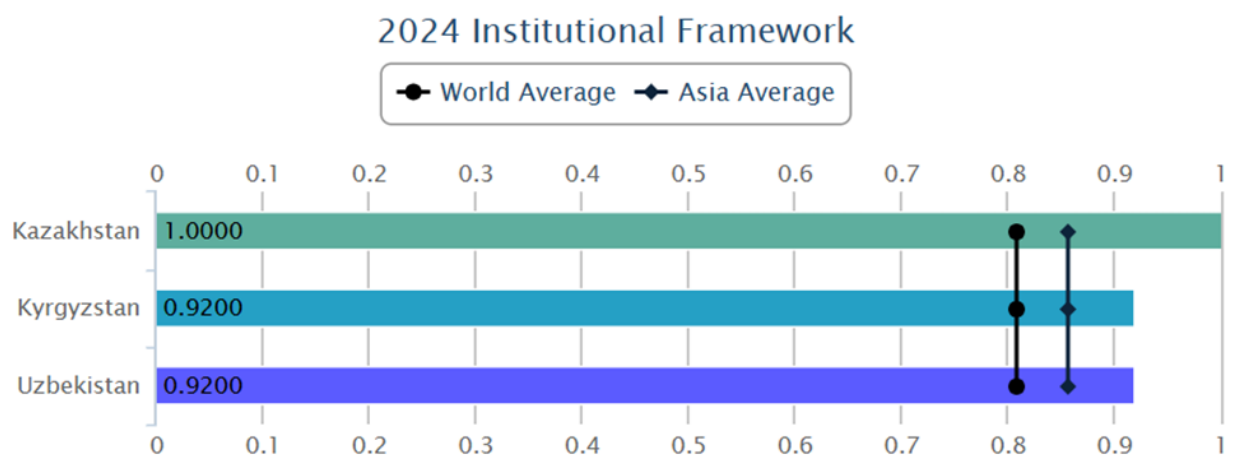


Figure 4 – Institutional Framework Index (World Bank, 2024)

Additional international benchmarks confirm Kazakhstan's leading position in digital development. The International Telecommunication Union's ICT Development Index assigns Kazakhstan a score of 90, followed by Uzbekistan at 86.5 and Kyrgyzstan at 85.9, suggesting a relatively high level of ICT adoption across all three countries (ICT Development Index 2025). Huawei's Global Digitalization Index places Kazakhstan in 58th position with a score of 33.2, while Uzbekistan ranks 60th with 32.7; Kyrgyzstan is not included in this index (HGDI 2024). Meanwhile, in the IMD World Digital Competitiveness Ranking 2024,



Kazakhstan is ranked 34th out of 67 countries, whereas Uzbekistan and Kyrgyzstan are not represented (IMD 2024).

These comparative findings show that Kazakhstan consistently leads the region in digital development, establishing itself as the digital frontrunner. Meanwhile, Uzbekistan is closing the gap by implementing focused reforms, and although Kyrgyzstan remains behind, it is steadily enhancing its digital capabilities.

### **China-Central Asia digital and technological cooperation: Case studies of Kazakhstan, Uzbekistan and Kyrgyzstan**

China and Central Asian states, particularly Kazakhstan, Uzbekistan, and Kyrgyzstan, have significantly expanded cooperation in digitalization and advanced technologies in recent years, creating a complex web of institutional agreements, corporate partnerships, and infrastructure projects that tie the region's digital future increasingly to Chinese technology. This collaboration has unfolded simultaneously at government-to-government, corporate, and societal levels, blending strategic ambitions with commercial interests, and reflecting broader geopolitical dynamics under the Digital Silk Road framework.

The digital and technological cooperation is a broad concept itself that requires clarification and classification. The analysis shows that the direction of the digital can be classified as digital infrastructure and connectivity, cooperation in e-governance and cloud system development, cooperation in smart city and surveillance systems development, innovation, research and education, as well as cooperation in capacity building and skills training.

Kazakhstan has been at the forefront of these trends, signing a series of memoranda and framework agreements that illustrate the scope of its cooperation with China. For example, a Memorandum of Cooperation between Kazakhstan's Ministry of Digital Development, Innovation, and Aerospace Industry and China's Ministry of Industry and Information Technology underscores both sides' shared commitment to advancing digital infrastructure and industrial technologies. Complementing this, the same Kazakh ministry signed a memorandum with the China International Development Cooperation Agency to promote high-technology projects, further institutionalizing bilateral collaboration in innovation. Financial and regulatory dimensions have deepened as well: the National Bank of Kazakhstan and the People's Bank of China concluded a memorandum of understanding on digital currency, highlighting interest in financial digitalization and cross-border fintech integration. At the same time, a memorandum between the Bureau of National Statistics of Kazakhstan and the National Bureau of Statistics of China established a framework for cooperation in statistical data exchange and digital governance of information systems.

The corporate sector reflects similar momentum. For instance, Samruk-Kazyna JSC and Huawei Technologies Kazakhstan signed a memorandum on digital transformation, telecommunication infrastructure development, and ICT



deployment, while the Akimat of Astana partnered with Huawei on a pilot project to deploy a 10G network using 50G PON technology. Huawei's central role in Kazakhstan's digital ecosystem is further evidenced by its participation in higher education and science: the Al-Farabi Kazakh National University and Northwestern Polytechnical University (China) signed a memorandum to establish a joint satellite ground station with \$300,000 of investment. In the commercial sphere, ALATAYALTYN JSC and UnionTech Software Technology Co., Ltd. created a joint venture through a framework agreement, while ALATAYALTYN also joined the Committee on Digital Economy and Digital Trade of the China WTO Society (CWTO) to launch a joint digital platform for smart city initiatives in both countries (Inform 2025).

At the political level, Kazakhstan has consistently stressed the strategic importance of digital cooperation with China. For example, during his 2023 Xi'an visit, President Tokayev met with Huawei President Liang Hua, after which Huawei announced investments in broadband research and plans to position Kazakhstan as a regional digital hub. Cooperation with KTJ to accelerate railway digitalization was also emphasized. Huawei now operates in Kazakhstan through all three of its global divisions—Carrier, Consumer, and Enterprise—and its involvement spans major initiatives such as Digital Kazakhstan, Safe City, and Smart Home, as well as LTE and 5G rollout (Global Times 2023). In 2022, Kazakhstan's Ministry of Digital Development signed an MoU with Huawei during the Digital Bridge Forum to establish a digital hub for advanced technologies. Huawei has participated in over 250 Digital Kazakhstan projects, including broadband expansion with more than 1,000 base stations. Dahua Technology, which opened a Kazakhstan office in 2017, has similarly broadened its focus beyond surveillance into IoT and networking, contributing to nationwide projects such as Sergek, developed with Korkem Telecom (Bokhoronov, 2023).

The central element of partnership between China and Kazakhstan lies in physical connectivity. Kazakhstan maintains terrestrial fiber-optic links to China through border crossings at Altynkol and Zharkent near Khorgos, with another at Dostyk, where a new rail connection is scheduled for completion by the end of 2025 (RailFreight.com 2018). These terrestrial links are reinforced by Chinese corporate projects, most notably Huawei's contract to implement "smart railways" for Kazakhstan Temir Zholy (KTJ), including modern fiber-optic infrastructure that enables Kazakhstan's railways to adopt advanced digital solutions (Huawei.com 2025). The importance of cooperation reached a new level during the Fifth China–Central Asia Foreign Ministers' Meeting in Chengdu in 2024, where Kazakhstan pledged to expand cooperation in highways, railways, aviation, shipping, ports, logistics, multimodal transport, and optical cable deployment (NewCentralAsia 2024).

Another sphere of cooperation between Kazakhstan and China is telecommunication. Transtelecom JSC has partnered with Chinese enterprises to

modernize networks and deploy solutions such as SD-WAN (RailNews 2024). All three major Kazakh telecom operators rely heavily on Chinese suppliers. Since the early 2000s, Huawei has assisted in LTE deployment and rural wireless access, with its infrastructure forming the backbone of peripheral access networks (Welch 2025).

Beyond telecommunications, Chinese companies have shaped Kazakhstan's cloud and data infrastructure. Huawei dominates in storage and cloud services for the national railway, while Lenovo provides solutions for government institutions and financial entities. In 2019, Inspur Weihai Overseas Service signed an agreement with Kazakhstan National Railways Telecommunications Company to jointly develop data centers under the Digital Kazakhstan initiative (Welch 2025). Lenovo has highlighted its role in cooperation with cloud providers and open data storage center, while signaling further investment (Trend.az 2023). Huawei, meanwhile, emphasizes cloud and data infrastructure as a strategic priority, showcasing its CloudEngine switches and iMaster NCE platforms for intelligent network management (Bokhoronov, Bekturganov 2023).

PRC firms are likewise central to Kazakhstan's smart city and surveillance initiatives. Safe City programs integrate IoT and AI systems to enhance traffic management and crime prevention but raise concerns over espionage, data security, and technological dependence. Kazakhstan's first pilot was launched in Aqkol in 2019 (Astanatimes 2019), using Dahua and Hikvision cameras supplied under the Digital Silk Road. Sergek, the country's leading smart city provider, has publicly acknowledged reliance on Dahua hardware (CivicIdeas 2022).

In the technological sector, Kazakhstan and China have strengthened their partnership through a series of strategic agreements in energy, technology, and infrastructure. These include PowerChina's plans to localize technologies, create a research and development center, and establish a decarbonization fund; China Southern Power Grid's cooperation with Kazakh partners on HVDC transmission, digital energy, and pumped-hydro storage; QazaqGaz's financing deal with China Construction Bank to expand national gas infrastructure; and Sinopec's technological partnership with Kazakhstan to advance petrochemical processing and develop high-value products (AstanaTimes 2025).

Kazakhstan's ambitions were further highlighted at the "Digital Silk Road – 2025" forum, which also underscored growing interest in tourism digitalization. In June 2024, Kazakh Tourism signed a memorandum with the Chinese platform Zowoyoo to promote Kazakhstan's tourism potential in China, allowing local operators, hotels, and cultural facilities to showcase their services not only on Zowoyoo but also across Douyin and Xiaohongshu (Kazakhtourism 2025).

The July 2025 launch of the Khan Tengri Innovation Hub in Shanghai's Zhangjiang Hi-Tech Park marked a significant development, representing the first specialized platform designed to integrate the technological potential of Central Eurasian countries with China's innovation ecosystem. Spearheaded by Kazakhstan's

Growth Vision Pro with support from the Ministry of Digital Development, Astana Hub, and Uzbekistan's IT Park, the hub seeks to strengthen cross-border technology transfer in digitalization, high technology, and R&D; enable Central Asian startups to access the Chinese market; and provide Chinese companies with a "soft landing" in Eurasia, Europe, the Middle East, and North Africa via the Middle Corridor. The hub also promotes joint R&D projects, venture capital flows, and greater awareness of Central Eurasia within China (gov.kz 2025).

If Kazakhstan represents a hub for regional digital integration, Uzbekistan illustrates high level of dependency on Chinese digital infrastructure. Reports revealed that China was the top foreign investor in Uzbekistan in 2024, contributing 27.9 percent of total foreign investments and loans (Belt and Road Portal 2025). On October 16, 2023, during the 3rd Belt and Road Forum for International Cooperation in Beijing, Uzbekistan's Ministry of Digital Technologies and China's Ministry of Industry and Information Technology signed a memorandum of cooperation to deepen digital ties. The agreement outlined collaboration in infrastructure interconnection, communication networks, 5G development, cybersecurity, and broader ICT initiatives. In parallel, the Computer Network Information Center (CNIC) and the Central Asia Drug Discovery and Development Center—both under the Chinese Academy of Sciences—formalized a partnership with Uzbekistan's Science and Technology Information Center to establish the Silk Road scientific data community on ScienceDB and the Central Asia node of the Common Science and Technology Resource Identification (CSTR) system. While ScienceDB serves as a global platform for sharing scientific data, CSTR assigns unique identifiers to technology resources, promoting open science and cross-border research collaboration (Tekir 2025).

Key milestones in Uzbekistan-China digital cooperation include the 1999 intergovernmental agreement on post and telecommunications and the 2005 agreement on communications and information technologies. Building on this framework, JSC *Uzbektelecom* signed a series of contracts with major Chinese partners: a 2006 deal with China Telecom on transit and leased channels, a 2015 agreement with China Unicom on international telecommunications services, and recent partnerships in 2023 with Tencent. Additionally, LLC *UZINFOCOM* and H3C Technologies Co. Ltd. issued a Joint Venture Declaration to expand collaboration in ICT (thegulfobserver.com 2025).

Chinese influence is particularly strong in Uzbekistan's surveillance infrastructure through the Safe Cities program. Huawei first piloted a "safe tourism" project in Bukhara, which included a command center, FRT-equipped cameras, an LTE network, and a dedicated data center (uza.uz 2018). This partnership continues with CITIC Group and COSTAR Group started to implement the Safe Cities project in Uzbekistan (Thediplomat 2019). Smart city initiatives further highlight expanding cooperation, as demonstrated by Uzbekistan's 2023 partnership with

China's SuperMap Software Co. Ltd. to launch the GIS Innovation project in Tashkent (SpotUz 2023).

Chinese firms have also engaged with regional authorities on digital systems for transport, energy, and utilities. Meanwhile, international developers have proposed large-scale smart city projects, including a multi-billion-dollar plan integrating governance, healthcare, education, and technology hubs.

E-government initiatives have also been prominent. For instance, project with *Huawei* was completed to establish a data center for the "E-Government" system at a cost of USD 58.4 million (thegulfoobserver.com 2025).

Uzbek–Chinese cooperation has expanded into smart industries and manufacturing. In 2023, China and Uzbekistan signed 41 agreements covering projects such as biotechnology clusters, agro-industrial parks, and PRC-backed electric vehicle (EV) production (President.Uz 2023). Since then, Uzbekistan has attracted significant Chinese investment in pharmaceuticals (daryo.uz 2024), semiconductors, EVs, and hardware, including China's MingYuan technology park in Jizzakh (InterFax 2024) and a microchip facility in Chirchik (InvestInUzbesita 2023).

Transport and logistics digitalization has advanced through PRC partnerships as well. In 2023, China Machinery Engineering Corporation signed an agreement with Uzbekistan's State Committee on Roads to install a "smart highway" system along the A380 corridor (GlobaCtfo 2024).

In terms of cooperation in AI, Shanghai-based AI company LinkWise has teamed up with Uzbekistan's Ministry of Digital Technologies and two Chinese firms to establish a Modular Intelligent Computing Center (MICC) in Central Asia. The project, implemented jointly with China Electronic Technology Development Co. and Shanghai Oriental Credits Industrial Development Co., aims to create a flexible, deployable "AI brain" that will supply the computing power needed to advance Uzbekistan's digital government, smart city initiatives, and industrial modernization (citynewscervice 2025).

Educational cooperation plays a crucial role in shaping the future of both countries, as internationally trained youth form the foundation of long-term development. In 2023, the Tashkent University of Information Technologies (TUIT) named after Muhammad al-Khwarizmi signed memoranda with *Xi'an University*, *Northwestern Polytechnical University*, the *China Institute of Communications*, and *ZTE University* to promote human resource development and academic exchanges. Additionally, together with *Huawei* and *ZTE*, TUIT established a Digital Education Lab and the Huawei Academy of Information and Network Technologies. Within the "Seeds for the Future" program, over 50 students gained internship experience at Huawei's headquarters in China (thegulfoobserver.com 2025).

If Uzbekistan reflects deep technological dependence, Kyrgyzstan's case illustrates a more emerging but still growing reliance on PRC firms. The country's

2024–2028 Digital Transformation Plan prioritizes fiber-optic expansion, integrating deployment with transport, energy, and other infrastructure projects. During the Fifth China–Central Asia Foreign Ministers’ Meeting in Chengdu in December 2024, Kyrgyzstan and China pledged deeper cooperation in connectivity, particularly in transport and optical cable development (fmprc.gov 2024).

Beyond connectivity, Kyrgyzstan has pursued cooperation with China in data infrastructure. In 2023, Kyrgyzstan signed an agreement with the China-based Center for Promotion of the Industrial Internet of the Silk Road (CPIISP), created to advance the Digital Silk Road across SCO member states (qazinform 2023). The agreement includes projects to build data centers, establish a semiconductor fabrication plant, and develop digital government archives and services. These initiatives are further supported by Chinese technology firms already active in Kyrgyzstan, for example China's IZP Technologies to set up trading center in Kyrgyzstan (Chinadaily 2015).

Smart city projects represent another area of Kyrgyz–Chinese cooperation. Since 2018, Kyrgyzstan has explored initiatives with Chinese partners, with Hikvision and Dahua installing extensive camera systems in Bishkek. Shenzhen Sunwin Intelligent Co. also secured a contract to deliver surveillance hardware and software nationwide (24kg 2022).

The scope of collaboration has broadened into technology, investment, and capacity-building. For example, at the 2024 SCO summit in Astana, Xi Jinping and President Sadyr Japarov pledged closer collaboration in biotechnology, e-commerce, manufacturing, and e-governance. In 2025, Kyrgyzstan and China signed a joint statement in Beijing to deepen their comprehensive strategic partnership, outlining cooperation in the digital economy, artificial intelligence, and modernization of judicial information system. While many projects remain at the planning stage, they signal growing collaboration in digital governance and e-commerce (Welch 2025).

Finally, cooperation in technology is supported by training, exchange, and promotional activities. For instance, in 2024, Huawei organized a commercial roadshow in Bishkek that included training on IP networks, data storage, and IT platforms (Huawei 2024).

It should be noted that there is less information available in open sources about digital and technological cooperation between Kyrgyzstan and China.

### **Expert perspectives on opportunities, risks, challenges, and future trends of China-Central Asia digital and technological cooperation**

To assess the opportunities, risks, challenges, and future trends of China–Central Asia digital and technological cooperation, this report incorporates insights from expert interviews and secondary sources.



Research Associate Oyuna Baldakova, the key expert interviewed for this report, emphasized that digital and technological cooperation is an expansive field that demands clear identification of its opportunities and risks. According to her, much depends on the specific level of cooperation and the type of companies engaged - whether they are private firms (like Alibaba) or semi-private firms (like Huawei). She underlined that the main opportunity lies in the development of digitalization at relatively low cost, since China provides affordable technological products and services. This dynamic creates opportunities for Central Asian states to accelerate digital development at a low price.

Despite these opportunities, challenges are evident. Baldakova stressed that data security is one of the most critical concerns: ensuring that data is properly stored, protected, and processed is essential in this cooperation. Without safeguards, the risk of breaches remains high.

In terms of risks, Baldakova identified dependency as a central concern. While Kazakhstan, for instance, has financial capacity to diversify and potentially replace Chinese digital tools with Western alternatives, the heavy reliance on Chinese technology creates long-term vulnerabilities. Cybersecurity also constitutes a key risk, given the potential exposure of critical infrastructure to external influence. To mitigate these risks, she stressed the importance of diversification as well as greater involvement of civil society. Citizens, she argued, should have a voice in assessing the implications of surveillance technologies, face recognition systems, and other sensitive tools imported from China, since not all members of society accept these developments without concern.

Looking ahead to future trends, Baldakova identified artificial intelligence (AI) as the central area of development. She argued that AI will become the defining field of technological cooperation (Baldakova, online interview, 3rd of September 2025). Another perspective was provided by Timur Turlov, who highlighted the opportunities for developing partnerships in e-commerce and the digital economy. He explained that joint investments in fiber optics, 5G networks, and satellite communications could substantially strengthen the technological foundations underpinning the digital aspirations of both China and Central Asian states. The digital economy, he argued, represents a natural area of collaboration, with the potential to generate significant value.

Turlov also pointed out that cooperation in areas such as electric vehicles, renewable energy, and artificial intelligence could yield transformative benefits in the future (timurturlov.com 2025).

Aidar Kurmashev, from Kazakhstan Institute for Strategic Studies added that the region faces a shortage of qualified human resources in IT, telecommunications, and artificial intelligence. Without targeted investment in education and the scientific base, he warned, partnerships with China risk remaining superficial, providing technology but not sustainable local expertise (KISI 2025).

This point was echoed by Jamal Ali, who highlighted that one of the region's persistent structural challenges is limited internet access, especially in rural and remote areas. The digital divide between urban and rural regions is not only economic but also infrastructural, exacerbating inequalities in connectivity and digital opportunities (Caspian-alpine 2024).

These expert views are consistent with wider reports. Kazakhstan's extensive adoption of Chinese surveillance systems highlights both its technological dependence and the associated security risks. In Kyrgyzstan, the personal device market reflects structural weaknesses such as large-scale smuggling of smartphones and other electronics, heavy dependence on Chinese-made hardware, and government initiatives to collaborate with PRC firms in local production. These dynamics intensify concerns over surveillance backdoors, weak regulations, and significant tax losses.

Concerns about security breaches are not hypothetical. A notable case reported by Le Monde revealed that between 2012 and 2017, data from the African Union headquarters in Ethiopia—constructed by China—was systematically transferred to servers in Shanghai. This episode illustrates the potential for PRC tech firms to serve as channels for state-led cyber espionage in developing countries (Tekir 2025).

Beyond security, there are political risks associated with the diffusion of Chinese-style governance models. Scholars have warned about the danger of importing elements of "digital authoritarianism." In 2016, Sebastian Heilmann coined the term "digital Leninism" to describe China's integration of advanced technologies into its authoritarian governance system. He argued that this approach represents a form of authoritarianism enhanced by big data and IT infrastructure, enabling extensive surveillance and censorship while reinforcing state control. Such dynamics, if transferred to Central Asia through technological cooperation, risk shaping governance models in ways that undermine democratic institutions and open digital ecosystems (Heilmann 2016).

In this context, experts emphasize the importance of constructing a sustainable balance based on national priorities, technological reliability, and open multilateral engagement. As Zhadyra Asetkyzy (baq.kz 2025) summarized, countries of Central Asia must remain vigilant in ensuring that cooperation with China aligns with their own long-term strategic and societal interests rather than leading to dependence or authoritarian drift.

The next table presents the results-chain model of China–Central Asia digital and technological cooperation based on the above discussion and analysis.

**Table 1 - Result-chain modeling of China-Central Asia digital and technological cooperation**

| Result chain | Description |
|--------------|-------------|
|--------------|-------------|



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Inputs</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Bilateral agreements, investment pledges, partnerships with external technology providers across infrastructure, governance, industry, and education.                                                                                                                                                                                          |
| <b>Activities</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Development of digital networks, 5G rollout, data centers, cloud systems, smart city and e-gov platforms, innovation hubs, and training programs.                                                                                                                                                                                              |
| <b>Outputs</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Operational fiber-optic corridors, 5G and cloud platforms, national data centers, industrial and research facilities, skilled ICT workforce.                                                                                                                                                                                                   |
| <b>Outcomes</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Improved connectivity, logistics, and governance; enhanced human capital; modernization of industries and support for innovative ecosystems.                                                                                                                                                                                                   |
| <b>Impacts</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p><b>Positive:</b> Regional integration reduced digital divide, efficient governance and logistics, wider access to advanced technologies.</p> <p><b>Negative:</b> Dependence on external providers, cybersecurity risks, threats to digital sovereignty, limited supplier diversification, skills aligned mainly with foreign platforms.</p> |
| <p>Note: compiled by author. Framework adapted from The Road to Results (Morra Imas &amp; Rist 2009). The “Impact” column highlights possible long-term effects of cooperation. Because these impacts take time to develop and are shaped by multiple factors, they are not easily measurable in the short term. The entries are therefore based on a balanced analysis of existing literature and expert opinion, presenting both potential benefits and risks rather than definitive forecasts.</p> |                                                                                                                                                                                                                                                                                                                                                |

## Policy recommendations

The rapid expansion of digital infrastructure, data systems, and technological cooperation in Central Asia creates both opportunities and vulnerabilities. To maximize benefits while mitigating risks, several policy directions should be prioritized:

*Diversify technology partnerships.* Promote diversification by engaging multiple international and domestic providers to reduce overdependence on a single country’s technology and standards.

*Strengthen cybersecurity and data protection.* Reinforce national frameworks for data governance, regular cybersecurity audits, and privacy safeguards, particularly in relation to cloud, AI, and surveillance systems.

*Enhance human, technological, and infrastructure capacity.* Invest in capacity-building to improve human resources, technological competencies, and infrastructure readiness for sustainable digital cooperation.

*Foster regional digital resilience.* Encourage collaborative approaches among Central Asian states to strengthen interoperability, safeguard critical systems, and ensure balanced engagement with major technology providers.

## **Conclusion**

Technological and digital collaboration between China and Central Asian countries has become a dynamic area of regional engagement under the Digital Silk Road framework, warranting clear categorization due to its broad scope. Kazakhstan, Uzbekistan, and Kyrgyzstan demonstrate varying degrees of integration but share a common reliance on Chinese infrastructure, expertise, and investment. This cooperation has yielded practical benefits such as improved connectivity, expanded cloud and data infrastructure, modernized telecommunications, and a rise in smart city projects. Additionally, it has fostered capacity building, research partnerships, and the emergence of new industries including electric vehicles, biotechnology, and digital agriculture.

However, this growing dependence involves risks and tensions. Heavy reliance on Chinese suppliers in sensitive domains like data infrastructure, surveillance, and cloud platforms raises concerns about sovereignty, cybersecurity, and long-term technological independence. Central Asia's limited domestic expertise in IT and telecommunications, paired with weak regulatory frameworks, intensifies vulnerability and may deepen structural reliance on China. The widespread use of surveillance technologies and the potential spread of "digital authoritarian" models also pose threats to civil liberties and transparent governance.

Looking forward, cooperation will be influenced by trends like AI expansion, e-governance integration, cross-border digital finance, and regional hub development linking Central Asia with wider Eurasia. Central Asian nations must balance opportunities offered by Chinese partnerships—such as affordable technology, swift modernization, and global market access—with the strategic need to protect national interests, diversify technology sources, and embrace multilateral cooperation.

The future of China-Central Asia digital ties hinges on transforming engagement into a platform for sustainable, inclusive growth rather than unilateral dependence, requiring good governance, investment in education and innovation, and transparent civil society dialogue. Properly managed, this partnership can help create a digitally empowered Central Asia that benefits from connectivity and innovation while safeguarding sovereignty and resilience.

## Bibliography

- 24.kg. (2021, July 1). Safe City Contract with Chinese Company Extended until March 2022.  
[https://24.kg/english/199585\\_Safe\\_sity\\_Contract\\_with\\_Chinese\\_company\\_extended\\_until\\_March\\_10\\_2022/](https://24.kg/english/199585_Safe_sity_Contract_with_Chinese_company_extended_until_March_10_2022/).
- Abuova, N. (2025, June 16). *Kazakhstan, China Sign Key Deals in Energy, Technology, Infrastructure*. The Astana Times.  
<https://astanatimes.com/2025/06/kazakhstan-china-sign-key-deals-in-energy-technology-infrastructure/>
- Adilet. (2013, May 21). *Закон Республики Казахстан от 21.05.2013 №94-V*.  
<https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm>.
- Adilet. (2015, November 24). *Закон Республики Казахстан от 24.11.2015 №418-V*.  
<https://adilet.zan.kz/rus/docs/Z1500000418>
- Adilet. (2016, February 24). *Закон Республики Казахстан от 24.02.2016 №40-VI*.  
<https://adilet.zan.kz/rus/docs/Z1600000040>
- Adilet. (2016, December 12). *Постановление Правительства Республики Казахстан от 12.12.2016 №832*.  
<https://adilet.zan.kz/rus/docs/P1600000832>
- Adilet. (2023, April 28). *Постановление Правительства Республики Казахстан от 28.04.2023 № 269*. <https://adilet.zan.kz/rus/docs/P2300000269>
- Akorda. (2025). *Об утверждении Информационной доктрины Республики Казахстан*. <https://akorda.kz/ru/ob-utverzhdanii-informacionnoy-doktriny-respubliki-kazahstan-2025248>.
- Baq.kz. (2025). *Китай и Центральная Азия расширяют технологии: эксперт о роли Казахстана как хаба*. [https://rus.baq.kz/kitay-i-tsentrlnaya-aziya-rasshiryayut-tehnologii-ekspert-o-rol-i-kazahstana-kak-haba\\_300015886/](https://rus.baq.kz/kitay-i-tsentrlnaya-aziya-rasshiryayut-tehnologii-ekspert-o-rol-i-kazahstana-kak-haba_300015886/)
- Bobokhonov, A., & Bekturganov, D. C. (2023). *China's Growing Technological Impact in Central Asia. Synopsis*.  
[https://sinopsis.cz/wp-content/uploads/2023/12/Technological\\_Impact.pdf](https://sinopsis.cz/wp-content/uploads/2023/12/Technological_Impact.pdf).
- Caspian Alpine. (2024). *Central Asia's Transition to a Digital Economy*.  
<https://caspian-alpine.org/central-asias-transition-to-a-digital-economy/>.
- Chen, Y., & Ping, Z. (2021). The Connotation, Characteristics and Development Trend of Digital Globalization. *People's Forum*, no. 5: 26–29.
- Cheney, C. (2019). China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. *Pacific Forum Working Paper* 19 (8): 3.  
[https://pacforum.org/wp-content/uploads/2019/08/issuesinsights\\_Vol19-WP8FINAL.pdf](https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf).
- China Daily. (2015, January 22). *China Digital Economy Initiatives*.  
[https://www.chinadaily.com.cn/business/2015-01/22/content\\_19374531.htm](https://www.chinadaily.com.cn/business/2015-01/22/content_19374531.htm).
- CIS Legislation. (2025). *On ICT Regulation in Uzbekistan*. <https://cis-legislation.com/document.fwx?rgn=116961>.

- City News Service. (2024). *Shanghai AI Firm to Build 'Digital Brains' in Uzbekistan*. <https://www.citynewsservice.cn/news/Shanghai-AI-firm-to-build-'digital-brains'-in-Uzbekistan-pk8aglen>.
- Civic Idea. (2022). *Digital Silk Road in Kazakhstan: Surveillance and Censorship under the Veil of Security*. <https://civicidea.ge/en/digital-silk-road-in-kazakhstan-surveillance-and-censorship-under-the-veil-of-security/>.
- CTFO. (2023, February 28). *China-Uzbekistan Cooperation News*. <https://global.ctfo.com/newsDetails?id=1860>.
- Daryo. (2024, February 17). *Uzbekistan and China Sign Agreements Worth \$3bn in Pharmaceutical Sphere*. <https://daryo.uz/en/2024/02/17/uzbekistan-and-china-sign-agreements-worth-3bn-in-pharmaceutical-sphere>.
- DLA Piper. (2025). *Data Protection Laws of Kyrgyzstan*. <https://www.dlapiperdataprotection.com/?t=law&c=KG>.
- DLA Piper. (2025). *Data Protection Laws of Uzbekistan*. <https://www.dlapiperdataprotection.com/index.html?t=law&c=UZ>.
- Fuchs, M. (2025, February 26). *Interview: Uzbekistan eager to boost cooperation with China in digital technologies, deputy minister says*. Belt and Road Portal. <https://eng.yidaiyilu.gov.cn/p/0B854TPE.html>
- Gabarró, P. P. (2020). Digital Connectivity: The Infrastructure of the Future. *Inter-American Development Bank*, 15–16. <http://dx.doi.org/10.18235/0002352>
- Gao, X. (2022). An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *The International Spectator* 57 (3): 15–30. <https://doi.org/10.1080/03932729.2022.2074710>
- Global Times. (2023, October 17). *Kazakhstan-China Digital Cooperation*. <https://www.globaltimes.cn/page/202310/1299974.shtml>.
- Ministry of Digital Development of Kazakhstan (2025, July 28). *Press Release*. Gov.kz. <https://www.gov.kz/memleket/entities/mdai/press/news/details/1041104?lang=ru>.
- Gulf Observer. (2023). *Digital Economy and Innovation: Uzbekistan-China Cooperation*. <https://thegulfobserver.com/digital-economy-and-innovation-a-new-stage-of-uzbekistan-china-cooperation/>.
- Gussarova, A. (2021). Beyond the GovTech: The pitfalls of Kazakhstan's digitalization agenda. In N. Kassenova & B. Duprey (Eds.), *Digital Silk Road in Central Asia: Present and future*. Davis Center for Russian and Eurasian Studies. [https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-10/Digital Silk Road Report 2021.pdf](https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-10/Digital%20Silk%20Road%20Report%202021.pdf).
- Heilmann, S. (2016). Leninism Upgraded: Xi Jinping's Authoritarian Innovations. *China Economic Quarterly* 20 (4): 15–22.
- Huawei. (2024). *Global Connectivity and Digital Index*. <https://www.huawei.com/en/gdi>.
- Huawei. (2024). *Huawei Commercial Roadshow in Bishkek*.

- <https://e.huawei.com/ae/news/2024/ae/huawei-commercial-roadshow-in-bishkek#:~:text=%5BBishkek%2C%20Kyrgyzstan%20%E2%80%93%20June%2012,technologies%20to%20Kyrgyzstan's%20business%20representatives.>
- Huawei Enterprise. (2025). *Railway All-Optical Network*. <https://e.huawei.com/en/solutions/enterprise-optical-network/industry-optical-transport-network/railway-all-optical-network>.
- IMD World Competitiveness Center. (2024). *World Digital Competitiveness Ranking*. <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/>.
- Inform.kz. (2023). *Более 90 соглашений на миллиарды долларов: какие отрасли охватило партнерство Казахстана и Китая*. <https://www.inform.kz/ru/bolee-90-soglasheniy-na-milliardi-dollarov-kakie-otrasli-ohvatilo-partnerstvo-kazahstana-i-kitaya-f50c4e>.
- Interfax. (2023). *China-Uzbekistan Cooperation Expands*. <https://interfax.com/newsroom/top-stories/103814/>.
- International Institute for Strategic Studies (IISS). (2022). *Digital Silk Road: Introduction*. IISS. <https://www.iiss.org/online-analysis/online-analysis/2022/12/digital-silk-road-introduction/>.
- International Telecommunication Union (ITU). (2025). *ICT Development Index (IDI)*. <https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/default.aspx>.
- Invest in Uzbekistan. (2023). *Chip Production Plans in Chirchik*. <https://invest-in-uzbekistan.org/en/novosti-uzbekistana/v-chirchike-planiruetsya-naladit-vypusk-chipov-sovmestno-s-kitaem/>.
- Kahkimov. (2024). *Digital Transformation of Uzbekistan Promotes Regional Integration in Central Asia*. *Uzbekistan.org.ua*. <https://uzbekistan.org.ua/en/news/7390-digital-transformation-of-uzbekistan-promotes-regional-integration-in-central-asia.html>.
- KISI. (2025). *Сотрудничество с Китаем: цифровой аспект*. *Kazakhstan Institute for Strategic Studies*. <https://kisi.kz/ru/sotrudnichestvo-s-kitaem-chifrovoj-aspekt/>.
- Kassenova, N., & Duprey, B. (2021). *Digital Silk Road in Central Asia: Present and Future*. *Russian and Eurasian Studies*. [https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-10/Digital\\_Silk\\_Road\\_Report\\_2021.pdf](https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-10/Digital_Silk_Road_Report_2021.pdf).
- Knight, S. (2015). *Delivering the digital region: leveraging digital connectivity to deliver regional digital growth*. *Australian Planner*, 52(1), 4–15. <https://doi.org/10.1080/07293682.2015.1019750>
- Ly, B. (2020). *Challenge and Perspective for Digital Silk Road*. *Cogent Business & Management* 7 (1): 1804180. <https://www.tandfonline.com/doi/full/10.1080/23311975.2020.1804180>



- Ministry of Digital Development of the Kyrgyz Republic. (2024). *Concept of Digital Transformation of the Kyrgyz Republic for 2024–2028*. <https://digital.gov.kg/wp-content/uploads/2024/06/concept-digital-transformation-of-the-kyrgyz-republic-for-2024-2028.pdf>.
- Ministry of Foreign Affairs of the PRC. (2024, December 1). *Foreign Ministers' Meeting Statement*. [https://www.fmprc.gov.cn/eng/wjbzhd/202412/t20241203\\_11537458.html](https://www.fmprc.gov.cn/eng/wjbzhd/202412/t20241203_11537458.html).
- Morra Imas, L. G., & Rist, R. C. (2009). *The Road to Results: Designing and Conducting Effective Development Evaluations*. *World Bank Publications*. <https://documents1.worldbank.org/curated/en/400101468169742262/pdf/The-road-to-results-designing-and-conducting-effective-development-evaluations.pdf>
- News Central Asia. (2024, December 2). *Joint Statement of the Fifth China-Central Asia Foreign Ministers' Meeting (Full Text)*. <https://www.newscentralasia.net/2024/12/02/joint-statement-of-the-fifth-china-central-asia-foreign-ministers-meeting-full-text/>.
- President.uz. (2023). *Президент Узбекистана – официальные заявления*. <https://president.uz/ru/lists/view/6345>.
- Qazinform. (2024). *Kyrgyzstan and China Strengthen Cooperation in Digitalization within SCO*. <https://qazinform.com/news/kyrgyzstan-and-china-strengthen-cooperation-in-digitalization-within-sco-122ca8>.
- QazTourism. (2025). *Kazakhstan Tourism Promotion Initiatives*. <https://qaztourism.kz/en/press-center/all/1878/>.
- Rail-News.kz. (2024). *Первый этап модернизации сетей передачи данных реализовали КТЖ и Huawei Technologies Kazakhstan*. <https://rail-news.kz/ru/news/17761-pervyi-etap-modernizacii-setei-peredaci-dannyx-realizovali-ktz-i-huawei-technologies-kazakhstan.html>.
- Railfreight. (2018, July 23). *Freight Handling at Chinese-Kazakh Border Now 30 Times Faster*. <https://www.railfreight.com/beltandroad/2018/07/23/freight-handling-at-chinese-kazakh-border-now-30-times-faster/?gdpr=accept>
- Radjabovich, M. I. (2025). *The Role of China's Digital Silk Road in Shaping the Digital Future of Central Asian Economies*. *Web of Discoveries: Journal of Analysis and Inventions* 3 (6): 4–9. <https://webofjournals.com/index.php/3/article/view/4576>.
- Rezapoor, D. (2025). *China's Cooperation with Central Asia with an Emphasis on Artificial Intelligence*. *Central Eurasia Studies* 17 (2): 157–87. [https://www.researchgate.net/publication/390549710\\_China's\\_Cooperation\\_with\\_Central\\_Asia\\_with\\_an\\_Emphasis\\_on\\_Artificial\\_Intelligence](https://www.researchgate.net/publication/390549710_China's_Cooperation_with_Central_Asia_with_an_Emphasis_on_Artificial_Intelligence).
- Spot.uz. (2023, May 23). *Uzbekistan GIS innovation project*. <https://www.spot.uz/ru/2023/05/23/uzb-gis/>.
- Strategy.uz. (2023). *Digital Uzbekistan initiatives*. <https://strategy.uz/index.php?news=1518&lang=en>.

- Sukhankin, S. (2021). Tracking the Digital Component of the BRI in Central Asia, Part One: Exporting 'Safe Cities' to Uzbekistan. *China Brief* 21 (3): 18–23. <https://jamestown.org/program/tracking-the-digital-component-of-the-bri-in-central-asia-part-one-exporting-safe-cities-to-uzbekistan/>
- Tazhiyev, K. (2021). *Towards a Central Asia-as-a-Platform strategy and a digital solutions centre for sustainable development* (Asia-Pacific Information Superhighway Working Paper Series No. 08/2021). United Nations ESCAP, ICT and Disaster Risk Reduction Division. <https://www.unescap.org/sites/default/d8files/event-documents/Towards%20a%20Central%20Asia-as-a-Platform%20Strategy%20and%20a%20Digital%20Solutions%20Centre%20for%20Sustainable%20Development.pdf>
- Tekir, G. (2025). Uzbekistan in the Belt and Road Initiative: Reviving Connectivity. *Journal of Eurasian Studies*. <https://doi.org/10.1177/18793665251362866>
- The Diplomat. (2019, June 28). *China Dominates Digital Infrastructure in Uzbekistan*. <https://thediplomat.com/2019/06/china-dominates-digital-infrastructure-in-uzbekistan/>
- Trend News Agency. (2025). *Kazakhstan-China Sign New Agreements*. <https://www.trend.az/casia/kazakhstan/3828387.html>
- Tukumov, Y. (2023). Emerging Dynamics of Asia and Central Asia: Innovation, Logistics, and Regional Stability. *Journal of Central Asian Studies* 91 (3): 7–15. <https://jcas-journal.com/index.php/jcas/article/view/14>
- Turlov, T. (2025). Expert: China-Kazakhstan See Partnership as Way Forward. <https://timurturlov.com/media/expert-china-kazakhstan-see-partnership-as-way-forward/>
- United Nations. (2024). *E-Government Development Index Overview*. UN E-Gov Knowledgebase. <https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index>
- UzA News Agency. (2018, July 6). *Huawei is implementing safe tourism pilot project in Bukhara*. <https://uza.uz/en/posts/huawei-is-implementing-safe-tourism-pilot-project-in-bukhara-06-07-2018>
- Welch, D. (2025). *Russia and China in Central Asia's Technology Stack: An Analysis of Kazakhstan, Kyrgyzstan and Uzbekistan*. German Marshall Fund of the United States. <https://www.gmfus.org/sites/default/files/2025-06/Russia%20and%20China%20in%20Central%20Asia%E2%80%99s%20Technology%20Stack.pdf>
- Vlast.kz. (2023). The BRI Turns Ten: China–Kazakhstan Relations Improve. *Vlast*. <https://vlast.kz/english/56655-the-bri-turns-ten-china-kazakhstan-relations-improve.html>
- World Bank. (2020, June). *Global Economic Prospects*. <https://doi.org/10.1596/978-1-4648-1553-9>



- Yang, G., and Jiang, M. (2015). The Networked Practice of Online Political Satire in China: Between Ritual and Resistance. *International Communication Gazette* 77 (3): 215–31. <https://doi.org/10.1177/1748048514568757>
- Yang, L. (2022). China–Kazakhstan Joint Construction of the ‘Digital Silk Road’ under the Background of COVID-19: Opportunities, Challenges and Paths. *Sociopolitical Sciences* 12 (1): 112–18. <https://doi.org/10.33693/2223-0092-2022-12-1-112-118>
- Yergaliyeva, A. (2019, January 23). Aqkol Becomes First Smart City in Kazakhstan. *Astana Times*. <https://astanatimes.com/2019/01/aqkol-becomes-first-smart-city-in-kazakhstan/>
- Zakiyeva, Z. (2021). Prospects of Digital Silk Road in Central Asia. *Вестник НАН РК* (4): 229–36. <https://doi.org/10.32014/2021.2518-1467.156>

# Watching the Watchers: China's Facial Recognition Technology and the Rise of Digital Authoritarianism in Central Asia

Yessimova Aida

## Abstract

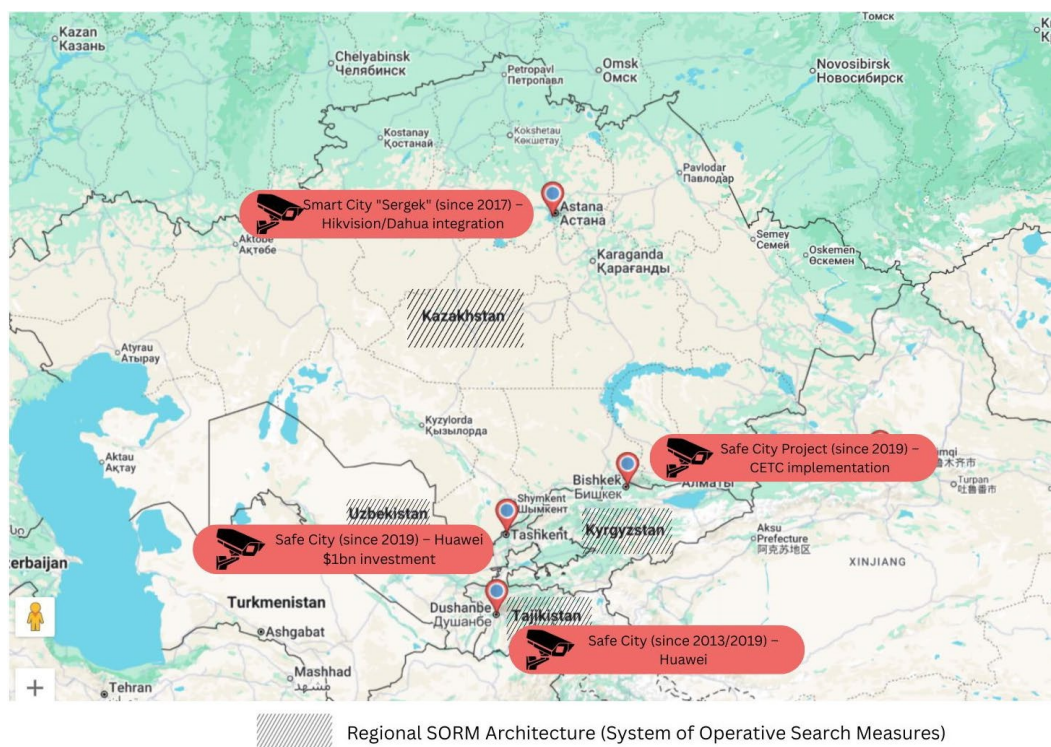
*This study investigates the impact of Chinese surveillance technologies in Kazakhstan, Kyrgyzstan, and Uzbekistan. It explores how these technologies, deployed by companies like Huawei, Hikvision, and Dahua, influence local security practices and governance, while raising concerns about privacy, data sovereignty, and political control. Using a mixed-methods approach with a survey and content analysis, the research reveals that while many respondents support surveillance for crime reduction and public safety, significant concerns persist regarding privacy invasion and foreign data access. The study highlights the legacy of Soviet-era surveillance practices, growing skepticism among younger populations, and the geopolitical implications of China's increasing influence. The paper concludes with recommendations for stricter regulatory frameworks, transparency in data handling, and the development of local alternatives to reduce reliance on foreign surveillance technologies.*

## INTRODUCTION

Central Asia, as a strategically important region at the crossroads of East and West, has become a focal point of growing interest from China, particularly within the framework of its "Digital Silk Road" initiative and its expanding economic and political influence through modern technologies. One of the most noticeable aspects of China's influence is the export of surveillance technologies, including video surveillance systems, which are being actively implemented across Central Asia. In recent years, China, through its technological giants such as Huawei, Hikvision, and Dahua, has not only provided high-tech solutions for "smart cities" but also significantly enhanced its role in regional security and citizen monitoring (Haronian, 2024; Yau, 2022). This expansion is increasingly framed within the counter-terrorism and security cooperation narrative of the

Shanghai Cooperation Organization (SCO), aligning with regional efforts to monitor "the three evil forces" of terrorism, extremism, and separatism.

The deployment of Chinese surveillance technologies in Central Asia is a critical component of the region's growing dependence on Chinese technologies, raising concerns about the political and economic sovereignty of the Central Asian states. The use of technologies like facial recognition-enabled surveillance cameras in countries such as Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan poses a significant threat to civil liberties and human rights (Figure 1). As illustrated in the 'Double Dependency' map, these Chinese-led projects are superimposed onto the regional SORM architecture, reflecting a layering of new technological tools over historical surveillance frameworks. These technologies, while purported to ensure public safety, also serve as tools for political control, particularly in authoritarian regimes (Dall'Agnola, 2025; Marat & Sutton, 2021).



The "Double Dependency" Map: Chinese Surveillance Expansion and Soviet

## Legacy in Central Asia

The purpose of this research is to analyze how Chinese video surveillance technologies are shaping security practices and governance in Central Asia. Special attention will be given to how these technologies are transforming governance practices in the region, increasing dependence on China, and introducing new risks to national security and citizen privacy. Furthermore, this study evaluates the potential for local civil society to advocate for digital rights and transparency in the face of these technological shifts.

This study will focus on the following main questions:

- How are Chinese video surveillance technologies being implemented in Central Asian countries, and what are the implications for local security systems?
- How do local governments and citizens perceive the use of Chinese surveillance technologies, and what does this mean for civil rights and freedoms?
- What role does civil society play in advocating for digital literacy and the protection of digital rights within the region?
- What are the economic and political consequences for Central Asian states as they continue their collaboration with Chinese companies in the field of security technologies?

This research draws on a wide range of sources, including government documents, reports from international organizations, and expert and civil society opinions, providing a deeper understanding of China's growing influence in the region and its role in shaping the future of Central Asia.

## **Literature Review**

The growing influence of Chinese surveillance technologies in Central Asia has become a critical area of study, particularly in relation to governance, security, and civil liberties. As the region continues to adopt these technologies, there is a growing concern over the balance between enhancing public safety and protecting individual privacy. The literature on this topic addresses both the geopolitical implications of Chinese technological exports and the local perceptions of these systems. Scholars such as Yau (2022) explore how Chinese surveillance systems are viewed as a continuation of Soviet-era control mechanisms, while others like Harold (2020) situate these technologies within

broader geopolitical strategies under the Belt and Road Initiative. Yau's work is particularly essential as it represents a necessary inclusion of independent Chinese expertise alongside Western and Central Asian views to create a more balanced body of knowledge. Comparative analyses by Sridhar (2020) offer insights into the competition between China and Russia in exporting surveillance models to the region, highlighting the complex political dynamics at play. Additionally, Dall'Agnola (2025) focuses on the public perception of these technologies in Central Asia, framing them as a form of "technocolonialism". Marat and Sutton (2021) provide an overview of the role of smart city technologies in reshaping urban governance, noting the risks of political control and data misuse. These works provide a strong foundation for understanding the broader context in which Chinese surveillance technologies are being implemented in Central Asia, but they also leave significant gaps, particularly regarding the local impact of these systems on political power structures and individual freedoms. My research will build upon and expand these studies by providing a more detailed analysis of how these technologies are perceived and utilized in the region, and their implications for civil liberties and governance in Kazakhstan, Kyrgyzstan, and Uzbekistan.

Yau's (2022) paper examines the increasing export of Chinese governance models to Central Asia, focusing on the role of Chinese surveillance technologies, including video surveillance systems, which are framed as tools to enhance public safety. The paper argues that these technologies serve not only to improve security but also to extend China's "digital control" over the region. As Yau (2022, p. 32) states, "China's surveillance systems not only enhance security but also extend Beijing's digital control across Central Asia." The paper discusses how these surveillance systems are adopted by Central Asian governments under the guise of improving urban safety, while highlighting the human rights concerns and potential political manipulation inherent in their use, particularly in authoritarian contexts. This paper is highly relevant to my research as it provides a foundational understanding of how Chinese surveillance technologies are reshaping governance and security practices in the region. It directly ties into my focus on political control and civil liberties, providing insights into how these technologies may be leveraged by governments for authoritarian control rather than merely improving safety. Yau's framing of surveillance systems as instruments of digital authoritarianism

resonates with my research, as it aligns with my interest in exploring how these systems may be used to consolidate power.

However, Yau's paper has some limitations, particularly in its lack of exploration of public perceptions of Chinese surveillance technologies in Central Asia. While it addresses the political and human rights implications from a government perspective, it largely overlooks how local populations view these systems. There is little engagement with how ordinary citizens in Kazakhstan, Kyrgyzstan, and Uzbekistan perceive the growing presence of Chinese surveillance technology in their cities, and whether these technologies are seen as a tool for security or an invasion of privacy. This gap is critical to my research, as I plan to address this issue by conducting surveys and interviews to capture local reactions to these surveillance technologies and better understand the public's concerns about privacy and foreign influence.

Additionally, while Yau effectively discusses the political implications of Chinese surveillance technologies, a more nuanced analysis could consider the internal governance needs of Central Asian countries. The adoption of these technologies is not solely driven by external political pressure from China but may also reflect local governance challenges, such as improving urban security or addressing rising crime rates. By exploring both the external influence and the internal governance needs of these countries, my research will offer a more comprehensive understanding of the motivations behind the adoption of Chinese surveillance systems.

Overall, Yau's paper provides an important theoretical foundation for my research by connecting Chinese surveillance technologies to broader political and security dynamics in Central Asia. However, its focus on governmental perspectives and its lack of attention to public perceptions and local governance dynamics leave room for further investigation. My research aims to fill these gaps by examining how Central Asians perceive these technologies and exploring the political implications of surveillance on local governance and civil liberties in the region.

Harold's (2020) book, *Digital Authoritarianism and the Belt and Road Initiative: China's Technological Influence in Central Asia*, explores how China's technological exports, particularly surveillance systems, align with its broader geopolitical strategy under the Belt and Road Initiative (BRI). The author argues that these technologies not only serve economic and infrastructural needs but



also consolidate China's influence in Central Asia by promoting "digital authoritarianism." As Harold (2020, p. 57) notes, "In Central Asia, the Belt and Road Initiative is as much about technological dominance as it is about trade routes." To understand the "dark side" of this dominance, one must look at the consequences of social credit and facial recognition in China itself, where such systems have been used to prevent civil society activists and "untrustworthy" individuals from purchasing high-speed train tickets. This practical application of digital surveillance demonstrates a level of political control that many in Central Asia may not immediately realize.

While Harold's work offers valuable insights into the geopolitical dynamics of China's influence, it lacks a detailed exploration of the practical implementation of Chinese surveillance systems in the region. The book focuses on the broader strategic and economic implications of technological exports but does not address the on-the-ground realities of how these technologies are deployed, operated, and perceived within individual Central Asian countries. My research will address this gap by examining the deployment of surveillance systems in specific countries such as Kazakhstan, Kyrgyzstan, and Uzbekistan, and exploring local perceptions of these technologies. By bridging the gap between geopolitical strategy and local implementation, my study will add depth to the understanding of Chinese technological influence in the region.

Sridhar's (2020) paper, *Cooperation or Competition: China and Russia's Surveillance Models in Central Asia*, offers a detailed comparison between the surveillance systems of China and Russia in the context of Central Asia. The paper highlights the growing competition between the two powers, both of which are seeking to expand their influence in the region through the adoption of modern surveillance technologies. Sridhar emphasizes that while China's surveillance systems are often framed as efficient solutions to urban safety and security, Russia's surveillance model is rooted in its legal frameworks designed to maintain strict control over its citizens. As Sridhar (2020, p. 112) states, "While China's surveillance systems promise efficiency, Russia's legal frameworks aim to control, creating a delicate balance in Central Asia," this efficiency is increasingly questioned by the lack of evidence that crime has significantly fallen since their introduction. The paper is an integral in providing a comparative analysis of China and Russia's approaches to surveillance technologies, offering a framework for understanding their roles in shaping governance and security practices in Central Asia. In fact, while petty crime may



be low in China, the country has seen a wave of ultra-violent "revenge on society" (*xianzhong*) attacks that these pervasive camera networks have failed to prevent (China Digital Times, 2024). This suggests that the "efficiency" narrative often serves as a rhetorical tool for governance rather than a proven solution for public safety. Furthermore, Sridhar misses the opportunity to delve into the internal factors driving Central Asian governments toward these solutions, such as economic incentives. Indeed, Sridhar's analysis is particularly valuable for contextualizing China's growing dominance in the region's surveillance market, which has increasingly gained traction with the expansion of the Belt and Road Initiative (BRI). By looking at both Chinese and Russian influences, Sridhar helps broaden the lens through which we view the geopolitical implications of these technologies, including their effect on regional sovereignty and the broader balance of power in Central Asia.

However, the paper presents several limitations. While it offers an insightful comparison of China's efficiency-driven surveillance model and Russia's control-oriented approach, it lacks a detailed exploration of the specific technologies being deployed and their impact on local political contexts. Sridhar provides a broad overview of the competing models, but he does not dive deeply into the technological specifics such as the use of facial recognition, biometric data, or advanced surveillance software – key technologies that play a pivotal role in the region's security infrastructure today. For example, China's Hikvision and Dahua have been instrumental in deploying video surveillance systems, while facial recognition and AI-driven data analysis are becoming increasingly common in urban areas. These technologies have profound implications not only for public safety but for privacy rights, freedom of expression, and personal autonomy – concerns that are not fully explored in Sridhar's analysis.

Additionally, the paper does not fully address the local political dynamics in which these technologies are implemented. In particular, it overlooks how local governments in countries like Kazakhstan, Kyrgyzstan, and Uzbekistan perceive and adopt these surveillance technologies. While Sridhar discusses the competition between China and Russia, he misses an opportunity to delve into the internal factors driving Central Asian governments to turn to Chinese surveillance solutions, often due to economic incentives or security concerns. For example, governments may see Chinese technology as more affordable or effective at addressing urban security issues like rising crime rates. This presents a gap that my research will fill by examining local decision-making

processes and how these technologies are justified in each country's specific political and social context.

Sridhar's paper also assumes a somewhat binary dynamic between Chinese efficiency and Russian control, but this oversimplification overlooks the complexities within Central Asian countries, where local political considerations and geopolitical pressures from both China and Russia often coexist. Local authorities may adopt Chinese surveillance technologies not only because of geopolitical allegiance but due to practical considerations about cost-effectiveness, technological compatibility, and regulatory challenges. In this way, Sridhar's analysis does not fully explore how local actors in Central Asia navigate the competing pressures from both China and Russia. My research will address these gaps by providing detailed case studies of how Chinese surveillance technologies, particularly facial recognition systems and AI-powered monitoring, are being implemented in specific Central Asian cities. It will also explore the local political contexts in which these systems are adopted, focusing on the governance motivations behind these decisions and the public's reaction to the growing presence of foreign surveillance technology. This will offer a more nuanced view of the technology adoption process and its implications for local autonomy and civil rights.

Dall'Agnola's (2025) paper, *From Old to New Colonial Dependencies: Public Perceptions of Chinese Surveillance Cameras in Central Asia*, explores how Chinese surveillance technologies are perceived by the public in Central Asia, arguing that they represent both a continuation of Soviet-era monitoring practices and a new form of Chinese "technocolonialism." The paper investigates how residents in Kazakhstan, Kyrgyzstan, and Uzbekistan view the growing presence of Chinese technology in their cities, particularly the widespread installation of surveillance cameras by Chinese companies like Hikvision, Dahua, and Huawei. Dall'Agnola uses interviews and surveys to analyze public perceptions, framing these technologies as a continuation of the authoritarian control mechanisms that were common during the Soviet era, yet now shaped by Chinese interests. As Dall'Agnola (2025, p. 18) asserts, "Surveillance cameras, once a tool of Soviet control, have now become instruments of China's quiet dominance."

One of the paper's key strengths is its exploration of the historical context of surveillance in Central Asia, highlighting how Soviet surveillance practices have

influenced the public's view of state monitoring systems. Dall'Agnola argues that, for many residents, Chinese surveillance systems represent a seamless transition from the Soviet era to a new form of external control—one that is not only about maintaining security but also about asserting digital dominance. This framing helps explain why many Central Asians view the increasing presence of Chinese surveillance cameras with a sense of unease, associating it with foreign influence and the loss of sovereignty. The argument that these technologies represent "technocolonialism" is particularly relevant to my research, as it aligns with my focus on the geopolitical implications of Chinese surveillance in the region. The paper's use of interviews and surveys provides important qualitative data on how ordinary citizens perceive these technologies. Yet, there is also a significant gap regarding the role of local civil society in advocating for digital rights and transparency. The surveys, conducted across Central Asian cities, reveal mixed opinions: some see the cameras as beneficial for public safety, while others view them as an invasion of privacy or a mechanism for control. This nuanced approach is valuable because it directly addresses the public's views on Chinese surveillance systems, a crucial element missing in many studies that focus more on government narratives or geopolitical strategy.

However, while Dall'Agnola's paper offers valuable insights into public perceptions, it lacks a more in-depth analysis of the political consequences these surveillance technologies have on local governance and authoritarian control. Although the paper discusses how these systems are perceived by the public, it does not fully explore how they are being used by Central Asian governments to strengthen political control and suppress dissent. Given that many Central Asian countries are authoritarian or have hybrid political systems, the deployment of Chinese surveillance technologies could be a double-edged sword: they provide public safety, but also become tools for the monitoring and suppression of oppositional voices. Dall'Agnola mentions state surveillance but does not analyze the political power structures in which these technologies are embedded.

For example, in Kazakhstan, the introduction of smart city technologies with facial recognition could not only aid in crime prevention but could also be used for political surveillance during protests or opposition movements. Kyrgyzstan and Uzbekistan also face similar dynamics, where Chinese technology could be a tool for monitoring political dissent while presenting itself as a solution to urban crime. My research will fill this gap by examining the political motivations behind the

adoption of Chinese surveillance systems and how these systems affect civil liberties and freedom of expression in Central Asia.

Additionally, Dall'Agnola's focus on public perception does not delve deeply into the legal frameworks surrounding these surveillance technologies. For example, who controls the data generated by Chinese cameras? Is the data shared with Chinese authorities? These questions are critical for understanding the sovereignty implications of surveillance technologies, but the paper does not fully engage with the legal challenges or the political implications of data security. My research will address this issue by exploring the legal and ethical dimensions of using foreign surveillance technologies in a sovereign state, specifically focusing on data protection, privacy laws, and foreign access to sensitive information.

Hence, while Dall'Agnola's paper provides essential insights into the public's perception of Chinese surveillance technologies in Central Asia, it does not explore the full political and governance implications of these systems. My research will complement this work by investigating the impact of these technologies on authoritarian practices, political control, and civil rights, offering a deeper understanding of the broader geopolitical and local governance consequences.

Marat and Sutton's (2021) paper, *Technological Solutions for Complex Problems: Emerging Electronic Surveillance Regimes in Eurasian Cities*, explores the growing role of electronic surveillance in urban areas, with a particular focus on the implementation of smart city projects in Central Asia. The authors examine the technological, political, and economic dimensions of these surveillance systems, providing a comprehensive view of how such technologies are reshaping urban governance. They note that while these systems contribute to improving urban safety, they also raise concerns about political control and the potential misuse of data. As Marat and Sutton (2021, p. 252) succinctly state, "In Eurasian cities, smart surveillance systems are more about political control than about solving crime." The paper offers a broad overview of the rise of smart city technologies, emphasizing how surveillance tools like CCTV, facial recognition, and big data analytics are being integrated into urban infrastructure in cities across Central Asia. The authors argue that, while these technologies improve safety and crime prevention, they also introduce new risks, particularly when they fall under the control of

authoritarian governments that may use them to monitor and suppress opposition. This argument is especially pertinent to my research, as it highlights the tension between public safety and civil liberties, a key theme in my study of Chinese surveillance technologies in the region. The paper will be instrumental in framing the technological aspects of my research, particularly regarding how these systems interact with governance practices and political control.

Marat and Sutton also discuss how the introduction of smart city technologies can redefine power dynamics within urban spaces, shifting power from local populations to those in charge of surveillance systems. This shift, the authors argue, can lead to the erosion of privacy and a concentration of power in the hands of those who control the surveillance infrastructure. This issue is directly relevant to my study of Chinese surveillance systems, particularly in cities where Chinese companies like Hikvision and Dahua have a growing presence. These companies are not only providing surveillance technologies but are also involved in data management, raising concerns about data sovereignty and the control of personal information.

However, while Marat and Sutton provide an excellent overview of how smart surveillance is being implemented in Eurasian cities, the paper lacks a deeper dive into the specific technologies being used in these projects, especially those provided by Chinese companies. The authors mention that these systems improve safety and governance but do not explore how specific surveillance tools, like facial recognition and AI-driven monitoring systems, affect individual freedoms and privacy. For instance, while CCTV systems are discussed, the paper does not detail how the data collected through these systems is used or the risks of misuse, particularly in authoritarian contexts where data could be used to track political dissent or monitor citizens' activities.

My research will fill this gap by providing a detailed examination of how Chinese surveillance technologies such as facial recognition and biometric data collection are being deployed in Central Asian cities, particularly in Kazakhstan, Kyrgyzstan, and Uzbekistan. Additionally, I will explore the impact of these technologies on personal freedoms and civil liberties, focusing on how these technologies are perceived by the public and how they influence local governance structures. By focusing on the specific types of surveillance technologies used and their practical implications, my research will offer a

more comprehensive understanding of the balance between security and freedom in smart city projects across Central Asia.

So, Marat and Sutton's paper provides a valuable overview of the political and technological dimensions of smart surveillance systems in Eurasian cities, especially within Central Asia. However, it lacks an in-depth analysis of the specific technologies and their impact on citizens' lives. My research will build on their work by offering detailed case studies of how Chinese surveillance systems affect civil liberties and the political control of local governments in the region.

In summary, the literature on Chinese surveillance technologies in Central Asia provides valuable insights into both the geopolitical and local dimensions of these systems. Scholars have explored the political motivations behind the adoption of Chinese surveillance tools, highlighting concerns about authoritarian control and the erosion of civil liberties. While works by Yau (2022), Harold (2020), and Sridhar (2020) provide a robust understanding of the broader implications of China's technological dominance, much of the research overlooks the specific technologies deployed and their impact on the daily lives of citizens. Additionally, the public perception of these systems remains underexplored, despite its critical importance in understanding the acceptance or resistance to foreign surveillance. Dall'Agnola (2025) and Marat and Sutton (2021) contribute to this gap by addressing public perceptions and urban governance, yet they do not fully delve into how these technologies influence local governance structures and the political control they exert. My research aims to fill these gaps by offering a comprehensive analysis of how Chinese surveillance technologies are perceived by local populations and how they shape governance and political power dynamics in Central Asia. Through this, I seek to provide a more nuanced understanding of the implications of Chinese surveillance systems in the region, particularly in terms of privacy, freedom, and sovereignty.

## METHODOLOGY

The growing influence of Chinese surveillance technologies in Central Asia, discussed in the literature review, points to significant gaps in understanding



both the implementation of these technologies and their public perception in the region. The literature indicates that Chinese surveillance technologies, particularly video surveillance systems (e.g., from Huawei, Hikvision, and Dahua), are increasingly seen as tools for enhancing state security. However, there is limited understanding of how these systems are perceived by local populations and the broader political, social, and ethical implications of their use. This research aims to address these gaps by examining the implementation of these technologies in Kazakhstan, Kyrgyzstan, and Uzbekistan, while simultaneously exploring the political, security, and privacy implications from both governmental and public perspectives.

Given the multidimensional nature of the research questions, a mixed-methods approach is employed, combining quantitative survey data and qualitative content analysis. This approach is particularly well-suited to the investigation of complex phenomena such as surveillance systems, which involve both objective technological implementations and subjective public perceptions (Teddlie & Tashakkori, 2009).

The first method employed is a survey aimed at gathering quantitative data on public perceptions of Chinese surveillance technologies. Surveys are commonly used in social research to collect data on attitudes, behaviors, and opinions from a large group of individuals (Fink, 2017). This method was selected because it allows for the collection of generalizable data on how Central Asian citizens perceive the growing presence of Chinese surveillance systems in their daily lives. This survey reached a total sample of 67 respondents across the target region. While this sample size reflects the specific scope of the study, it is crucial to contextualize this figure within the regional political climate. Conducting research on surveillance and Chinese technological influence is a highly sensitive political issue in Central Asia, often subject to censorship or self-censorship. Consequently, reaching a large audience publicly is inherently challenging, as many individuals may be reluctant to express dissenting opinions or discuss government-led security initiatives due to fear of repercussions. Therefore, this sample represents a critical cross-section of urban, tech-savvy populations who are most likely to be impacted by these technologies.

The survey was designed to address the following questions:

- How do people feel about the installation of Chinese surveillance technologies in their cities?
- What concerns do they have about privacy and data security?
- How do they perceive Chinese influence in the region?

The survey included both demographic questions (such as age, gender, education level, and employment status) and perception-related questions focused on the presence of Chinese surveillance cameras. Specifically, the survey sought to measure:

- Respondents' attitudes toward the effectiveness of surveillance systems in improving public safety.
- Concerns regarding the privacy implications of these technologies, particularly foreign access to data.
- Overall trust in the local government's use of Chinese technology.

The survey was distributed through various online channels, including social media, email lists, and forums, which enabled access to a diverse group of respondents across the target countries. This method was chosen to ensure broad participation and to capture a wide range of opinions from urban populations who are most likely to be impacted by the technologies.

The quantitative data was analyzed using statistical methods to identify key trends and patterns in public perceptions. Descriptive statistics, such as frequency distributions and percentages, were used to summarize demographic information and to assess the general views on privacy, data security, and public safety. Cross-country comparisons were made to examine any significant differences in perceptions across Kazakhstan, Kyrgyzstan, and Uzbekistan, particularly regarding issues of safety and foreign influence. Additionally, correlational analysis was conducted to explore whether certain demographic factors (such as age or education level) influenced individuals' attitudes toward Chinese surveillance technologies.

Content analysis is the second method used in this research. It is a widely recognized qualitative method that involves the systematic review of publicly available documents, policy reports, and media articles related to Chinese surveillance technologies in Central Asia (Neuendorf, 2017). This method was

chosen because it allows for a comprehensive examination of the official narratives surrounding the implementation of these technologies and how they are justified by local governments and Chinese companies. These narratives are critical to understanding the political, economic, and social dynamics at play.

The content analysis specifically focuses on documents such as government publications, corporate communications from Chinese companies, and media reports on the installation and usage of surveillance systems in Kazakhstan, Kyrgyzstan, and Uzbekistan. The primary goal is to explore how these technologies are framed in relation to security enhancement, public safety, and privacy concerns. This is crucial for understanding how governments and companies portray the surveillance systems, especially in terms of their potential to combat crime and enhance urban management, versus the risks they pose to individual freedoms and national sovereignty (Marat, 2021; Yau, 2022).

In applying content analysis, the following steps were taken:

1. Government documents, policy reports, and media articles from reputable sources such as government websites, news outlets, and reports by international organizations were systematically collected. This ensured the sources were reliable and current.
2. The content was coded thematically to identify recurring themes, such as security vs. privacy, foreign influence, and public safety. This helped uncover the dominant narratives surrounding the deployment of Chinese technologies.
3. Additionally, discourse analysis was used to examine the tone and framing of these technologies in the public and political spheres. This helped assess whether the technologies were being presented as solutions to security problems or as tools of digital authoritarianism (Dall'Agnola, 2025).

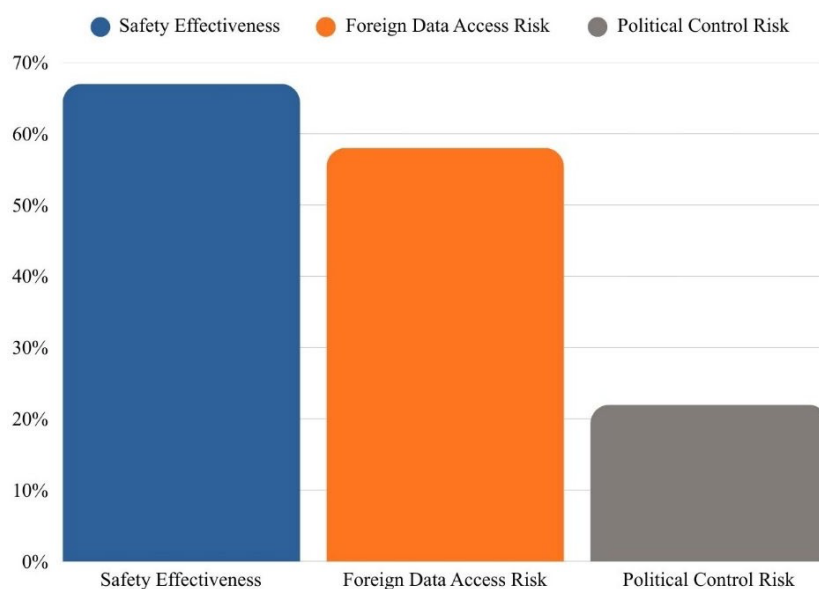
This method was selected because it provides a structured approach to understanding how these technologies are politically constructed and justified by key stakeholders, while also offering insights into how local perceptions are influenced by official narratives.

In general, the combination of the survey and content analysis offers a method of data triangulation, which helps validate and enrich the research findings by

comparing data from multiple sources and perspectives (Patton, 2015). By combining qualitative insights from government and media sources with quantitative data from the public, the research provides a comprehensive analysis of the role and impact of Chinese surveillance technologies in Central Asia. This triangulation allows for a deeper understanding of how policy frameworks align with public opinion and provides a more holistic view of the geopolitical, social, and ethical implications of these technologies in the region.

## RESULTS AND DISCUSSION

This section integrates the findings from the survey with the broader academic literature to provide an in-depth analysis of the public perceptions and implications of Chinese surveillance technologies in Central Asia. By examining both the quantitative survey results and qualitative open-ended responses, this discussion explores the themes of privacy, security, and geopolitical influence, while incorporating the scholarly perspectives on Chinese surveillance in the region.



The Trade-off Between Perceived Security and Digital Privacy.

The survey results highlight a complex relationship between the public's perception of Chinese surveillance technologies and their concerns about

privacy and security. As seen in the responses, there is significant support for surveillance technologies as a means to enhance public safety. A majority (67%) of respondents viewed Chinese surveillance technologies as effective tools for crime reduction, aligning with the official rhetoric of Central Asian governments, which often frame these technologies as essential for urban security (Figure 2). This perception is consistent with findings from Yau (2022), who argues that Chinese surveillance systems are marketed as tools to combat crime and maintain public order across Central Asia (Yau, 2022).

However, a substantial proportion of the population (22%) expressed concerns that these systems are not only tools for security but also mechanisms for political control, particularly in authoritarian regimes where civil liberties are at risk (Figure 2). These concerns resonate with the "digital authoritarianism" thesis proposed by Harold (2020), who discusses how the Chinese state uses surveillance systems to assert its influence and control in regions like Central Asia (Harold, 2020).

This division in public opinion is reflective of the broader geopolitical context surrounding the Belt and Road Initiative (BRI), which has facilitated China's growing technological footprint in Central Asia. As Sridhar (2020) points out, China's growing dominance in surveillance technologies is framed as part of its broader economic strategy, providing affordable technological solutions while ensuring increased dependence on Chinese systems (Sridhar, 2020). In this light, the use of surveillance systems becomes a double-edged sword—offering security benefits but also raising significant concerns about data sovereignty and the erosion of local governance autonomy.

### **Concerns about Privacy and Data Sovereignty**

One of the key findings of the survey was the widespread concern regarding data privacy and the potential for foreign access to personal data. A majority (58%) of respondents expressed concerns that China could access the data collected by surveillance cameras, highlighting the fear of data misuse and foreign control (Figure 2). These concerns are echoed by Dall'Agnola (2025), who argues that surveillance technologies deployed by Chinese firms like Hikvision and Dahua represent a form of "technocolonialism", whereby local data is vulnerable to manipulation by foreign governments, undermining

national sovereignty (Dall'Agnola, 2025). The risk of data leakage and the potential for surveillance systems to be used for political surveillance is a persistent issue in Central Asia, where local governments often lack stringent data protection laws (Marat & Sutton, 2021).

In the context of Central Asia's geopolitical dynamics, these concerns are further compounded by the growing economic dependence on China. As Marat (2018) discusses, the Chinese government often ties infrastructure projects—such as surveillance systems—to larger economic deals under the BRI. This creates a situation where Central Asian governments, although receiving much-needed technological upgrades, may inadvertently compromise their sovereignty by becoming overly reliant on Chinese systems for critical national infrastructure (Marat, 2018).

### **The Influence of Soviet Legacy on Public Acceptance**

The survey also revealed that many respondents accepted surveillance systems due to the legacy of Soviet-era collectivism, where the prioritization of state security often took precedence over individual privacy. This acceptance reflects a deeply ingrained mindset in Central Asia, where public security was historically enforced through extensive state surveillance. As Dall'Agnola (2025) notes, this Soviet legacy has contributed to public acceptance of surveillance practices, especially in Kazakhstan, Kyrgyzstan, and Uzbekistan, where citizens are more inclined to tolerate state surveillance in exchange for the perceived benefits of public order and security (Dall'Agnola, 2025). This historical context helps explain why many respondents do not view the presence of surveillance cameras as intrusive, but rather as a necessary tool for maintaining law and order.

However, this acceptance is not without its limitations. As the survey findings suggest, there is a growing skepticism, particularly among younger, more educated respondents, about the long-term implications of such systems. Many respondents expressed concerns that these technologies could be used for political control rather than solely for security purposes. This shift in attitude reflects broader changes in public awareness of privacy rights and a growing resistance to the erosion of individual freedoms in the digital age.



## Geopolitical Context and Public Opinion

The dual nature of support and concern for Chinese surveillance technologies in Central Asia is also shaped by the broader geopolitical dynamics of the region. As Sridhar (2020) observes, Central Asia's adoption of Chinese surveillance technologies is framed as part of the larger competition between China and Russia for influence in the region. While Russia has historically had more influence over security-related matters through legal frameworks like SORM (System of Operative Search Measures), China's technological superiority in areas like facial recognition and artificial intelligence has made it the preferred partner for many Central Asian governments (Sridhar, 2020). This geopolitical competition has significant implications for local governance, as the adoption of foreign surveillance technologies could weaken national autonomy and make these countries more susceptible to external control.

In this context, Yau (2022) highlights the complexity of the region's dependence on Chinese technologies, as these systems not only enhance public security but also deepen China's influence over national and regional governance (Yau, 2022). The survey responses echo this concern, with many respondents recognizing the trade-off between technological advancement and national sovereignty.

Interestingly, recent policy shifts in China itself indicate a growing recognition of the risks associated with pervasive surveillance. As of March 2025, the Chinese government issued guidelines stating that facial recognition technology should not be forced upon individuals when other effective methods are available (Reuters, 2025). This development suggests that even the primary exporter of these systems is responding to negative feedback regarding privacy, a point that should encourage Central Asian policymakers to consider similar protective frameworks.

## Recommendations for Future Implementation of Surveillance Systems

Based on the survey results and existing literature, several key recommendations emerge for the future implementation of Chinese surveillance technologies in Central Asia:

- **Regulatory Frameworks:** There is a clear need for stricter regulations governing the use of surveillance technologies. Respondents emphasized the importance of protecting data

privacy and ensuring that surveillance systems are used transparently and ethically. As Harold (2020) suggests, robust legal frameworks are necessary to prevent the misuse of data and to protect civil liberties while enhancing security (Harold, 2020).

- **Transparency and Public Access:** Several respondents recommended that governments provide public access to information about the data collected by surveillance systems. This would increase public trust in these technologies and ensure that citizens are aware of the extent of monitoring.
- **Local Technological Development:** There is widespread support for developing local alternatives to foreign surveillance technologies. Many respondents suggested that Central Asian countries should invest in their own technological infrastructure, reducing their reliance on foreign powers like China. This would not only protect national sovereignty but also ensure that data is securely stored within national borders.
- **International Collaboration on Data Protection:** Given the geopolitical context, it is also recommended that Central Asian countries collaborate with international bodies to develop stronger data protection standards. These standards would ensure that personal data is not misused by foreign governments or corporations and that citizens' rights are protected.
- **Digital Advocacy and Literacy:** Central Asian civil society must advocate for transparency and digital rights, promoting literacy to help citizens understand the risks associated with pervasive surveillance. This involvement is crucial to ensure that the deployment of technologies like facial recognition does not proceed without public oversight and protection of fundamental freedoms.

The survey results, when viewed in the context of existing literature, highlight the complex interplay between security, privacy, and geopolitical influence in the adoption of Chinese surveillance technologies in Central Asia. While there is substantial support for the use of these technologies to enhance public safety, concerns about data privacy, foreign influence, and the erosion of national sovereignty remain significant. The growing dependence on China for technological infrastructure, as well as the legacy of Soviet-era surveillance practices, further complicates the region's stance on these issues. Moving

forward, there is a need for stronger regulatory frameworks, greater transparency, and a focus on national technological development to ensure that the benefits of surveillance technologies do not come at the cost of civil liberties or national autonomy.

## Limitations

While this study provides valuable insights into public perceptions of Chinese surveillance technologies in Central Asia, it is not without its limitations. One key limitation is the relatively small sample size of 67 respondents, which, although diverse, may not fully capture the views of the broader population in the region. The sample was heavily skewed towards younger, urban, and more educated individuals, particularly in the 18-34 age range. This demographic is more likely to engage with and be aware of digital technologies, which may not be representative of rural populations or older individuals who may have different perspectives on surveillance technologies. Consequently, the findings may reflect a more tech-savvy viewpoint, leaving out the perspectives of individuals who have less access to or knowledge of such technologies.

Geographically, the survey responses were primarily from Kazakhstan and Kyrgyzstan, with minimal participation from Uzbekistan and no respondents from Turkmenistan and Tajikistan. This geographic limitation restricts the scope of the study in capturing regional differences in attitudes toward Chinese surveillance technologies. While Kazakhstan and Kyrgyzstan may have similar views on surveillance due to their political, cultural, and economic ties, Uzbekistan and Turkmenistan may have different experiences and concerns, given their distinct political environments and the level of exposure to Chinese technologies in these countries.

Additionally, the study relied on self-reported data, which is inherently susceptible to biases. Respondents may have given socially desirable answers or inaccurately recalled their experiences, particularly when discussing sensitive topics such as privacy and government surveillance. Given the authoritarian political climate in many Central Asian countries, there is a possibility that respondents underreported their concerns about the invasion

of privacy or the potential misuse of surveillance systems, either due to fear of political repercussions or a reluctance to express dissenting opinions.

Another significant limitation is the lack of longitudinal data. The survey was a one-time snapshot of public opinion, and as such, it cannot track changes in attitudes over time. Public perceptions may shift as surveillance systems become more integrated into everyday life, or as the geopolitical landscape in Central Asia evolves with China's growing influence. Longitudinal research would provide a better understanding of how attitudes toward surveillance technology may change as these systems become more widespread and as the political and security contexts in the region evolve.

Furthermore, the study focused primarily on public opinion and did not explore the perspectives of government officials, policymakers, or surveillance experts. Including insights from these groups would provide a more holistic view of the issue, allowing for a deeper understanding of the political and strategic motivations behind the adoption of Chinese surveillance technologies. Governmental perspectives are crucial for understanding the rationale behind the widespread use of these technologies, as well as the potential implications for national security, sovereignty, and citizen privacy.

These limitations underscore the need for further research on this topic, particularly with a larger and more representative sample of respondents, as well as in-depth interviews with policymakers, technology experts, and other key stakeholders. Additionally, research that spans a longer period of time and covers a broader geographic range would help provide a more comprehensive and nuanced understanding of the growing role of Chinese surveillance technologies in Central Asia and their implications for privacy, governance, and international relations in the region.

## CONCLUSION

This study has explored the growing influence of Chinese surveillance technologies in Central Asia, with a particular focus on how these technologies shape local security practices, governance, and citizens' perceptions of privacy and sovereignty. As China's technological footprint expands in the region, particularly through the Belt and Road Initiative (BRI), Chinese surveillance

companies such as Huawei, Hikvision, and Dahua have played a pivotal role in implementing high-tech solutions that ostensibly enhance urban security. However, this technological integration raises significant concerns about civil liberties, data sovereignty, and geopolitical influence.

The findings of this study indicate a complex public opinion landscape. While many respondents recognize the potential benefits of surveillance systems for crime reduction and public safety, a notable proportion of the population expressed concerns about the invasion of privacy and the erosion of national sovereignty. This tension between the perceived benefits of improved security and the potential risks associated with foreign control of data highlights the broader implications of digital authoritarianism discussed in the literature (Harold, 2020; Yau, 2022). Respondents were particularly concerned about the possibility that China could access personal data collected by surveillance systems, fearing data misuse and the loss of control over sensitive national information.

Moreover, the study found that the legacy of Soviet-era surveillance practices plays a significant role in the acceptance of state surveillance in Central Asia. Many respondents did not view the installation of surveillance cameras as intrusive, reflecting an ingrained tendency to prioritize state security over individual privacy. However, there was a noticeable shift, especially among younger, more educated respondents, who voiced concerns about the long-term political implications of adopting such technologies in authoritarian regimes. These findings underscore the need to consider both historical contexts and modern governance challenges when evaluating the adoption of surveillance systems in the region.

The geopolitical context surrounding the adoption of Chinese surveillance technologies is also critical. As Central Asian countries continue to deepen their economic and political ties with China, the region becomes more dependent on Chinese technologies, which in turn increases China's strategic influence. This creates a delicate balance between the economic benefits of technological investment and the potential loss of national autonomy. As Sridhar (2020) and Dall'Agnola (2025) suggest, this growing dependence on Chinese technologies is akin to a form of "technocolonialism", where local governance structures may become more susceptible to external influence and control.

Looking ahead, the study highlights several important recommendations for managing the deployment of Chinese surveillance technologies in the region. Clear regulatory frameworks and transparency in data collection are critical to ensuring that surveillance systems do not infringe on individual rights. Additionally, there is a strong call for technological independence and the development of local alternatives to reduce reliance on foreign surveillance systems, ensuring that data sovereignty is maintained. These findings suggest that while the adoption of modern surveillance technologies can undoubtedly improve urban security, it is essential that these systems be carefully regulated to protect civil liberties and maintain national sovereignty.

In conclusion, this study has shed light on the multifaceted relationship between technological advancement, governance, and civil liberties in Central Asia. As Chinese surveillance systems continue to shape the security landscape in the region, it is imperative for policymakers to strike a balance between leveraging technological advancements for public safety and safeguarding the fundamental rights of citizens. Further research is needed to explore these dynamics in greater detail, particularly through longitudinal studies and the inclusion of governmental perspectives, to better understand the evolving role of Chinese technologies in Central Asia's political and social fabric.

## Bibliography

- Altynbayev, K. (2019, November 12). *Chinese hardware in Kazakh cities raises spying concerns*. Caravansarai. [https://central.asianews.com/en\\_GB/articles/cnmi\\_ca/features/2019/12/11/feature-01](https://central.asianews.com/en_GB/articles/cnmi_ca/features/2019/12/11/feature-01)
- Bekturganov, D. (2022). *Digital Silk Road in Kazakhstan: Surveillance and censorship under the veil of security*. Eurasian Research Institute. <https://www.eurasian-research.org/publication/digital-surveillance-solutions-in-central-asian-states/>
- Central Asia Barometer. (2022). *Central Asians' sentiments toward the use of surveillance cameras to reduce crime (Wave 11)*. Central Asia Barometer. <https://cabarometer.org/en/projects/central-asia-barometer-survey-wave-11> ([cabarometer.org](https://cabarometer.org/en/projects/central-asia-barometer-survey-wave-11) in Bing)
- Caspian Policy Center. (2024). *China's growing influence in Central Asia through surveillance systems*. Caspian Policy Center. <https://api.caspianpolicy.org/media/uploads/2020/09/PB-Chinas-growing-influence-in-CA-through-surveillance-systems.pdf>
- China Digital Times. (2024). *Words of the week: "Revenge on society" attacks lead to government monitoring of individuals with "four lacks and five frustrations"*. China Digital Times. <https://chinadigitaltimes.net/2024/11/words-of-the-week-revenge-on-society-attacks-lead-to-government-monitoring-of-individuals-with-four-lacks-and-five-frustrations/> ([chinadigitaltimes.net](https://chinadigitaltimes.net/2024/11/words-of-the-week-revenge-on-society-attacks-lead-to-government-monitoring-of-individuals-with-four-lacks-and-five-frustrations/) in Bing)
- Dall'Agnola, J. (2025). From old to new colonial dependencies: Public perceptions of Chinese surveillance cameras in Central Asia. *Swiss Political Science Review*. <https://doi.org/10.1111/spsr.12655>
- Dall'Agnola, J. (2025). Digital Silk Road: Keeping watch along the Digital Silk Road. In E. Schatz & R. Silvey (Eds.), *Seeing China's Belt and Road* (pp. 164–184). Oxford University Press. <https://doi.org/10.1093/oso/9780197789261.003.0009> ([doi.org](https://doi.org/10.1093/oso/9780197789261.003.0009) in Bing)
- Dahua Technology. (2018, July 11). *Dahua delivers complete solution for Pengsheng Industrial Park in Uzbekistan*. Dahua Security. <https://www.dahuasecurity.com/fr/newsEvents/successStories/61/711>



- Fink, A. (2017). *How to conduct surveys: A step-by-step guide*. SAGE Publications.  
[https://books.google.kz/books/about/How to Conduct Surveys.html?id=jlBEi7jsk-gC&redir\\_esc=y](https://books.google.kz/books/about/How_to_Conduct_Surveys.html?id=jlBEi7jsk-gC&redir_esc=y)
- Haronian, N. (2024, October 9). *Surveillance on the steppe*. Brown Political Review.  
<https://brownpoliticalreview.org/surveillance-on-the-steppe>
- Kassenova, N., & Duprey, B. (Eds.). (2021). *Digital Silk Road in Central Asia: Present and future*. Davis Center for Russian and Eurasian Studies.  
[https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-10/Digital\\_Silk\\_Road\\_Report\\_2021.pdf](https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-10/Digital_Silk_Road_Report_2021.pdf) ([daviscenter.fas.harvard.edu](https://daviscenter.fas.harvard.edu) in Bing)
- Marat, E., & Sutton, D. (2020). Technological solutions for complex problems: Emerging electronic surveillance regimes in Eurasian cities. *Europe-Asia Studies*, 73(1), 243–267. <https://doi.org/10.1080/09668136.2020.1832965>
- Mills, L., & Wang, M. (2019, November 15). *Facial recognition deal in Kyrgyzstan poses risks to rights*. Human Rights Watch.  
<https://www.hrw.org/news/2019/11/15/facial-recognition-deal-kyrgyzstan-poses-risks-rights> ([hrw.org](https://www.hrw.org) in Bing)
- Neuendorf, K. A. (2017). *The content analysis guidebook*. SAGE Publications.  
<https://books.google.kz/books?hl=en&lr=&id=nMA5DQAAQBAJ&oi=fnd&pg=PP1>
- Pao, W. (2024, November 18). *2024 Security 50 industry report: Optimism prevails as security returns to growth trajectory*. Asmag.  
<https://www.asmag.com/rankings>
- Patton, M. Q. (2015). *Qualitative research and evaluation methods*. SAGE Publications.  
<https://books.google.kz/books?hl=en&lr=&id=ovAkBQAAQBAJ&oi=fnd&pg=PP1>
- Reuters. (2025, March 21). *China says facial recognition should not be forced on individuals*. Reuters. <https://www.reuters.com/technology/china-says-facial-recognition-should-not-be-forced-individuals-2025-03-21/>
- Sridhar, V. (2020, September 18). *Cooperation or competition: China and Russia's surveillance models in Central Asia*. The Geopolitics.  
<https://thegeopolitics.com/cooperation-or-competition-china-and-russias-surveillance-models-in-central-asia/>

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research*. SAGE Publications.

[https://books.google.kz/books/about/Foundations\\_of\\_Mixed\\_Methods\\_Research.html?id=c3uojOS7pK0C&redir\\_esc=y](https://books.google.kz/books/about/Foundations_of_Mixed_Methods_Research.html?id=c3uojOS7pK0C&redir_esc=y) ([books.google.kz in Bing](#))

Yau, N. (2019, August 7). *Smart cities or surveillance? Huawei in Central Asia*. The Diplomat. <https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/>

Yau, N. (2022). Chinese governance export in Central Asia. *Security and Human Rights*, 32(1–4), 28–40. <https://doi.org/10.1163/18750230-bja10009>

# Digital Infrastructure and Sovereignty in Central Asia: Chinese Investments and State Strategies (2018-2025)

## Abstract

*This paper provides the first comprehensive analysis of Chinese digital infrastructure investments in Central Asia through verified project-level data. Documenting \$2.97 billion across Kazakhstan and Uzbekistan (2018-2025), we reveal telecommunications (64%) and surveillance systems (34%) dominate Chinese engagement. We develop a "stratified digital sovereignty" framework demonstrating how states exercise differential control across infrastructure layers (physical, protocol, platform, data), resolving contradictions between technological dependence and innovation success.*

*Kazakhstan's "strategic hedging" approach limits Chinese investment (\$1.05 billion) while maintaining vendor diversity, enabling Kaspi.kz's \$17.5 billion valuation. Uzbekistan's "accelerated integration" strategy attracts larger investment (\$1.93 billion), expanding its digital economy from 2% to 22% of GDP in four years, while accepting deeper dependencies including surveillance systems for "political affairs management." Despite Chinese infrastructure adoption, local platforms thrive through strategic positioning and state protection, with both countries producing unicorns. However, deployment of 1.4 million surveillance cameras without privacy frameworks raises governance concerns. Technology transfer remains limited, focusing on operational training rather than knowledge sharing.*

*The research contributes theoretically by showing sovereignty operates differentially across technological layers rather than being binary. Empirically, it provides baseline data challenging inflated investment estimates while documenting transformation. Policy implications suggest Central Asian states can preserve sovereignty through layer-specific strategies, Western competitors should focus on platform/service layers where local knowledge matters, and surveillance governance requires urgent attention. The shift toward AI infrastructure and CNY-denominated financing signals a critical juncture where 2025-2027 policy choices will determine whether Central Asia maintains technological options or locks into Chinese ecosystems permanently.*

## Introduction: Digital Transformation and Strategic Adaptation in Central Asia

### *The Transformation Paradox*

Uzbekistan's digital economy expanded from 2 percent to 22 percent of GDP between 2020 and 2024, while Kazakhstan's fintech platform Kaspi.kz achieved a

\$17.5 billion valuation on NASDAQ.<sup>1</sup> These achievements emerged through \$2.97 billion in Chinese digital infrastructure investments across sixteen documented projects from 2018-2025 (see Table 1). Internet penetration in Uzbekistan surged from 46 percent to 86 percent in six years, IT services exports grew twenty-two-fold to \$344 million, and Kazakhstan reached 86 percent internet coverage alongside 85 percent cashless transaction adoption.<sup>2</sup>

| Sector               | Kazakhstan      | Uzbekistan        | Total             | Percentage  |
|----------------------|-----------------|-------------------|-------------------|-------------|
| Telecommunications   | \$1,025M        | \$874.8M          | \$1,899.8M        | 63.9%       |
| Surveillance Systems | \$23M*          | \$1,000M          | \$1,023M          | 34.4%       |
| AI/Data Centers      | \$0             | \$50M             | \$50M             | 1.7%        |
| <b>Total</b>         | <b>\$1,048M</b> | <b>\$1,924.8M</b> | <b>\$2,972.8M</b> | <b>100%</b> |

Table 1. Chinese Digital Infrastructure Investments in Central Asia (2018-2025).

Source: Ministry of Digital Development (2025); Uzbektelecom (2024); Government Procurement Portal (2022-2025). \*\*Note: Kazakhstan surveillance investment likely underestimated due to verification challenges.

Yet this modernization creates new dependencies. The deployment of 1.4 million surveillance cameras—1.3 million in Kazakhstan and 114,000-plus in Uzbekistan—enables social monitoring with systems designed for "political affairs management" according to project documentation.<sup>3</sup> Financial mechanisms including subsidized loans and CNY-denominated financing raise questions about sustainability as debt obligations accumulate and markets approach saturation.

Central Asia thus provides a critical laboratory for understanding how developing states navigate digital transformation within asymmetric relationships, where infrastructure for economic modernization becomes intertwined with mechanisms of technological dependence and social control.

### *The Research Problem: Beyond Simple Narratives*

The economic benefits appear substantial. Uzbekistan's transformation brought millions online, enabling access to e-commerce, digital finance, and education. Kazakhstan developed one of the world's most successful fintech ecosystems with near-universal 4G coverage reaching 85 percent of the population.<sup>4</sup> However, emerging constraints complicate purely optimistic assessments. Telecommunications markets approach limits. Kazakhstan's rural expansion faces low population density constraints, while Huawei's 70 percent market share limits competitive space.<sup>5</sup> Surveillance systems achieve comprehensive coverage but

require ongoing Chinese technical support, imposing significant maintenance costs.

Technology transfer has proven limited despite consistent provisions in agreements. The Kazakhstan-Huawei Innovation Center established in 2019 produced no significant patents during the study period.<sup>6</sup> Local personnel learned system management but not development capabilities, as Chinese companies retained control over critical source code and hardware designs. Financial sustainability strains emerge as Uzbekistan's \$900 million China Development Bank loan required budget support when telecommunications revenues proved insufficient, while the shift toward CNY-denominated financing creates direct exposure to Chinese monetary policy.<sup>7</sup>

### *Policy Strategy Convergence and Divergence*

Understanding these dynamics requires examining how Chinese export strategies align with Central Asian development priorities. China's Digital Silk Road addresses domestic overcapacity, expands market opportunities, and projects influence through infrastructure provision, enabling technology firms to scale internationally while establishing technical standards that create long-term dependencies.<sup>8</sup>

Kazakhstan's "Digital Kazakhstan" program welcomed foreign investment while maintaining autonomy through vendor diversification. The government maintains a 49 percent foreign ownership ceiling in telecommunications to prevent complete control while ensuring investment quality. Data localization requirements keep user information within national borders, subject to Kazakhstani law. This multi-vendor approach sees Huawei commanding 70 percent market share, with Nokia and Ericsson maintaining 20 percent and 10 percent respectively, preserving switching options.<sup>9</sup>

Uzbekistan's "Digital Uzbekistan 2030" strategy embraces comprehensive partnership, prioritizing transformation over independence.<sup>10</sup> President Mirziyoyev's administration views Chinese technologies as enabling both modernization and stability, with surveillance systems serving dual regime security and development objectives. The country's Chinese-dominant vendor strategy sees Huawei controlling 85 percent and ZTE 15 percent of telecommunications infrastructure. These divergent approaches—Kazakhstan's strategic hedging versus Uzbekistan's comprehensive integration—demonstrate that recipient state strategies significantly shape investment impacts, challenging narratives of passive technological colonization.

### *Research Questions and Analytical Framework*

This study addresses three interconnected questions. First, how do Chinese digital infrastructure investments reshape economic structures and technological capabilities in Kazakhstan and Uzbekistan, and what evidence exists regarding benefits and sustainability constraints? Second, what strategies do Kazakhstan and Uzbekistan employ to maximize benefits while managing sovereignty concerns, and how do domestic factors explain variation despite similar Chinese offerings? Third, how can we theoretically understand relationships between infrastructure dependence, technological sovereignty, and state agency during rapid digital transformation?

The analysis applies a "stratified digital sovereignty" framework building on infrastructure and sovereignty scholarship to explain how states exercise differential control across layers (physical, protocol, platform, data).<sup>11</sup> This approach resolves apparent contradictions—innovation flourishing within dependent contexts—by recognizing that sovereignty operates differently across technological layers rather than being binary.

#### *Theoretical Contributions and Empirical Approach*

The empirical analysis documents \$2.97 billion in verified investments, employing rigorous verification protocols distinguishing between announced projects, implemented investments, and operational systems. The research combines investment tracking with outcome measurement, examining transformation indicators alongside emerging constraints. Kazakhstan's GDP per capita rose from \$9,812 to \$13,247 between 2020 and 2024, while Uzbekistan's increased from \$1,724 to \$3,093. Digital economy contributions vary significantly, with Uzbekistan's dramatic expansion to 22 percent of GDP contrasting with Kazakhstan's steady 3.1 percent, reflecting different development stages and strategies.<sup>12</sup>

Policy implications prove significant across stakeholders. Central Asian governments can preserve sovereignty through layer-specific strategies while enabling development, though strategic windows may narrow as dependencies deepen. Chinese companies face sustainability challenges requiring evolution from hardware sales toward genuine partnership. Western competitors should focus on platform and service layers where local knowledge provides advantages rather than matching Chinese infrastructure pricing.<sup>13</sup> International organizations can support alternative financing, governance capacity building, and regional cooperation to strengthen recipient positions.

### *Report Structure and Analytical Progression*

This report proceeds through seven analytical sections building toward comprehensive understanding. The literature review positions research within existing scholarship while identifying gaps requiring new frameworks. The theoretical section develops the stratified sovereignty framework through synthesis. The methodology establishes credibility through transparent protocols and limitation discussions.

The empirical analysis presents findings systematically, documenting investment patterns, economic benefits, sustainability concerns, and technology transfer outcomes. The comparative analysis examines divergent strategies between Kazakhstan and Uzbekistan, demonstrating how domestic factors shape outcomes. The discussion synthesizes findings to explore broader implications for understanding digital infrastructure politics within asymmetric relationships.

Understanding these dynamics proves essential as other regions face similar technology adoption choices, market saturation intensifies, and governance challenges of dual-use infrastructure become apparent worldwide. The shift toward AI infrastructure and CNY-denominated financing signals a new phase where 2025-2027 policy choices will determine whether Central Asia maintains technological flexibility or locks into specific ecosystems permanently.

## **Literature Review**

### *Development Theory and Technology Transfer: From Linear Models to Digital Complexity*

The technology transfer debate reveals fundamental tensions between optimistic modernization narratives and structural dependency critiques, with digital infrastructure creating unprecedented analytical challenges. While Rostow (1960) positioned technology adoption as enabling "take-off" into sustained growth, dependency theorists fundamentally challenged this linear progression. Cardoso and Faletto (1979, p. 23) argued that "technological dependency creates a situation where innovation remains concentrated in core countries while periphery countries remain permanent importers of obsolete technologies." Evans' (1979) "dependent development" concept attempted synthesis by recognizing that peripheral states could achieve growth within dependent relationships, though his manufacturing focus may not translate to digital contexts where network effects create different dependency mechanisms.



Contemporary scholars increasingly document innovation within constraint. Lee (2013) and Fu et al. (2011) demonstrate through East Asian cases that technological learning and "creative adaptation" can occur within dependent relationships, while Kim's (1997) South Korean analysis reveals that successful upgrading required specific state capacities that may not exist in smaller economies. Digital infrastructure fundamentally complicates these frameworks. Plantin et al. (2018, p. 298) theorize the "platformization of infrastructure," where digital platforms become essential while traditional infrastructures operate through interfaces enabling new control mechanisms. Star's (1999, p. 380) concept of "irreversible momentum" through technical standards and Bratton's (2016) documentation of infrastructure's "dual-use capabilities" for both economic and surveillance functions reveal characteristics that neither modernization optimism nor dependency pessimism adequately captures.

### *Digital Sovereignty: Competing Paradigms and Central Asian Implications*

Digital sovereignty scholarship reveals paradigmatic differences reflecting structural positions and analytical priorities, with implications for understanding Central Asian navigation strategies. European frameworks emphasize regulatory autonomy through governance rather than technological control, exemplified by GDPR (Pohle & Thiel, 2020). Chinese conceptualizations operate from different premises, with Hong's (2017, p. 123) "网络主权" extending sovereignty into digital realms through technical architectures, while Mueller (2020) critiques this as fragmenting global connectivity—though his analysis may underestimate the model's appeal for states seeking control during rapid digitalization.

Global South scholarship provides overlooked alternatives. Avila Pinto's (2018, p. 19) analysis of Brazil's Marco Civil theorizes "strategic autonomy" as continuous navigation between great powers through regulatory and technical choices. This dynamic conception supports Couture and Toupin's (2019) sovereignty as "performance" and Milan and Treré's (2019, p. 321) "data activism" demonstrating civil society contestation within dependent frameworks. However, these approaches assume democratic accountability that may not exist in authoritarian contexts. The paradigmatic divide reflects distinct relationships to existing infrastructure: Europeans regulate platforms they cannot replace, China builds alternatives from technological strength, while Global South frameworks emphasize navigation within constraints—none directly addressing states lacking both regulatory capacity and technological capabilities.

### *Belt and Road Initiative: Beyond Debt Trap Debates*

BRI scholarship exhibits methodological disagreements producing contradictory assessments, with the "debt trap diplomacy" debate exemplifying these tensions. Brautigam's (2020, p. 2) empirical analysis finds "no evidence of deliberate debt trap diplomacy" through project-level verification revealing "mutual interests, miscalculations, and sometimes genuine efforts at debt relief." Carmody et al. (2022, p. 62) maintain that structural analysis remains essential, as infrastructure creates "path dependencies constraining future options, even without formal conditionalities." Singh's (2020) distinction between commercial and concessional financing demonstrates methodological sophistication, though may underestimate how technological dependencies operate through technical rather than debt relationships.

Digital Silk Road scholarship increasingly addresses technological specificity. Hillman (2021) documents evolution from cables to smart cities and AI platforms, while Tugendhat and Voo (2021, p. 23) find "recipient countries actively shaping deployments rather than passive acceptance," though within technological and financing constraints. Greene and Triolo (2020) reveal how technical standards carry geopolitical implications by shaping trajectories and creating dependencies. Summers' (2020, p. 810) emphasis on local actors "actively reshaping projects through negotiation, resistance, and creative adaptation" supports empirical approaches documenting implementation variations. Neither empirical verification nor structural analysis adequately explains why similar Chinese offerings produce different outcomes, suggesting need for frameworks integrating constraints with implementation analysis.

### *Surveillance Technology: Determinism versus Contextual Adaptation*

Surveillance scholarship reveals competing explanations for digital monitoring expansion, with implications for understanding Chinese technology impacts. Zuboff's (2019) "surveillance capitalism" analyzes Western corporate data extraction, while Wang and Minzner (2015, p. 345) document China's "turn toward comprehensive security" where "stability maintenance (weiwén) has become the organizing principle." Greitens et al. (2020, p. 15) demonstrate how "Chinese surveillance technology exports reflect domestic practices, particularly those developed in Xinjiang," suggesting technological determinism where systems create similar capabilities regardless of context.

Empirical studies reveal significant contextual variation challenging deterministic assumptions. Feldstein's (2019) finding that "liberal democracies are 50% more likely to deploy facial recognition systems supplied by Chinese firms than autocracies" contradicts both authoritarian diffusion theories and democratic resistance narratives. Lyon's (2018) "surveillance culture" demonstrates population-specific understanding and negotiation of

monitoring systems. Glasius et al. (2018) reveal how authoritarian control affects both deployment and scholarly access, while Heydemann and Leenders' (2011) authoritarian learning framework shows regimes adapting technologies rather than adopting uniform models—supporting contextual adaptation while acknowledging limited resistance scope in authoritarian settings.

### *Central Asian Studies: Methodological Contributions and Digital Infrastructure Gaps*

Regional scholarship provides valuable empirical foundations while revealing analytical limitations. Yau's (2020) operational BRI analysis systematically documents projects but potentially privileges Chinese categories over recipient perspectives. Indeo (2020) reveals complex multilateral relationships beyond simple bilateral frameworks, though geopolitical focus may underestimate technological dependency mechanisms. Recent innovations include Maracchione and Jardine's (2024) machine learning analysis of Chinese policy discourse and Zhang's (2024) examination of perception formation, though these emphasize Chinese perspectives over implementation outcomes.

The literature reveals systematic gaps in digital infrastructure analysis. While Li-Chen Sim and Aminjonov (2020) document traditional infrastructure challenges including transparency and debt, and the *Journal of Infrastructure, Policy and Development* (2018) provides technical foundations, comprehensive documentation of telecommunications (63.9% of investments) and surveillance systems (34.4%) remains absent. Shamiev's (2020) mining sector analysis of "lock-in processes" suggests analytical approaches, though extractive dynamics may not translate to digital contexts where dependencies operate through standards rather than resource control.

### *Synthesis: Theoretical Convergence and Empirical Requirements*

The literature converges around rejecting binary dependence-autonomy frameworks while exposing persistent empirical gaps. Across development studies, sovereignty literature, BRI scholarship, and surveillance studies, scholars increasingly recognize complex navigation dynamics within structural constraints. Evans' dependent development, Avila Pinto's strategic autonomy, Summers' implementation variation, and Lyon's cultural adaptation all emphasize agency within structure. However, theoretical sophistication has not produced empirical synthesis—development studies emphasize economic outcomes, surveillance studies focus on control, and geopolitical analyses examine competition without systematic integration.

Methodological disagreements compound challenges, with empirical verification and structural analysis producing contradictory conclusions about identical

phenomena. Regional studies rely on announced rather than implemented outcomes, aggregate rather than project-level analysis, and single-country rather than comparative approaches. Our analysis addresses these limitations through systematic documentation across Kazakhstan and Uzbekistan, applying established theoretical insights to digital contexts using verified project-level data. This approach extends scholarship by testing how frameworks developed for different contexts apply to Chinese digital infrastructure in Central Asian settings, supporting nuanced understanding of contemporary infrastructure politics where technological dependencies operate through standards and capabilities rather than traditional debt or resource control mechanisms.

## **Methodology and Data**

### *Research Design and Case Selection*

This study employs qualitative comparative case study methodology following Przeworski and Teune's (1970) "most similar systems design" to examine Chinese digital infrastructure investments in Kazakhstan and Uzbekistan from 2018-2025. Building on Beach and Pedersen's (2013) process tracing methodology, the analysis identifies causal mechanisms linking investments to sovereignty outcomes through systematic examination of implementation processes and documented outcomes.

Kazakhstan and Uzbekistan provide controlled comparison through four shared characteristics that enable analytical leverage. Both gained independence from the Soviet Union in 1991, maintain authoritarian governance systems with identical Freedom House scores of 12/100 in 2024, depend on hydrocarbon exports as primary revenue sources, and joined China's Belt and Road Initiative between 2013 and 2014. Their economic variation provides explanatory power for understanding differential outcomes. Kazakhstan's GDP per capita reached \$14,005 in 2024 compared to Uzbekistan's \$3,093, with total economies of \$288.41 billion and \$114.97 billion respectively according to World Bank data.<sup>1</sup> This income differential of 4.5 to 1 enables examination of how economic capacity shapes digital infrastructure adoption patterns and negotiation strategies.

### *Data Collection and Three-Stage Verification Protocol*

#### *Investment Database Construction*

Primary documentation for investment tracking encompassed multiple official sources across governmental, corporate, and multilateral institutions. Government procurement portals provided tender documentation and contract

details, including Kazakhstan's [digitalkazakhstan.kz](http://digitalkazakhstan.kz) and [stat.gov.kz](http://stat.gov.kz) platforms alongside Uzbekistan's [mitc.uz](http://mitc.uz) and [statistics.uz](http://statistics.uz) systems. Corporate documentation included annual reports from Huawei Technologies covering 2018 through 2024, ZTE Corporation financial statements and investor relations materials, and Alibaba Group SEC filings that detailed regional investment allocations. Multilateral development banks provided project verification through detailed documentation, particularly Asian Infrastructure Investment Bank Project Number 000758 for Uzbekistan's Fixed Broadband Expansion and World Bank Project P171683 for Kazakhstan Digital Acceleration. Policy frameworks established through Kazakhstan's "Digital Kazakhstan" State Program adopted through Government Resolution Number 827 on December 12, 2017, and Uzbekistan's "Digital Uzbekistan 2030" strategy announced through Presidential Decree UP-6079 on October 5, 2020, provided strategic context for investment priorities.<sup>2</sup>

### *Three-Stage Verification Requirements*

Following Glasius et al.'s (2018) methodology for conducting research in authoritarian field environments, this study implemented conservative verification protocols requiring multiple independent sources for each investment claim. The verification process proceeded through three distinct stages designed to ensure data reliability while acknowledging the opacity inherent in infrastructure investments involving dual-use technologies.

Stage one involved initial identification through systematic scanning of government announcements, media reports, corporate press releases, and bilateral cooperation agreements. This comprehensive search yielded over fifty potential investments ranging from \$5 million equipment purchases to \$1.2 billion infrastructure programs. Stage two required corporate confirmation through matching each potential project with annual reports, SEC filings, or verified executive statements from involved companies. Uzbekistan's Safe City project exemplifies this verification process, moving from initial media identification in Eurasianet's September 2019 reporting through corporate confirmation in Huawei's 2019 Annual Report to implementation verification via government procurement portal documentation and UN Human Rights Committee reporting in 2020.<sup>3</sup> This corporate verification stage eliminated thirty-four of fifty initially identified projects, representing a 68 percent exclusion rate due to insufficient documentation.

Stage three demanded implementation evidence through tender documents, technical specifications, or independent verification from international organizations or financial institutions. This final verification stage reduced the database to sixteen projects totaling \$2.97 billion in confirmed

investments, representing documented minimum investment levels achieved through conservative estimation protocols that excluded any investments lacking multiple forms of verification.

### *Process Tracing Framework*

The analysis applies four-stage process tracing to establish causal chains linking Chinese investments to documented outcomes in both countries. Antecedent conditions examination documents specific infrastructure deficits through government statistics, including Kazakhstan's 4G coverage expansion from 68 percent in 2018 to 85 percent by 2024 and Uzbekistan's growth from 31 percent to 67 percent according to official telecommunications ministry data.<sup>4</sup> Policy frameworks emerge through analysis of bilateral cooperation agreements and memoranda of understanding, while political economy contexts become visible through examination of budget allocations and development priorities articulated in official planning documents.

Investment decision analysis traces financing mechanisms through examination of loan agreements, commercial contracts, and vendor financing arrangements documented in corporate filings and government procurement records. Technology selection processes reveal themselves through tender specifications and procurement requirements published on government portals, while local partner identification demonstrates political connections through joint venture agreements and partnership announcements in official media. Implementation process tracking follows projects from agreement signature to operational deployment through regulatory documentation, technical deployment evidence from government reporting, and workforce development programs documented in corporate sustainability reports and bilateral education agreements. Outcome assessment employs multiple quantitative indicators including network coverage statistics from telecommunications ministries, economic indicators from national statistical offices, and governance changes documented through policy implementation reports and international organization assessments.

### *Access Constraints and Research Limitations*

Following Glasius et al.'s (2018, p. 25) guidance on navigating "between the Scylla of self-censorship and the Charybdis of endangering sources," this study relied on systematic document analysis of publicly available sources rather than direct engagement with governmental or corporate decision-makers.<sup>5</sup> Access to governmental archives and internal corporate documentation remained restricted due to the sensitive nature of digital infrastructure projects involving dual-use surveillance technologies, necessitating reliance on publicly disclosed information.



Several investment categories remain unverified despite evidence suggesting their significance for understanding total Chinese engagement. Data center investments show substantial operational deployment but lack publicly disclosed financial amounts in corporate reports or government documentation. Payment infrastructure investments, particularly UnionPay's expansion achieving 100 percent merchant acceptance targets in both countries, remain confidential under commercial arrangements between financial institutions. Security sector investments face classification restrictions preventing financial disclosure, with only Kazakhstan's \$23 million Almaty facial recognition system achieving verification despite documented deployment of 1.3 million cameras nationwide and over 114,000 cameras in Uzbekistan. Operational expenditures remain within confidential maintenance contracts between Chinese vendors and local operators, while technology transfer valuations remain unavailable due to intellectual property protections and competitive sensitivity claims.

Following Fujii's (2018, p. 12) principle of "transparency about the limits of transparency," this study explicitly acknowledges these constraints while maximizing analytical leverage from available documentary evidence.<sup>6</sup> The \$2.97 billion in verified investments represents documented minimum levels, with total Chinese digital infrastructure investment likely reaching substantially higher amounts when including unverified categories. This conservative approach ensures reliability of included data while establishing clear boundaries for empirical claims, strengthening analytical credibility by preventing overextension beyond available evidence while acknowledging constraints inherent in researching opaque investment flows in authoritarian contexts.

## Results and Discussion

### *Investment Patterns and Economic Transformation*

The verified \$2.97 billion in Chinese digital infrastructure investments across sixteen projects reveals allocation patterns that reflect political receptivity rather than market logic. Uzbekistan received \$1.93 billion (65 percent) despite its economy being one-quarter the size of Kazakhstan's, which received \$1.05 billion (35 percent). This asymmetric distribution extends Nordin and Weissmann's (2018) framework on recipient state agency, demonstrating how domestic political calculations shape investment flows beyond pure economic rationality.

| Category         | Kazakhstan       | Uzbekistan       | Analysis                 |
|------------------|------------------|------------------|--------------------------|
| Total Investment | \$1.05B<br>(35%) | \$1.93B<br>(65%) | Political<br>receptivity |



|                           |                                           |                        |                                                                              |
|---------------------------|-------------------------------------------|------------------------|------------------------------------------------------------------------------|
| <b>Telecommunications</b> | \$1.03B                                   | \$875M                 | over market size<br>Kazakhstan's 5G focus vs Uzbekistan's coverage expansion |
| <b>Surveillance</b>       | \$23M verified*                           | \$1.00B                | Divergent sovereignty-security priorities                                    |
| <b>Primary Projects</b>   | 5G Network (\$975M)                       | Safe (\$1B)            | City Infrastructure vs control emphasis                                      |
| <b>Vendor Mix</b>         | Huawei 70%,<br>Nokia 20%,<br>Ericsson 10% | Huawei 85%,<br>ZTE 15% | Hedging vs integration                                                       |

Table 1. Chinese Digital Infrastructure Investment Patterns (2018-2025)

Source: Government procurement portals; corporate annual reports (2018-2024). \*\*Note: Kazakhstan surveillance likely underestimated; 1.3 million cameras deployed suggests higher investment.

The sectoral concentration in telecommunications (63.9 percent) and surveillance systems (34.4 percent) indicates prioritization of control-enabling technologies alongside connectivity infrastructure. Temporal patterns reveal three phases: experimental pilots (2018-2020, \$623 million), acceleration (2021-2023, \$1.74 billion), and strategic deepening emphasizing AI capabilities (2024-2025, \$607 million). This progression demonstrates how initial cautious engagement evolved into comprehensive digital transformation commitments once early projects proved successful.

Both countries achieved remarkable economic transformation despite different strategic approaches. Kazakhstan's digital economy reached \$2.3 billion (3 percent of GDP) with cashless transactions increasing from 45 percent to 85 percent between 2020-2024. More dramatically, Uzbekistan's digital economy expanded from 2 percent to 22 percent of GDP during the same period, with IT services exports growing twenty-two-fold to \$344 million. These metrics demonstrate how infrastructure investment enables economic

modernization regardless of sovereignty approach, though with different dependency implications examined below.

### *Strategic Divergence: Hedging versus Integration*

Kazakhstan and Uzbekistan's contrasting approaches to Chinese digital infrastructure reveal conscious sovereignty calculations shaped by distinct regime priorities and geopolitical constraints. These strategies cannot be explained through simple cost-benefit analysis but reflect deeper political economy factors that determine how states navigate technological dependencies.

Kazakhstan's multi-vector hedging strategy accepts technological dependence while preserving strategic flexibility through institutional design. The \$975 million 5G framework mandates multi-vendor deployment despite coordination costs estimated at 15-20 percent above single-vendor solutions. Kazakhtelecom's retention of network ownership under the 49 percent foreign ownership ceiling demonstrates how legal frameworks preserve control despite technological dependence. Data localization requirements ensure user information remains subject to Kazakhstani rather than Chinese law, while the Trans-Caspian Fiber cable's redundant routing through Azerbaijan and Georgia prevents exclusive reliance on any single partner.

Uzbekistan pursues accelerated integration, embracing comprehensive Chinese partnership to achieve rapid modernization while subordinating sovereignty concerns to development imperatives. The \$1 billion Safe City program with explicit "political affairs management" modules represents conscious acceptance of surveillance capabilities in exchange for social stability tools. The MobiuZloan arrangement (\$150 million) with mandatory Huawei equipment and Chinese technical personnel illustrates how Uzbekistan intentionally creates dependencies to accelerate transformation. This approach enabled the digital economy's expansion from 2 percent to 22 percent of GDP in four years—transformation that might otherwise require decades.

| Dimension                     | Kazakhstan         | Uzbekistan     | Implications                      |
|-------------------------------|--------------------|----------------|-----------------------------------|
| <b>Digital Economy Growth</b> | 2.8% → 3.1% GDP    | 2% → 22% GDP   | Speed vs sustainability trade-off |
| <b>Internet Penetration</b>   | 76% → 86%          | 47% → 67%      | Gradual vs rapid expansion        |
| <b>Platform Success</b>       | Kaspi.kz (\$17.5B) | Uzum (\$1.16B) | Both achieved                     |

|                                |                           |                            |                                                  |
|--------------------------------|---------------------------|----------------------------|--------------------------------------------------|
| <b>Surveillance Deployment</b> | 1.3M cameras (resistance) | 114K+ cameras (acceptance) | unicorn status<br>Civil society capacity differs |
| <b>Technology Transfer</b>     | Limited patents           | Operational training       | Neither achieved genuine transfer                |

*Table 2. Comparative Strategic Outcomes*

*Source: National statistical offices; corporate valuations; government reports (2024-2025).*

These divergent approaches reflect different risk assessments shaped by structural factors. Kazakhstan's 7,000-kilometer border with China creates immediate security concerns about technological dependence. Its established Western investment relationships (\$23.4 billion in U.S. foreign direct investment) create reputational incentives for maintaining sovereignty credentials. Conversely, Uzbekistan's post-Karimov development urgency and limited alternative financing create imperatives for rapid transformation that override sovereignty concerns. The absence of meaningful civil society resistance enables comprehensive surveillance deployment that Kazakhstan's more open political environment constrains.

#### *Innovation Within Dependence: Platform Success Stories*

The emergence of billion-dollar platforms challenges technological determinism by demonstrating innovation possibilities within infrastructure dependencies. Kazakhstan's Kaspi.kz achieved a \$17.5 billion valuation with fourteen million active users (70 percent of population) while operating entirely on Chinese telecommunications infrastructure. This success resulted from regulatory protection, government promotion, and strategic positioning in financial services where local knowledge provides competitive advantages over foreign platforms.

Uzbekistan's Uzum platform reached \$1.16 billion valuation within eighteen months, demonstrating how rapid infrastructure deployment can accelerate platform development. The comprehensive Chinese infrastructure foundation enabled indigenous innovation that would typically require years of gradual development. Both cases validate the stratified sovereignty framework by showing that infrastructure dependence does not

automatically eliminate platform-layer innovation when supported by appropriate state strategies.

However, technology transfer promises remain largely unfulfilled despite bilateral commitments. Training programs emphasize operational capacity rather than innovation development. Huawei certified 100,000 specialists in Kazakhstan, but focused on network operation rather than system design. Core technologies including algorithms, security protocols, and system architectures remain within Chinese vendor control. The Kazakhstan-Huawei Innovation Center established in 2019 produced no significant patents during the study period. This pattern reflects global practices protecting intellectual property while meeting contractual obligations for capacity building, but fundamentally limits technological sovereignty development.

### *Sustainability Constraints and Future Trajectories*

Despite documented benefits, emerging constraints suggest limits to continued growth trajectories. Kazakhstan's telecommunications market approaches saturation with 85 percent 4G coverage, as remaining areas feature population densities below three people per square kilometer making expansion economically unviable. Surveillance deployment faces operational challenges as maintenance costs for 1.3 million cameras strain budgets while public resistance, exemplified by facial recognition deactivation following 2023 protests, constrains expansion.

Uzbekistan confronts different sustainability challenges despite enthusiastic technology adoption. The planned surveillance expansion to 200,000 cameras requires substantial operational budgets competing with social spending priorities. The \$900 million China Development Bank loan creates debt service obligations, while currency exposure through CNY-denominated financing introduces exchange rate risks. Both countries face technology obsolescence pressures as the anticipated 6G transition will require substantial new investments potentially exceeding fiscal capacity.

| Challenge         | Current Status              | Policy Response                       | Future Risk                       |
|-------------------|-----------------------------|---------------------------------------|-----------------------------------|
| Market Saturation | 85% coverage (KZ), 67% (UZ) | Shift service optimization            | to Diminishing investment returns |
| Debt Obligations  | \$900M loan (UZ)            | CDB Seeking multilateral alternatives | Currency exposure via CNY         |

|                           |                           |                                 |                           |
|---------------------------|---------------------------|---------------------------------|---------------------------|
| <b>Surveillance Costs</b> | 15-20% annual maintenance | Budget reallocation pressure    | Civil society resistance  |
| <b>Technology Lock-in</b> | 5G standards adopted      | Multi-vendor strategy (KZ only) | 6G transition constraints |
| <b>Innovation Gaps</b>    | Limited patent production | Platform protection policies    | Continued dependency      |

Table 3. Sustainability Indicators and Policy Implications

Source: Government budget documents; technical assessments; author calculations (2024-2025).

## Policy Implications and Recommendations

### *Critical Juncture and Strategic Imperatives*

The 2025-2027 period represents a critical juncture as both Kazakhstan and Uzbekistan face decisions about 6G adoption, AI governance, and surveillance expansion that will create path dependencies lasting decades. The deployment of 1.4 million surveillance cameras without comprehensive privacy frameworks creates dangerous precedents requiring urgent policy attention before capabilities become further entrenched. Kazakhstan's hedging approach preserves options for technology transitions and regional cooperation, while Uzbekistan's integration creates switching costs that may lock in Chinese standards permanently. These divergent experiences with \$2.97 billion in Chinese digital infrastructure provide concrete lessons for strategic technology governance.

Central Asian governments should formalize sovereignty-preserving strategies through specific policy instruments adapted to their current positions. Kazakhstan must codify its implicit multi-vendor requirements through procurement regulations mandating minimum percentages from non-Chinese suppliers in critical infrastructure, similar to India's 2020 telecommunications reforms requiring 30 percent trusted vendor sourcing. The country's successful maintenance of vendor diversity despite 15-20 percent efficiency costs demonstrates that such strategies remain economically viable. Uzbekistan, having already accepted comprehensive Chinese integration, should maximize technology transfer within existing relationships by establishing joint research centers with enforceable patent-sharing agreements, following Vietnam's model where Samsung's \$17 billion investment included mandatory

technology transfer resulting in 200 local supplier companies by 2023. Both countries urgently need comprehensive data governance frameworks—Estonia's Data Protection Inspectorate model provides a tested framework combining technical auditing with citizen advocacy, adaptable to authoritarian contexts through phased implementation beginning with government data before expanding to private sector coverage.

### *International Engagement and Regional Cooperation*

Competition with Chinese digital infrastructure proves most viable at platform and service layers where local knowledge provides sustainable advantages, as demonstrated by Kaspi.kz's \$17.5 billion valuation achieved while operating on Huawei infrastructure. International development organizations must recalibrate strategies recognizing that Chinese dominance at physical infrastructure layers appears irreversible given demonstrated cost advantages and deployment speed. The European Union's Global Gateway initiative, with €300 billion promised for digital infrastructure, should prioritize governance capacity building—particularly algorithmic transparency and privacy-preserving authentication systems—rather than attempting to match Chinese hardware investments. The United States International Development Finance Corporation's \$500 million digital infrastructure commitment should focus on areas where Chinese companies face structural disadvantages, particularly enterprise software and cybersecurity services requiring deep Western system integration.

Regional cooperation mechanisms prove more effective than individual strategies for managing technological dependencies. The proposed Central Asian Digital Common Market could enable collective bargaining that individual states cannot achieve, similar to how the African Union's Digital Transformation Strategy 2020-2030 created continental frameworks for engaging with technology powers. Critical coordination needs include joint negotiation of 6G technical standards through existing Shanghai Cooperation Organization mechanisms, collective approaches to AI governance preventing regulatory arbitrage, and shared frameworks for cross-border data flows balancing security with economic integration. Regional development banks should establish dedicated facilities for refinancing Chinese infrastructure loans approaching maturity, as Sri Lanka's recent \$3 billion IMF program demonstrates how strategic refinancing can reduce dependency while maintaining infrastructure benefits. Supporting these mechanisms requires acknowledging that developing states rationally choose Chinese technologies for legitimate development objectives—Kazakhstan's explicit premium for vendor diversity and Uzbekistan's acceptance of surveillance systems represent conscious sovereignty calculations that external actors must respect while offering alternatives. The goal should not be eliminating Chinese

technology but ensuring Central Asian states maintain sufficient alternatives to preserve strategic autonomy during critical technological transitions ahead.

## Conclusion

This analysis of \$2.97 billion in Chinese digital infrastructure investments across Kazakhstan and Uzbekistan demonstrates that developing states exercise greater agency in shaping technological futures than dependency theories suggest, though within structural constraints that increasingly define available options. The stratified digital sovereignty framework reveals how states manage differential control across technological layers rather than facing binary choices between development and autonomy—Kazakhstan's strategic hedging preserves future flexibility at the cost of efficiency, while Uzbekistan's accelerated integration achieves rapid transformation at the price of deeper dependencies. Both countries achieved remarkable economic benefits, with Uzbekistan's digital economy expanding from 2 percent to 22 percent of GDP and Kazakhstan's Kaspi.kz achieving a \$17.5 billion valuation, proving that infrastructure dependence need not eliminate innovation when supported by appropriate regulatory frameworks and state strategies. Yet the deployment of 1.4 million surveillance cameras without comprehensive privacy governance, the limited technology transfer despite bilateral promises, and the approaching market saturation in telecommunications reveal sustainability challenges that will intensify during the critical 2025-2027 period when 6G standards emerge and current infrastructure loans mature. Central Asia's experience provides essential insights for other developing regions engaging with dominant technological powers, demonstrating that early infrastructure decisions create path dependencies lasting decades, that platform-layer competition remains viable despite infrastructure dependence, and that regional cooperation mechanisms offer more effective sovereignty preservation than individual state strategies. As digital infrastructure increasingly determines economic competitiveness and state capacity globally, understanding these complex trade-offs between immediate development benefits and long-term sovereignty implications becomes crucial for both scholarly analysis and policy practice, particularly as the window for maintaining technological flexibility rapidly narrows in our increasingly interconnected yet fragmented digital world.



## Bibliography

- Asian Infrastructure Investment Bank. (2025, January). Project #000758: Uzbekistan fixed broadband expansion project. AIIB Project Database.
- Asan Forum. (2024). China's strategic thinking toward Central Asia, 2013–2024. *The Asan Forum*, 12(3), 15–42. <https://theasanforum.org/chinas-strategic-thinking-toward-central-asia-2013-2024/>
- Astana Times. (2025, January 29). National Bank: Kazakhstan's cashless payments surge to over 85% in 2024. <https://astanatimes.com/2025/01/national-bank-kazakhstans-cashless-payments-surge-to-over-85-in-2024/>
- Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? *Sur International Journal on Human Rights*, 15(27), 15–27. <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>
- Beach, D., & Pedersen, R. B. (2013). *Process-tracing methods: Foundations and guidelines*. University of Michigan Press. [https://www.researchgate.net/publication/287260232\\_Process-Tracing\\_Methods\\_Foundations\\_and\\_Guidelines](https://www.researchgate.net/publication/287260232_Process-Tracing_Methods_Foundations_and_Guidelines)
- Blanchard, J.-M. F., & Flint, C. (2017). The geopolitics of China's Belt and Road Initiative. *Eurasian Geography and Economics*, 58(3), 223–243. [10.4324/9781032616001](https://doi.org/10.4324/9781032616001)
- Bratton, B. H. (2016). *The stack: On software and sovereignty*. MIT Press. <https://observatory.constantvzw.org/books/benjamin-h-bratton-the-stack-on-software-and-sovereignty-2.pdf>
- Brautigam, D. (2020). A critical look at Chinese 'debt-trap diplomacy': The rise of a meme. *Area Development and Policy*, 5(3), 1–14. [10.1080/23792949.2019.1689828](https://doi.org/10.1080/23792949.2019.1689828)
- Cardoso, F. H., & Faletto, E. (1979). *Dependency and development in Latin America*. University of California Press. <http://www.rochelleterman.com/ComparativeExam/sites/default/files/Bibliography%20and%20Summaries/Cardoso%201972.pdf>
- Carmody, P., Taylor, I., & Zajontz, T. (2022). China's spatial fix and 'debt-trap diplomacy' in Africa: Constraining belt or road to development? *Political Geography*, 92, 102497. <https://doi.org/10.1016/j.polgeo.2022.102497>
- Couture, S., & Toupin, S. (2019). What does the notion of 'sovereignty' mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch*. Yale University Press. <https://yalebooks.yale.edu/book/9780300233070/the-internet-in-everything/>
- Eurasianet. (2019, September). Uzbekistan: Surveillance state takes shape.

- Evans, P. (1979). *Dependent development: The alliance of multinational, state, and local capital in Brazil*. Princeton University Press. <https://press.princeton.edu/books/paperback/9780691021850/dependent-development?srltid=AfmBOorZ1u7X9aUN9q3D0qvli4hHceE6eSMdYnfzI4GPrgjbAiwAmAPC>
- Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance>
- Florini, A. (2019). *The coming democracy: New rules for running a new world*. Island Press. [10.2307/20033695](https://doi.org/10.2307/20033695)
- Freedom House. (2024a). *Freedom in the world 2024: Kazakhstan*. <https://freedomhouse.org/country/kazakhstan/freedom-world/2024>
- . (2024b). *Freedom in the World 2024: Uzbekistan*. <https://freedomhouse.org/country/uzbekistan/freedom-world/2024>
- . (2024c). *Nations in transit 2024: Uzbekistan*. <https://freedomhouse.org/country/uzbekistan/nations-transit/2024>
- Fu, X., Pietrobelli, C., & Soete, L. (2011). The role of foreign technology and indigenous innovation in the emerging economies. *World Development*, 39(7), 1204–1212. <https://doi.org/10.1016/j.worlddev.2010.05.009>
- Fujii, L. A. (2018). *Interviewing in social science research: A relational approach*. Routledge.
- Gazeta.uz. (2024, April 17). Freedom House: Democracy score in Central Asia continues to decline. <https://www.gazeta.uz/en/2024/04/16/freedom-house/>
- Glasius, M., de Lange, M., Bartman, J., Dalmasso, E., Del Sordi, A., Lv, A., Michaelsen, M., & Ruijgrok, K. (2018). *Research, ethics and risk in the authoritarian field*. Palgrave Macmillan.
- Government of Kazakhstan. (2017). *Digital Kazakhstan state program* (Resolution No. 827).
- Government of Uzbekistan. (2020). *Digital Uzbekistan 2030* (Presidential Decree No. UP-6079).
- Greene, R., & Triolo, P. (2020). *Will China control the global internet via its digital silk road?* Carnegie Endowment for International Peace.
- Greitens, S. C., Lee, M., & Yazici, E. (2020). Counterterrorism and preventive repression: China's changing strategy in Xinjiang. *International Security*, 44(3), 9–47.

- Heydemann, S., & Leenders, R. (2011). Authoritarian learning and authoritarian resilience: Regime responses to the 'Arab Awakening.' *Globalizations*, 8(5), 647–663.
- Hillman, J. E. (2021). *The digital silk road: China's quest to wire the world and control the future*. Harper Business.
- Hong, Y. (2017). *Networking China: The digital transformation of the Chinese economy*. University of Illinois Press.
- Huawei Investment & Holding Co., Ltd. (2019). *Annual report 2018*. Huawei.
- . (2020). *Annual report 2019*. Huawei.
- . (2021). *Annual report 2020*. Huawei.
- . (2022). *Annual report 2021*. Huawei.
- . (2023). *Annual report 2022*. Huawei.
- . (2024). *Annual report 2023*. Huawei.
- . (2025). *Annual report 2024*. Huawei.
- Indeo, F. (2020). China-Russia cooperation within the BRI framework: Partnership dynamics and perspectives. *International Political Economy*, 27(2), 230–250.
- Journal of Infrastructure, Policy and Development. (2018). Special issue: Belt and Road Initiative (BRI): Enhancing ICT connectivity in China–Central Asia corridor. *Journal of Infrastructure, Policy and Development*, 2(1).
- Keohane, R. O., & Nye, J. S. (2011). *Power and interdependence* (4th ed.). Longman.
- Kim, L. (1997). *Imitation to innovation: The dynamics of Korea's technological learning*. Harvard Business School Press.
- Kun.uz. (2025, February 10). Uzbekistan's GDP reached \$115 billion in 2024. <https://kun.uz/en/news/2025/02/10/uzbekistans-gdp-reached-115-billion-in-2024>
- Lee, K. (2013). *Schumpeterian analysis of economic catch-up: Knowledge, path-creation, and the middle-income trap*. Cambridge University Press.
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.
- Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*, 25(2), 185–213.
- Maracchione, M., & Jardine, B. (2024). Central Asian studies in the People's Republic of China: A structural topic model analysis. *Central Asian Survey*, 43(1), 45–67.
- Milan, S., & Treré, E. (2019). Big data from the South(s): Beyond data universalism. *Television & New Media*, 20(4), 319–335.
- Mueller, M. (2020). Against sovereignty in cyberspace. *International Studies Review*, 22(4), 779–801.
- Nordin, A. H. M., & Weissmann, M. (2018). Will Trump make China great again? The Belt and Road Initiative and international order. *International Affairs*, 94(2), 231–249.

- Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293–310.
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 1–19.
- Przeworski, A., & Teune, H. (1970). *The logic of comparative social inquiry*. Wiley-Interscience.
- Reuters. (2024, January 19). Kaspi.kz commands \$17.5 bln valuation in Nasdaq debut.
- Rostow, W. W. (1960). *The stages of economic growth: A non-communist manifesto*. Cambridge University Press.
- Shamiev, A. (2020). Chinese political and lending conditionality in Tajikistan's mining sector: Lock-in processes and dependency creation. *Eurasian Geography and Economics*, 61(2), 110–135.
- Sim, L.-C., & Aminjonov, F. (2020). Central Asia's importance for SREB success: Challenges and opportunities. *Asian Survey*, 60(1), 85–109.
- Singh, A. (2020). Belt and Road Initiative and debt sustainability: A new framework for analysis. *China & World Economy*, 28(5), 129–148.
- Srnicek, N. (2017). *Platform capitalism*. Polity Press.
- Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, 43(3), 377–391.
- State Council of the People's Republic of China. (2022, January 12). *14th five-year plan for digital economy development*.
- Summers, T. (2016). China's 'new silk roads': Sub-national regions and networks of global political economy. *Third World Quarterly*, 37(9), 1628–1643.
- . (2020). Negotiating the boundaries of China's Belt and Road Initiative. *Environment and Planning C: Politics and Space*, 38(5), 809–813.
- TAdviser. (2024). *ICT market of Uzbekistan*.
- Trading Economics. (2025, February). Kazakhstan GDP. <https://tradingeconomics.com/kazakhstan/gdp>
- . (2025, February). Kazakhstan GDP per capita. <https://tradingeconomics.com/kazakhstan/gdp-per-capita>
- . (2025, February). Uzbekistan GDP. <https://tradingeconomics.com/uzbekistan/gdp>
- Tugendhat, H., & Voo, J. (2021). *China's global AI exports: Technology distribution and data safety*. Oxford Information Labs.
- United Nations Human Rights Committee. (2020). *Reports on surveillance system implementation*. United Nations.
- Wang, Yiwei. (2016). Offensive for defensive: The Belt and Road Initiative and China's new grand strategy. *The Pacific Review*, 29(3), 455–463.
- Wang, Yuhua, & Minzner, C. (2015). The rise of the Chinese security state. *The China Quarterly*, 222, 339–359.

- World Bank. (2025, February). Kazakhstan overview: Development news, research, data. <https://www.worldbank.org/en/country/kazakhstan/overview>
- . (2025, January). Project P171683: Kazakhstan digital acceleration. World Bank Project Database.
- . (2025, February). Uzbekistan overview: Development news, research, data. <https://www.worldbank.org/en/country/uzbekistan/overview>
- Worldometer. (2025, February). Kazakhstan GDP. <https://www.worldometers.info/gdp/kazakhstan-gdp/>
- . (2025, February). Uzbekistan GDP. <https://www.worldometers.info/gdp/uzbekistan-gdp/>
- Yau, J. (2020). Operational analysis of BRI implementation from 2013–2019: Framework mapping across five cooperation priorities. *China Quarterly of International Strategic Studies*, 6(2), 140–160.
- Zhang, L. (2024). Central Asia in China's strategic mirror: Perception formation and policy implications. *Asian Affairs*, 55(1), 78–95.
- ZTE Corporation. (2018–2024). *Financial statements and investor relations materials, 2018–2024*. ZTE Corporation.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

# ЦИФРОВОЕ НЕРАВЕНСТВО КАК ИНСТРУМЕНТ ГЕОПОЛИТИЧЕСКОГО ВОЗДЕЙСТВИЯ: ПРАВОВЫЕ И ПУБЛИЧНО-ПОЛИТИЧЕСКИЕ ПОСЛЕДСТВИЯ ВЛИЯНИЯ КИТАЙСКИХ ТЕХНОЛОГИЙ В ЦЕНТРАЛЬНОЙ АЗИИ

Шаймарданова Дилафруз Дилмуратовна, Ташкентского государственного юридического университета

## Аннотация

*Статья посвящена изучению вопроса о том, как цифровое неравенство в Центральной Азии может быть использовано для достижения геополитических целей, в частности, для усиления технологического влияния Китая в регионе.*

*Центральное место в исследовании занимает анализ механизмов формирования этой зависимости: от сравнительного анализа моделей технологического партнерства, предлагаемых КНР, ЕС и США, до ключевой правовой коллизии, при которой национальные законы о локализации данных вступают в противоречие с экстерриториальным законодательством Китая о разведке.*

*Эта динамика демонстрируется на примере реализации инфраструктурных проектов КНР, таких как «умные города». В заключение автор оценивает риски текущей модели партнерства для национальной безопасности и предлагает ряд политических рекомендаций по их минимизации*

## Введение

### **Актуальность исследования**

Цифровая трансформация критически важна для социально-экономического прогресса Центральной Азии, однако цифровое неравенство в регионе создает геополитическую уязвимость, которая активно используется внешними акторами, как инструмент влияния. В попытке преодолеть технологическое неравенство, страны региона вынуждены опираться на комплексные решения от развитых государств, что порождает структурную зависимость и риски для национальной безопасности.

Научная новизна данной работы заключается в анализе цифрового неравенства не как сугубо технической или экономической проблемы, но и как фактор, играющий роль в геополитическом влиянии внешних доноров.



В центре исследования находится анализ правовых и публично-политических последствий технологического присутствия Китая, который использует эту уязвимость для формирования долгосрочной зависимости

### ***Проблема исследования***

В попытке преодолеть цифровое неравенство в своем регионе, страны Центральной Азии осознают масштаб стоящих перед ними задач, которые сложно решить самостоятельно. Для их эффективного решения им приходится опираться на поддержку более развитых государств, способных предложить комплексные и оперативные решения.

Однако такой подход ведет к зависимости, порождая при этом новые уязвимости и потенциальные риски для национальной безопасности.

*Цель исследования:* состоит в том, чтобы провести комплексный анализ правовых и публично-политических последствий технологического присутствия Китая и его инициатив в Центральной Азии, а также оценить, как использование цифрового неравенства может служить инструментом геополитического влияния на регион.

*Задачи исследования:*

- Проанализировать теоретические основы цифрового неравенства как геополитического феномена
- Исследовать эволюцию китайского технологического присутствия в Центральной Азии
- Сравнить модели технологического сотрудничества КНР, ЕС и США в регионе
- Оценить правовые и политические риски технологической зависимости
- Разработать рекомендации по минимизации негативных последствий

### **Обзор литературы**

Цифровая трансформация в Центральной Азии, происходящая на фоне геополитической конкуренции, представляет собой одну из самых сложных и обсуждаемых тем в сфере международных отношений. Несмотря на рост количества исследований в этой области, среди ученых нет единого мнения о том, как найти баланс между выгодами от технологического прогресса и рисками, связанными с цифровой зависимостью.

Современное понимание цифрового неравенства вышло за рамки простого доступа к технологиям. Исследования Яна Ван Дейка и Александра Ван Дейрсена показывают, что истинный разрыв кроется в отсутствии навыков и стратегических компетенций. Для Центральной Азии это означает, что нехватка цифровой грамотности превращает страны региона в пассивных потребителей технологий, создавая фундаментальную уязвимость.



И эта уязвимость открывает двери для того, что Ник Коулдри и Улиес Мехиас называют «колонизацией данных». В условиях, когда данные, по выражению Клайва Хамби, стали «новой нефтью», борьба за ресурсы трансформировалась в борьбу за контроль над информацией. Таким образом, технологическое отставание напрямую ведет к риску потери суверенитета над национальными данными.

Конкуренция за данные проявляется в столкновении различных «геополитик технологий», по терминологии Сучкова. Центральная Азия сегодня стоит перед выбором между двумя принципиально разными моделями цифрового развития: китайской и западной.

Китайская модель, продвигаемая в рамках инициативы «Пояс и путь», предлагает комплексные решения «под ключ», включающие финансирование, строительство и обслуживание. Исследователи, такие как Изимов и Мураталиева, отмечают высокий потенциал этого подхода для быстрой модернизации. Однако другие ученые (Страйкер, Цзы Яу Янь, Джардин) предупреждают, что за скоростью и эффективностью скрывается угроза

Инициативы США и ЕС чаще всего ориентированы на предоставление консультативной, финансовой или экспертной помощи. Они направлены на поддержку местных проектов и реформ, соответствующих западным стандартам и менталитету, но не предполагают полного цикла «от А до Я» и требуют от стран-партнеров соблюдения следующих ключевых правовых и этических стандартов:

- Элементы конфиденциальности по умолчанию: Требуют, чтобы защита персональных данных была встроена в архитектуру цифровых систем с самого начала, а не добавлялась как опциональный элемент.
- Участие общественности: Требует активного вовлечения гражданского общества в процессы цифровизации, чтобы цифровые решения отражали общественные потребности и снижали риск их использования в авторитарных целях.
- Право быть забытым: Предоставляет гражданам право требовать удаления их личной информации из баз данных, устанавливая приоритет права человека над неограниченным сбором данных.

Несмотря на концептуальную проработанность, прозрачность и акцент на фундаментальных ценностях, западная модель часто проигрывает в конкуренции, поскольку соблюдение этих требований является медленным и ресурсоемким, что стратегически невыгодно для политических элит региона, нацеленных на быстрый экономический рост.

Таким образом, в научной литературе геополитическая конкуренция в ЦА сводится к фундаментальному выбору между двумя моделями цифрового развития.

Центральная Азия стоит перед сложным выбором: как обеспечить цифровую безопасность и независимость, не рискуя попасть в технологическую ловушку и столкнуться с юридическими проблемами.

## **Методология и данные**

### ***Методологический подход***

**Исследование основывается на междисциплинарном подходе, сочетающем методы политического анализа, сравнительного правоведения и геополитических исследований.**

### ***Методы исследования***

- Качественный анализ документов - изучение национальных стратегий цифрового развития, международных соглашений и отчетов международных организаций
- Сравнительный анализ - сопоставление подходов КНР, ЕС и США к технологическому сотрудничеству с Центральной Азией
- Кейс-стади - детальный анализ конкретных проектов (система «Сергек» в Казахстане, проекты Huawei в Узбекистане, «Безопасный город» в Таджикистане)
- Контент-анализ - систематический анализ публичных заявлений, корпоративных отчетов и медиа-материалов

### ***Источники данных***

- Официальные документы правительств стран Центральной Азии
- Отчеты международных организаций (ITU, Всемирный банк, ПРООН)
- Корпоративные отчеты технологических компаний
- Аналитические материалы исследовательских центров
- Данные о технологических контрактах и инвестициях

### ***Ограничения исследования***

- Отсутствие официальной информации о деталях соглашения и договоров, затрудняет проведение полного финансового и технического анализа
- Быстрое изменение технологического ландшафта

### ***Этические соображения***

Исследование соблюдает принципы академической этики, избегая необоснованных обвинений и основываясь на верифицируемых фактах и открытых источниках информации.

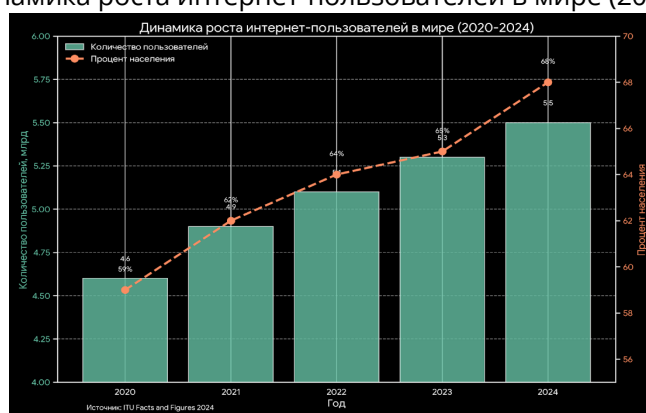
## Результаты и обсуждение

### Многоуровневая структура цифрового неравенства

В современном мире цифровизация и доступ к интернету стали неотъемлемой частью жизни человека. Сегодня это рассматривается, не как роскошь, а как фундаментальная потребность, определяющий фактор социально-экономического развития как на индивидуальном, так и на государственном уровне.

Несмотря на активный рост, цифровой доступ остается неравномерным. Так по данным аналитической платформы DataReportal на начало 2025 года глобальная аудитория интернет-пользователей достигла 5,56 миллиарда человек, что составляет 67,9% от общей численности населения Земли<sup>79</sup>.

«Рис.1 Динамика роста интернет-пользователей в мире (2020-2024)»<sup>80</sup>



Однако, согласно данным Международного союза электросвязи, около 3,7 миллиарда человек по всему миру оказались исключены из цифрового пространства и лишены доступа к базовым услугам по причине отсутствия доступа к интернету, техническим устройствам или необходимым цифровым компетенциям для работы с информационно-коммуникационными технологиями<sup>81</sup>.

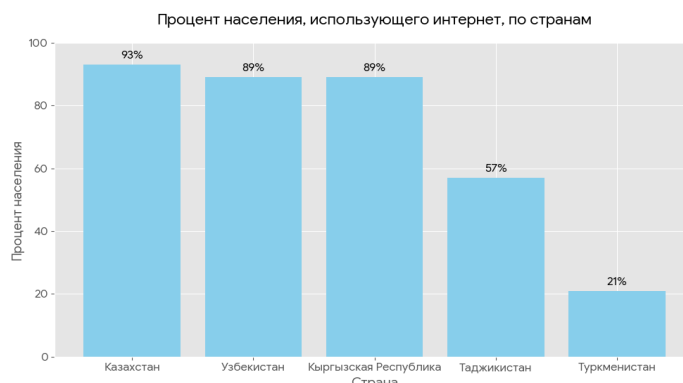
«Рис.2 Процент населения, использующего интернет в ЦА»<sup>82</sup>

<sup>79</sup>DataReportal, Digital 2025: Global Overview Report, DataReportal, January 2025, <https://datareportal.com/reports/digital-2025-global-overview-report>.

<sup>80</sup> Составлен на основе данных ITU Facts and Figures 2024, International Telecommunication Union 2020-2024.

<sup>81</sup> International Telecommunication Union, «More Urgent Than Ever: Universal Connectivity to Bring 3.7 Billion People Online», International Telecommunication Union, December 1, 2020, <https://www.itu.int/hub/2020/12/more-urgent-than-ever-universal-connectivity-to-bring-3-7-billion-people-online/>.

<sup>82</sup> Составлен на основе данных World Bank (Всемирный банк). Individuals using the Internet (% of population) - Europe & Central Asia.



Особенно остро цифровой разрыв проявляется в неравенстве между городом и селом. Если в городских районах доступ к сети имеют 82,7% жителей, то в сельской местности этот показатель падает почти вдвое - до 47,4%.

Такой разрыв обусловлен не только экономическими и техническими проблемами, но и усугубляет социальную и экономическую изоляцию граждан<sup>83</sup>.

Пандемия COVID-19 в 2020 году наглядно показала нашу глубокую зависимость от цифровых технологий. В условиях самоизоляции они стали главным инструментом для поддержания функционирования ключевых сфер: дистанционного образования, удаленной работы, а также получения государственных и медицинских услуг<sup>84</sup>. Этот период ознаменовался активным внедрением технологий во всех сферах жизни человека.

Международное сообщество все в большей степени осознает, что цифровое неравенство является общей проблемой. Об этом свидетельствуют инициативы ООН (Инициатива ООН «Глобальный цифровой договор», направленная на формирование общего будущего в цифровой сфере<sup>85</sup>, в области цифрового развития, программы Всемирного банка по цифровой трансформации и декларации крупных международных форумов<sup>86</sup>.

В рамках международных программ развития страны с развитой цифровой инфраструктурой получают возможность формировать долгосрочные зависимые отношения через предоставление цифровых решений,

<sup>83</sup> Ibid. (4 International Telecommunication Union, «More Urgent Than Ever: Universal Connectivity to Bring 3.7 Billion People Online», International Telecommunication Union, December 1, 2020, <https://www.itu.int/hub/2020/12/more-urgent-than-ever-universal-connectivity-to-bring-3-7-billion-people-online/>.)

<sup>84</sup> United Nations Development Programme. Цифровая стратегия 2022-2025. Программа развития Организации Объединенных Наций. 2022. [https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-ABRIDGED-VERSION-PRINT\\_RU\\_Interactive.pdf](https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-ABRIDGED-VERSION-PRINT_RU_Interactive.pdf).

<sup>85</sup> United Nations, «Global Digital Compact», ООН, 2024, <https://www.un.org/ru/summit-of-the-future/global-digital-compact>.

<sup>86</sup> Всемирный банк. «Всемирный банк предоставляет дополнительную поддержку для цифровой трансформации Кыргызской Республики.» Пресс-релиз, 12 января 2024 г. <https://www.vsemirnyjbank.org/ru/news/press-release/2024/01/12/world-bank-provides-additional-support-for-the-kyrgyz-republic-s-digital-transformation..>

инфраструктурных объектов и технической экспертизы для стран с «технологическим дефицитом»<sup>87</sup>.

Современное понимание цифрового неравенства выходит за рамки простого наличия или отсутствия доступа к цифровым технологиям оно сопряжено с рядом других проблем.

Каждый из них не существует сам по себе, а в совокупности определяет глубину и характер неравенства.

Согласно классической модели Я. Ван Дейка, цифровое неравенство включает четыре взаимосвязанных уровня<sup>88</sup>

#### Материальный доступ или технический фактор.

Он является базовым уровнем, включающий доступность цифровых услуг, широкополосных сетей, персональных устройств (компьютеры, смартфоны) и стабильного интернет-соединения.

#### Мотивационный доступ

Мотивационный доступ представляет собой психологический барьер, отражающий желание или нежелание использовать технологии. Зачастую эти барьеры оказываются более устойчивыми, чем технические, поскольку связаны с глубинными социальными установками и требуют долгосрочных трансформаций. (Доверия к цифровым платформам и сервисам, возрастные и поколенческие различия в восприятии технологий, культурные и религиозные установки относительно цифровизации и д.р.)

#### Навыки и компетенции

Доступ через навыки включает способность эффективно использовать цифровые технологии. Я. Ван Дейк выделяет несколько уровней цифровых навыков<sup>89</sup>:

Операционные навыки - базовые технические умения работы с устройствами и программами

Информационные навыки - способность искать, отбирать, обрабатывать и оценивать информацию в цифровой среде.

Стратегические навыки - умение использовать цифровые технологии для достижения личных и профессиональных целей

#### Использование

Отражает эффективность применения доступных технологий для решения жизненных задач, личного и профессионального развития.

---

<sup>87</sup> Сучков, М.А. ««Геополитика технологий»: международные отношения в эпоху Четвертой промышленной революции.» Вестник Санкт-Петербургского университета. Международные отношения 15, № 2 (2022): 138–157. <https://doi.org/10.21638/spbu06.2022.202>.

<sup>88</sup> Van Dijk, Jan A. G. M. «Digital divide research, achievements and shortcomings.» Poetics 34, no. 4–5 (2006): 221–235..

<sup>89</sup> Van Deursen, Alexander J. A. M., and Jan A. G. M. Van Dijk. «The first-level digital divide shifts from inequalities in physical access to inequalities in material access.» New Media & Society 21, no. 2 (2019): 354–375.

Вышеуказанные уровни доступа образуют сложную систему взаимодействия и созависимости друг с другом тем самым влияя на уровень цифрового неравенства.

Недостатки, существующие на каждом уровне, усиливают неравенство на последующих этапах, и это работает и наоборот - успешное использование технологий мотивирует к развитию навыков и расширению доступа.

Особое значение для экономики и политики имеют факторы «Навыки и компетенции» и «Использование». Как отмечают Н. Коулдри и У. Мехиас, в своей концепции «колонизации данных» они проводят параллели между традиционным колониализмом и цифровыми технологиями<sup>90</sup>. Если в прошлом колониализм основывался на насильственном захвате земель и ресурсов, то в наши дни сбор данных носит более «мягкий» и добровольный характер, так как пользователи соглашались на передачу информации в обмен на технические блага.

Эту идею усиливает концепция Клайва Хамби «Данные - это новая нефть», которая давно стала основой цифровой экономики<sup>91</sup>. Подобно сырой нефти, данные не имеют ценности без обработки и анализа. Осознавая это, государства стремятся к контролю над собственными «месторождениями данных», так как этот ресурс обладает ключевым политическим и экономическим значением и является предметом геополитической конкуренции.

Технологическая зависимость от других стран создает комплекс рисков, включая возможность дистанционного мониторинга и сбора информации, навязывание долгосрочных обязательств по техническому обслуживанию и модернизации, а также теоретическую возможность отключения критически важных компонентов. Более того, кибератаки на инфраструктуры стран-поставщиков могут привести к трансляции уязвимостей всем государствам-получателям. В результате, многоаспектная природа цифрового неравенства выходит за рамки внутренних социальных вопросов, трансформируясь в определяющий геополитический фактор на международной арене.

### ***Эволюция китайского присутствия в регионе***

Сотрудничество КНР с ЦА началось задолго до формального запуска инициативы «Один пояс, один путь» в 2013 году.

После распада СССР новые независимые государства столкнулись с необходимостью дипломатического признания, формирования

---

<sup>90</sup> Couldry, Nick, and Ulises A. Mejias. The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford, CA: Stanford University Press, 2019.

<sup>91</sup> University of Sheffield. (n.d.). Clive Humby. Retrieved from <https://sheffield.ac.uk/cs/people/academic-visitors/clive-humby>

экономических систем, урегулирования территориальных вопросов и развития инфраструктуры<sup>92</sup>.

Это в свою очередь открыло для КНР новые возможности для укрепления и расширения своего присутствия в регионе в том числе решить вопросы безопасности своих приграничных территории.

КНР рассматривает Центральную Азию как важную «линию обороны» и буферную зону в своей борьбе с «тремя злами» - терроризмом, сепаратизмом и религиозным экстремизмом. Деятельность этих угроз представляет собой непосредственную опасность для стабильности западных территорий Китая, которые находятся в непосредственной близости к Центральной Азии. Соответственно сотрудничество с центральноазиатскими странами в борьбе с «тремя злами» становится ключевым аспектом обеспечения национальной безопасности Китая<sup>93</sup>.

С 1996 года, а затем с 2001 года власти КНР использовали формат Шанхайской организации сотрудничества для плавного развития своего влияния в Центральноазиатском регионе.

Прямым конкурентом для КНР в регионе была только Россия, которая имела историческую связь и влияние на страны ЦА.

Инициирование и развитие Россией Таможенного союза (с 2010 года) и становление полноценной организации в виде Евразийского экономического союза подтолкнуло КНР к поиску более эффективных механизмов расширения своего влияния на западном направлении<sup>94</sup>.

Однако, в связи с началом вторжения России на Украину в 2014 году и последующие международные санкции ограничили ресурсы России и создали политические риски для сотрудничества с ней. Страны Центральной Азии начали активно диверсифицировать внешнеполитические связи, укрепляя отношения с Индией, Пакистаном, Японией, Южной Кореей, ОАЭ и Турцией.

В 2021 году ЕС в качестве альтернативной модели международного сотрудничества в сфере инфраструктурного развития для региона подготовила программу «Global Gateway» («Глобальный шлюз»).

На первом саммите «ЕС - Центральная Азия» в апреле 2025 года был анонсирован инвестиционный пакет, в рамках которого предусмотрено выделение около \$14 миллиардов для развития данной инициативы. Эти инвестиции охватывают четыре ключевых приоритетных направления: транспорт (\$3,5 млрд.), критическое сырье (\$3,4 млрд.), водно-

---

<sup>92</sup> Stryker, Cian. Importing Chinese Surveillance Technology: Are Central Asian States on the Path to Digital Authoritarianism? Master's thesis, Harvard Graduate School of Arts and Sciences, 2021.

<sup>93</sup> 战术演化 (Zhànshù Yǎnhuà), «15 亿白送? 中国与中亚的“硬核扶贫”背后真相揭秘», Baidu Baijiahao, 20 июня 2025 г., <https://baijiahao.baidu.com/s?id=1835350871890629685&wfr=spider&for=pc>.

<sup>94</sup> Изимов, Р.Ю., и З.Т. Мураталиева. «Центральноазиатский трек инициативы «Пояс и путь»: возможности и риски.» Вестник международных организаций 13, № 3 (2018): 128–142. <https://doi.org/10.17323/1996-7845-2018-03-08>.



энергетический сектор и климат (\$7,5 млрд.), а также цифровую связь (\$117 млн.)<sup>95</sup>.

Модель ЕС по развитию цифровой сферы в Центральной Азии представляет собой не только программу технологической помощи, но и поэтапную стратегию для внедрения стандартов и нормативных актов ЕС для создания единой экономической и политической среды в регионе.

ЕС в рамках программы предлагает конкретные механизмы для сокращения цифрового неравенства, основанные на принципе «values-based alternative» (альтернатива, основанная на ценностях).

Несмотря на концептуальную проработанность, прозрачность, финансовые ресурсы и базирование на фундаментальных ценностях и стандартах, модель Европейского Союза в Центральной Азии сталкивается с фундаментальной уязвимостью при прямой конкуренции с подходом КНР, а именно с тем, что соблюдение всех этих требований является заведомо медленными и ресурсоемкими.

Для политических элит региона, чья легитимность часто зависит от способности обеспечить быстрый экономический рост, данное предложение может оказаться стратегически невыгодным.

Что касается США являющегося одним из конкурентов РФ и КНР, то с приходом администрации президента Дональда Трампа в январе 2025 года американская модель внешней помощи претерпела кардинальные изменения.

До прихода администрации Трампа в январе 2025 года американская стратегия преодоления цифрового неравенства базировалась на комплексном многоуровневом подходе, сочетающем внутренние и международные инициативы.

США реализовала свои цели через специализированные агентства, в первую очередь через USAID (Агентство США по международному развитию). Деятельность агентства была направлена на содействие экономическому и социальному развитию других стран, включая сокращение цифрового неравенства и формирование «открытых» цифровых экосистем. Помощь выражалась через поддержку грантовых исследований в области цифровой и медиа-грамотности, техническая помощь в развитии национальных систем кибербезопасности, консультативная поддержка реформ электронного правительства, стимулирование развития цифровой экономики через инкубационные программы, поддержка технологических стартапов и инновационных экосистем<sup>96</sup>.

---

<sup>95</sup>European Commission, EU-Central Asia Factsheet, апрель 2025, [https://ec.europa.eu/commission/presscorner/api/files/attachment/881028/EU-Central%20Asia\\_Factsheet\\_2025-04.pdf](https://ec.europa.eu/commission/presscorner/api/files/attachment/881028/EU-Central%20Asia_Factsheet_2025-04.pdf).

<sup>96</sup> U.S. Agency for International Development, «Our Mission,» accessed September 3, 2025, <https://oig.usaid.gov/mission>.

Американские программы зачастую базировались на двусторонних соглашениях о технической помощи и не предполагали создания долгосрочных институциональных обязательств для стран-реципиентов.

Новый подход к внешней политике США отражен в президентском указе «О переоценке и перестройке внешней помощи Соединенных Штатов»<sup>97</sup>.

Данный указ установил новую политику, согласно которой все проекты внешней помощи будут поддерживаться только в том случае, если они напрямую совпадают с национальными интересами США. В связи с этим все программы и гранты в настоящее время пересматриваются или приостанавливаются.

В условиях нарастающей технологической конкуренции между тремя державами, снижение присутствия одной из них в регионе открывает дополнительные возможности для других геополитических игроков. Это фактически может означать передачу инициативы в формировании глобальных цифровых стандартов и экосистем главному геополитическому сопернику.

Таблица 1. Сравнительный анализ подходов: КНР, США и ЕС

| Критерий             | Модель США                                                                    | Модель ЕС                                                      | Модель КНР                                                                                                                          |
|----------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Суть подхода         | Ранее предоставление ресурсов и инструментов для самостоятельной реализации.  | Предлагают помощь, но на основе своих ценностей и стандартов.  | Предлагают комплексные, готовые решения для быстрого результата.                                                                    |
| Механизмы реализации | Грантовая поддержка, техническая помощь, консультации по реформам.            | Прозрачное финансирование, соблюдение международных стандартов | Инвестиции, строительство инфраструктуры и оборудование.                                                                            |
| Результат            | Страна-получатель сама отвечает за реализацию, без долгосрочных обязательств. | Развитие согласно принципам и ценностям ЕС                     | Быстрая реализация, но с риском зависимости от китайских технологий, тем самым обеспечивая долгосрочное присутствие своих компаний. |

Программа «Один пояс, один путь», выдвинутая в 2013 году председателем КНР Си Цзиньпином, а затем в 2017 году создание инициативы «Цифровой Шелковый путь» стали отправными точками для масштабной международной программы сотрудничества для регионов<sup>98</sup>.

Подтверждением тому служит Договор о вечном добрососедстве, заключенный на саммите «Центральная Азия — Китай» в Астане 17 июня 2025 года, в рамках которого КНР предоставила странам региона

<sup>97</sup> The White House. Presidential Memorandum on Reevaluating and Realigning United States Foreign Aid. Presidential Actions, January 1, 2025. <https://www.whitehouse.gov/presidential-actions/2025/01/reevaluating-and-realigning-united-states-foreign-aid/>.

<sup>98</sup> Министерство иностранных дел Китайской Народной Республики, «Состоялась встреча Си Цзиньпина и Н. Назарбаева», Министерство иностранных дел КНР, 7 сентября 2013 г., [https://www.mfa.gov.cn/rus/zxxx/201309/t20130911\\_766180.html](https://www.mfa.gov.cn/rus/zxxx/201309/t20130911_766180.html).

безвозмездные инвестиции в размере около \$210 миллионов для реализации совместных проектов<sup>99</sup>.

КНР в отличие от других стран-доноров, предлагает Центральной Азии масштабную, быструю и существенную финансовую поддержку.

Готовность КНР к столь масштабным, быстрым и финансово щедрым инвестициям в Центральную Азию обусловлена не только экономическими интересами в рамках BRI.

Данная программа позволяет КНР расширять свое геополитическое и геоэкономическое стратегическое пространство не только в Центральной Азии, но и на всем Евразийском континенте. КНР создает новые транспортные коридоры, обеспечивающие поставки энергетических ресурсов, минуя сухопутные и морские маршруты, традиционно контролируемые другими крупными державами<sup>100</sup>.

### ***Сотрудничество и развитие системы «Умных городов» в регионе***

Сотрудничество КНР с регионом началось с выхода на рынки Центральной Азии таких китайских цифровых компаний, как ZTE, Hikvision и Dahua. Однако эти компании не являются самостоятельными инициаторами, а выступают технологическими операторами для реализации масштабных стратегических проектов, продвигаемых правительством КНР. Именно правительство формирует цели, выделяет финансирование и выстраивает политическую основу сотрудничества, а компании становятся технологическим проводником этих решений.

Такая деятельность является отражением комплексного подхода Китая к технологической помощи, который включает не только поставку оборудования, но и передачу технологий, обучение специалистов и создание долгосрочных партнерских отношений.

Этот комплексный подход ярко иллюстрирует деятельность Huawei, открывшей представительство в Узбекистане еще в 1999 году<sup>101</sup>. С тех пор компания глубоко интегрировалась в экономики стран ЦА, реализуя проекты от развития мобильных сетей 5G и создания центров обработки данных до оснащения госсектора<sup>102,103,104</sup>.

---

<sup>99</sup> 宸铠说 (Chén Kǎi Shuō). «中国大手一挥, 15 亿无偿送给中亚, 双方一致同意, 再签一项新条约.» Baidu Baijiahao, 19 июня 2025 г. <https://baijiahao.baidu.com/s?id=1835320437599696014&wfr=spider&for=pc>.

<sup>100</sup> Бояркина, А.В. «Китайская инициатива «Пояс и путь» в контексте концепции Си Цзиньпина «Сообщество единой судьбы человечества».» Theories and Problems of Political Studies, № 9 (2020): 120–126

<sup>101</sup> Huawei, «Local States», <https://www.huawei.com/uz/corporate-information/local-states>.

<sup>102</sup> Ibid <https://www.huawei.com/uz/corporate-information/local-states>

<sup>103</sup> Tsz Yau Yan. «Smart Cities or Surveillance? Huawei in Central Asia: Chinese Surveillance Technologies Are Popular among Central Asia's Governments.» The Diplomat, August 7, 2019. <https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/>

<sup>104</sup> Huawei, «Huawei prodoljajet razvivat' 5G v Uzbekistane,» Huawei, May 17, 2022, <https://www.huawei.com/uz/news/uz/2022/huawei-prodoljajet-razvivat-5g-v-uzbekistane>.

В том числе в рамках сотрудничества КНР с регионом, китайскими технологическими компаниями:

В 2020 году КНР оказал безвозмездную помощь Казахстану, передав суперкомпьютер стоимостью \$15,4 млн. для эксплуатации Казахским национальным университетом имени аль-Фараби, в том числе КНР взял на себя ответственность за его поставку, установку и обслуживание<sup>105</sup>.

В 2022 году внесено более \$500 млн. в телекоммуникационные проекты Huawei и ZTE в Узбекистане КНР, что формирует не только экономические, но и технологические обязательства для страны<sup>106</sup>.

В 2023 году разработана была инициатива по созданию Лаборатории пространственно-временного искусственного интеллекта, финансирование которой в размере около \$140,5 млн. реализуется в рамках программы по формированию Евразийского научно-технологического кластера.

В долгосрочных планах КНР намерен предоставить грант в размере около \$210 млн странам ЦА и предоставить странам ЦА в течении ближайших лет 3 тысячи квот для переподготовки кадров в данной области, для совместного развития региона и углубления сотрудничества с Китаем<sup>107</sup>.

Эта стратегия финансовой и образовательной поддержки также создает фундамент для долгосрочного технологического влияния.

В том числе длительное присутствие китайских компаний приводит к полной интеграции их стандартов в национальную ИКТ-инфраструктуру. Предоставляя различные гранты и открывая региональные центры обучения (например, академии Huawei), КНР формирует в странах Центральной Азии целый пласт IT-специалистов, чьи знания, практический опыт и профессиональная сертификация неразрывно связаны с экосистемой одного конкретного поставщика. Тем самым переход на альтернативные технологии становится практически невозможным без полной перестройки сетей, сопоставимой по стоимости с созданием новой системы с нуля.

Сочетая прямые инвестиции, безвозмездную помощь, передачу технологий и подготовку специалистов, КНР формирует устойчивую зависимость ключевых секторов экономики стран ЦА от своих решений и стандартов.

Для стран Центральной Азии китайский путь развития становится предпочтительным ориентиром, поскольку он воспринимается как более реалистичный, адаптируемый и политически удобный. Помимо тесных

---

<sup>105</sup> Постановление Правительства Республики Казахстан от 14 января 2020 года № 56 «О заключении Соглашения между Правительством Республики Казахстан и Правительством Китайской Народной Республики об оказании безвозмездной помощи по проекту «Оборудование и материалы для создания суперкомпьютерного центра», <https://adilet.zan.kz/rus/docs/P2000000056>.

<sup>106</sup> Invest in Uzbekistan, «Huawei and ZTE Contract with Uzbekistan Is Worth More Than \$500 Million», Invest in Uzbekistan, accessed September 3, 2025, <https://invest-in-uzbekistan.org/uz/novosti-uzbekistana/en-huawei-and-zte-contract-with-uzbekistan-is-worth-more-than-500-million/>.

<sup>107</sup> Информационное агентство Казинформ. «Китай предоставит странам Центральной Азии грант в размере 1,5 млрд юаней.» Inform.kz, 19 мая 2023 г. <https://www.inform.kz/ru/kitay-predostavit-stranam-tsentralnoy-azii-grant-v-razmere-15-mlrd-yuaney-84dc6a/>.

географических и экономических связей с Китаем, в регионе существуют общие черты в системе государственного управления, такие как стремление к централизации, государственный контроль над критически важной инфраструктурой и информационным пространством, а также схожие приоритеты в сфере безопасности

На этом фоне более либеральные и децентрализованные модели ЕС и США воспринимаются как менее адаптированные к политическим условиям региона.

### *Обзор проектов «Умного/Безопасного города» в регионе*

Китайская модель управления цифровым пространством, известная как «Цифровой суверенитет», основывается на масштабной государственной инициативе «Золотой щит» (Golden Shield Project), начатой в 1998 году. Этот проект, получивший международное название «Великий файрвол» (Great Firewall), изначально был нацелен на создание комплексной информационной системы общественной безопасности<sup>108</sup>.

Активная фаза его внедрения, совпавшая с завершением второй фазы проекта в 2008 году, продемонстрировала эффективность фильтрации внешнего интернет-трафика. Однако «Золотой щит» - это не только инструмент контроля над контентом, но и основа для развертывания национальных систем видеонаблюдения и мониторинга<sup>30</sup>.

Именно в рамках «Золотого щита» и его логического продолжения, в первой половине 2000-х годов, в КНР была запущена инициатива «Безопасный город»

Безопасность это один из фундаментальных аспектов комфортной жизни в любом крупном городе мира. Концепции «умного города» и «безопасного города», хотя и взаимосвязаны, решают различные, но дополняющие друг друга задачи городского развития<sup>109</sup>:

Концепция «умного города» предполагает более глубокую интеграцию цифровых решений в городскую инфраструктуру. Цифровизация охватывает все сферы: от транспорта и энергетики до экологии и предоставления услуг. Все эти меры направлены на повышение эффективности работы города, снижение негативного воздействия на окружающую среду и улучшение качества жизни горожан.

Концепция «Безопасный город» фокусируется на обеспечении безопасности жителей и жизненно важных объектов. Для этого используются передовые технологии: умные системы видеонаблюдения, оперативные центры для координации экстренных служб, системы оповещения о ЧС и надежная

---

<sup>108</sup> Gissonna, N. «Great Firewall.» Encyclopedia Britannica, September 12, 2025.

<https://www.britannica.com/topic/Great-Firewall>.

<sup>109</sup> Giffinger, Rudolf, Christian Fertner, Hans Kramar, Robert Kalasek, Nataša Milanović, and Evert Meijers. «Smart cities - Ranking of European medium-sized cities.» Working Paper. Vienna: Vienna University of Technology, 2007.

киберзащита. В результате снижается уровень преступности, повышается скорость реагирования на происшествия и обеспечивается защита от различных угроз.

При внедрении проектов «Умный город» и «Безопасный город» страны Центральной Азии проявляют интерес к китайскому опыту, и это не случайно.

Китай одним из первых в мире приступил к развертыванию масштабных систем видеонаблюдения в 2005 году, причем инициатива «Безопасный город» была запущена еще раньше, в первой половине 2000-х<sup>110</sup>. К 2025 году страна, пройдя этапы пилотных проектов и интеллектуальной модернизации, внедрила полное комплексное цифровое управление<sup>111</sup>

«Рис.3 Улица в КНР с камерами наблюдения»<sup>112</sup>



В том числе мировой рынок безопасности находится под сильным влиянием китайских технологических гигантов, что подтверждается глобальными данными.

Согласно отчету «Security 50» за 2024 год от ASmag.com, две китайские компании - Hikvision и Dahua занимают более половины доли рынка среди десяти крупнейших производителей физической безопасности. Их доминирование ощутимо и в Центральной Азии, где их решения являются основой для большинства государственных и коммерческих систем безопасности.

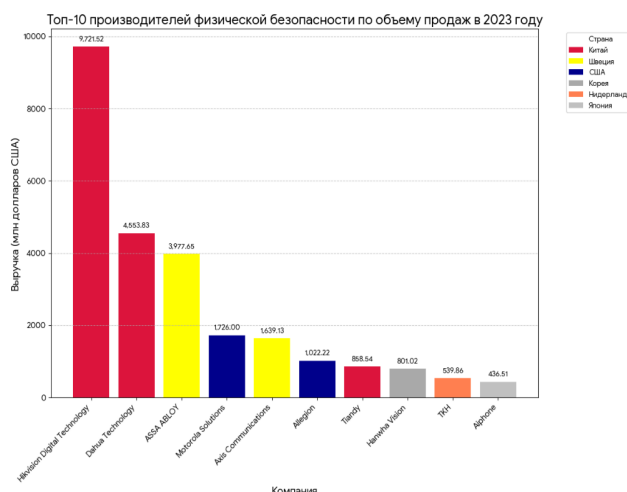
Рис.4.Топ-10 производителей физической безопасности по объему продаж в 2023 году.

<sup>110</sup> Суханкин, Сепрей. «Tracking the Digital Component of the BRI in Central Asia, Part One: Exporting “Safe Cities” to Uzbekistan.» China Brief 21, no. 3 (February 11, 2021). Jamestown Foundation. <https://jamestown.org/program/tracking-the-digital-component-of-the-bri-in-central-asia-part-one-exporting-safe-cities-to-uzbekistan/>.

<sup>111</sup> South China Morning Post, «China to Build Giant Facial Recognition Database to Identify Anyone,» *South China Morning Post*, October 16, 2017, <https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any>.

<sup>112</sup> BuzzFeed News (из статьи This Is What A 21st-Century Police State Really Looks Like)





Первые пробные совместные проекты стартовали в 2013 году, в Таджикистане, когда правительство заключило контракт с Huawei на 22 млн долларов. Были установлены сотни камер видеонаблюдения и дорожных камер в Душанбе, хотя первоначально они не имели систем распознавания лиц. Несмотря на это, система показала эффективность: только осенью 2019 года сумма штрафов за нарушение ПДД превысила \$14 млн.

В том же году правительство решило модернизировать проект и объявило о внедрении камер Huawei с распознаванием лиц по всей стране<sup>113</sup>.

Huawei является крупным инвестором и подрядчиком в сфере телекоммуникаций и интернет-связи. В декабре 2023 года Служба связи Таджикистана и компания Huawei Technology Таджикистан подписали Меморандум о сотрудничестве<sup>114</sup>. Данный документ регулирует развитие цифровых технологий, телекоммуникаций и связи в стране.

В рамках подписанного меморандума Huawei берет на себя обязательства по оказанию технической поддержки и содействию в развитии мобильных сетей Таджикистана. Ключевым аспектом сотрудничества станет модернизация 7600 базовых станций, что позволит расширить зону покрытия и улучшить качество интернет-соединения, особенно в регионах с ограниченным доступом. Все эти мероприятия осуществляются с целью достижения задач, поставленных государством в рамках программ цифровизации и формирования концепции «умного города».

<sup>113</sup> Tsz Yau Yan. «Smart Cities or Surveillance? Huawei in Central Asia: Chinese Surveillance Technologies Are Popular among Central Asia's Governments.» The Diplomat, August 7, 2019. <https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/>.

<sup>114</sup> ASIA-Plus. «Служба связи Таджикистана и «Хуавэй Таджикистан» подписали Меморандум о сотрудничестве.» ASIA-Plus, 13 декабря 2023 г. <https://www.asiaplustj.info/ru/news/tajikistan/society/20231213/sluzhba-svyazi-tadzhikistana-i-huawei-tadzhikistan-podpisali-memorandum-o-sotrudnichestve..>



Помимо прямых каналов с КНР международная интернет-связь Таджикистана, опирается на маршруты через Кыргызстан и Узбекистан, что создает еще больше рисков уязвимости в сфере безопасности.<sup>115</sup>

В Кыргызстане попытки запустить «Безопасный город» начались еще в 2011 году с российской компанией «Стилсофт», но проект не был реализован. В 2018 году разгорелась тендерная борьба между Huawei и российской «Вегай». Сначала правительство заключило контракт на \$60 млн. с Huawei, однако переговоры сорвались, и «Вега» получила заказ на установку дорожных камер стоимостью \$33 млн. Позднее Кыргызстан выбрал китайскую компанию CEIEC для установки системы распознавания лиц в Бишкеке, причем, по сообщениям, на безвозмездной основе<sup>116</sup>.

В 2017 году в Казахстане отечественной компанией ТОО «Көркем Телеком» был разработан проект, с целью создания умного и безопасного города - «Сергек» - интеллектуальная система видеонаблюдения, установленная на перекрестках, вдоль дорог и в местах большого скопления людей. Она обеспечивает контроль за безопасностью на дороге и в общественных местах. Система видеонаблюдения использует продукты компании «Dahua», для которых проводится локальная перепрошивка программного обеспечения, так как программное обеспечение и алгоритмы создаются местными специалистами<sup>117</sup>.

Создание собственного программного обеспечения и алгоритмов для системы «Сергек» является стратегически верным шагом. Это позволяет нейтрализовать риски, связанные с облачными сервисами производителя и обработкой данных на зарубежных серверах. Однако это не решает фундаментальную проблему к аппаратному обеспечению (самой камере).

Модификация программного обеспечения затрагивает преимущественно пользовательское пространство операционной системы устройства, но не затрагивает ядро операционной системы и низкоуровневые компоненты самого устройства. Риск заключается в том, что какой бы безопасной ни была надстройка, она выполняется поверх потенциально уязвимого и непрозрачного фундамента.

Эти риски подтверждаются и наглядно отражены в бюллетенях безопасности, публикуемых как самим производителем, так и независимыми исследователями в области кибербезопасности.

Так, в официальном отчете Dahua (DHCC-SA-202201-001) была раскрыта критическая уязвимость (CVE-2021-33046), позволявшая удаленно сбросить пароль администратора на огромном перечне устройств, произведенных в

---

<sup>115</sup> Digital Report. «Обзор Телеком Рынка Таджикистана: Фиксированная, Мобильная и Международная Связь.» Digital Report, 5 июня 2017 г. <https://digital.report/tadzhikistan-svyaz/>.

<sup>116</sup> Umarov, Temur. «China Looms Large in Central Asia.» Carnegie Moscow Center, , <https://carnegie.ru/commentary/81402>

<sup>117</sup> Enelane, Nikolai. «Kak Rabotaet Proekt 'Sergek'.» Informbiuro, 2019. <https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html>.

период с 2017 по 2021 год<sup>118</sup>. Это напрямую затрагивает оборудование, которое могло быть закуплено на начальных этапах проекта «Сергек»

Аналогичным образом, отчет от ведущей антивирусной компании Bitdefender продемонстрировал наличие уязвимостей, которые позволяли злоумышленнику без аутентификации получить полный контроль над камерой через ошибки в реализации базовых протоколов, таких как ONVIF (это международный стандарт для IP-систем видеонаблюдения, созданный для обеспечения совместимости оборудования разных производителей). В отчете подчеркивается, что подобные атаки могут обходить даже встроенные механизмы проверки целостности прошивки, что делает их особенно опасными<sup>119</sup>.

Эти примеры наглядно иллюстрируют, как система, несмотря на все меры безопасности на уровне программного обеспечения, «наследует» и подвергается рискам, изначально заложенным в аппаратной платформе и ее закрытом низкоуровневом ПО.

Техническая уязвимость представляет собой серьезный геополитический риск и заключается в ключевой уязвимости цифрового суверенитета: он подрывается не на политическом, а на аппаратно-правовом уровне, где наличие риска само по себе является угрозой.

Тем не менее, зависимость от китайского оборудования оставалась, так как видеонаблюдение продолжали предоставлять решения от «Dahua», так как производить камеры в Казахстане нерентабельно потому что итоговая себестоимость локально произведенной камеры, ввиду отсутствия в стране компонентной базы, дефицита профильных кадров и несопоставимого масштаба производства, будет в разы выше, чем у готовой продукции «Dahua».

Несмотря на то, что Китай и его компании предлагают высококачественные и эффективные продукты и услуги, полная зависимость от них сопряжена с рисками.

Примером таких рисков является ситуация, когда безопасность инфраструктуры полностью зависит от технологий китайских компаний. При глубоком проникновении китайских технологий, такой подход может обернуться неожиданными и даже негативными последствиями.

---

<sup>118</sup> Dahua International, «DHCC-SA-202201-001: Security Advisory - Access control vulnerability found in some Dahua products» (Dahua International, January 12, 2022), <https://www.dahuasecurity.com/aboutUs/trustedCenter/details/602>.

<sup>119</sup> Bitdefender, «Vulnerabilities Identified in Dahua Hero C1 Smart Cameras» (Bitdefender, July 30, 2025), <https://www.bitdefender.com/en-us/blog/labs/vulnerabilities-identified-in-dahua-hero-c1-smart-cameras>.

## ***Цена технологического партнерства и зависимости***

### Кибератака на POST Luxembourg

В Люксембурге 23 июля 2025 года произошла масштабная кибератака, парализовавшая работу телекоммуникационной системы страны на несколько часов<sup>120</sup>.

Злоумышленники, атаковали оборудование Huawei, которое использовалось государственным оператором POST Luxembourg. Целью атаки было не проникновение в системы или кража данных, а дестабилизация критически важных сервисов. В результате на несколько часов были отключены сети 4G и 5G, что привело к серьезным последствиям: невозможности вызова экстренных служб, сбоям в работе электронного банкинга и отключению системы оповещения населения.

Инцидент выявил критическую уязвимость в стандартизированном сетевом компоненте и подчеркнул существенные риски, связанные с «единицами отказа» в национальной цифровой инфраструктуре. В ответ власти Люксембурга инициировали официальное расследование и приступили к срочному пересмотру стратегий киберустойчивости, включая обсуждение внедрения механизмов автоматического межсетевого переключения мобильных устройств для обеспечения стабильности связи в чрезвычайных ситуациях.

«Рис. 5 логотипа почтово-телекоммуникационной государственной корпорации «POST Luxembourg»»<sup>121</sup>



### Штаб-квартира Африканского союза

Инцидент с утечкой данных из штаб-квартиры Африканского союза в Аддис-Абебе, чье строительство и оснащение полностью осуществлялось при поддержке иностранных партнеров, наглядно демонстрирует уязвимости,

<sup>120</sup> Antipov, Alexander. «Кибератака на Huawei оставила целую страну без связи и тревог.» SecurityLab.ru, 4 августа 2025 г. <https://www.securitylab.ru/news/562044.php>.

<sup>121</sup> A sign for Luxembourg's national mail and telecom company, POST Luxembourg. Image: GilPe via Wikimedia Commons / CC BY-SA 4.0

возникающие при полной зависимости от зарубежных технологий и сотрудничества<sup>122</sup>.

В 2012 году Китайская Народная Республика, в партнерстве с ведущими технологическими гигантами Huawei и ZTE, преподнесла в дар Африканскому Союзу 20-этажное здание штаб-квартиры. Общая стоимость этого проекта составила приблизительно \$200млн.

«Рис. 6 Общий вид: здание штаб-квартиры Африканского союза (АС) в столице Эфиопии Аддис-Абебе в январе 2017 года»<sup>123</sup>



Ситуация приобрела скандальный характер в 2018 году, когда французское издание «Le Monde» опубликовало расследование, согласно которому данные с серверов штаб-квартиры ежедневно передавались в КНР на протяжении пяти лет.<sup>124</sup>

На сегодняшнее время ситуация неоднозначна, так как данные утверждения не получили официального подтверждения от независимых технических экспертов или международных организаций. Официальные представители как Африканского союза, так и КНР категорически отвергли обвинения, охарактеризовав их как дезинформацию, направленную на подрыв китайско-африканских отношений.

Тем не менее, как следует из расследовании «Financial Times», в последующем Африканский союз самостоятельно принимал ряд

---

<sup>122</sup> Sherman, Justin. «What's the Deal with Huawei and This African Union Headquarters Hack?» New America, May 28, 2019. <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/whats-the-deal-with-huawei-and-this-african-union-headquarters-hack/>.

<sup>123</sup> Bild: Reuters/T. Negeri

<sup>124</sup> Vitkine, Benoît, and Joël Leblond. «À Addis-Abeba, le siège de l'Union africaine espionné par les Chinois.» Le Monde, January 26, 2018. [https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois\\_5247521\\_3212.html](https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html).

технических мер по устранению последствий связанных с утечкой данных без помощи КНР, в том числе произвел замену серверного оборудования и пересмотрел политику кибербезопасности<sup>125</sup>

Это противоречие указывает о сложной и неоднозначной позиции организации в данном вопросе.

Такая модель «закрытого урегулирования», может свидетельствовать о зависимости и неспособности получателя помощи привлечь дарителя к ответственности за такие нарушения. Если бы за подобное нарушение был ответственен нейтральный сторонний поставщик, логичной реакцией АС было бы публичное осуждение, судебные иски и прозрачный процесс восстановления доверия.

Ситуация с Африканским союзом демонстрирует, что наличие технологической помощи от иностранных государств в сфере критической инфраструктуры требует не только политической оценки, но и системного технического контроля.

Факт того, что утечка данных продолжалась в течение пяти лет до ее обнаружения, указывает на недостаток регулярного мониторинга и независимого аудита систем безопасности. При этом само наличие технических уязвимостей не является достаточным основанием для обвинений в установке шпионских устройств, поскольку их происхождение может быть связано как с производственными дефектами, так и с умышленным вмешательством<sup>126</sup>.

### Санкции в отношении Huawei Technologies Co. Ltd

Санкции 2019 года, направленные на ограничение технологического влияния китайских компаний, обернулись неожиданными и негативными последствиями для инициаторов и для мировой экономики

Решение Бюро промышленности и безопасности (BIS) Министерства торговли США о включении Huawei и других организаций в «Список организаций» (Entity List) в мае 2019 года было мотивировано обеспокоенностью правительства относительно соблюдения компаниями требований национальной безопасности и соответствия внешнеполитическим интересам США<sup>127</sup>

Ключевым фактором стало китайское законодательство, в частности Закон о национальной разведке 2017 года, который обязывает все китайские организации и граждан оказывать содействие государственным

---

<sup>125</sup> Manson, Katrina, and John Aglionby. «African Union Tries to Expunge Chinese Cyber-Snooping.» Financial Times, January 29, 2018. <https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5>.

<sup>126</sup> Justin Sherman, «What's the Deal with Huawei and This African Union Headquarters Hack?», New America, May 28, 2019, <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/whats-the-deal-with-huawei-and-this-african-union-headquarters-hack/>.

<sup>127</sup> Addition of Entities to the Entity List, Federal Register 84, no. 98 (May 21, 2019), <https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>.



разведывательным службам КНР, тем самым предоставляя им широкие полномочия по требованию информации от частных компаний.

Согласно данному закону статьи 7 и 14 прямо устанавливают обязанность для всех китайских организаций, компаний и граждан оказывать «поддержку, содействие и сотрудничество» государственным разведывательным службам КНР в работе по обеспечению национальной безопасности, независимо от их местонахождения<sup>128</sup>.

Однако, закон не содержит четких процедурных ограничений или механизмов контроля, тем самым создавая правовую неопределенность в отношении масштабов и методов такого сотрудничества.

Главной проблемой является экстерриториальное действие данного закона создает потенциальный правовой конфликт для стран-импортеров использующих китайские технологий от таких компании, как Huawei, ZTE, CEIEC, Hikvision, Dahua и других китайских поставщиков критически важной инфраструктуры.

Данная ситуация усугубляется тем, что в китайском праве национальная безопасность имеет безусловный приоритет над коммерческими интересами, что подтверждается комплексом специального законодательства таких как «Закон КНР о национальной разведке», «Закон КНР о кибербезопасности» и д.р.

Таким образом, сочетание местного закона о локализации данных и китайского разведывательного законодательства создает системную уязвимость.

Введенные меры запрещают американским компаниям поставлять технологии китайским фирмам без специальных лицензий, при этом их экстерриториальное действие распространяется на любые компании по всему миру, использующие американские компоненты.

Для стран, чья инфраструктура уже построена на китайском оборудовании, перспектива его полной замены сопряжена с колоссальными трудностями.

Так, например, в 2020 году Великобритания и Канада, использовавшие оборудование китайских технологических компании, столкнулись с проблемой, что процесс связанный со сменой оборудования потребует не менее 5-7 лет. Замена тысяч базовых станций и антенн Huawei по всей стране оценивается в миллиарды фунтов<sup>129</sup>

Данные расходы конечно же ложатся либо на телекоммуникационных операторов, что неизбежно может привести к росту тарифов для потребителей, либо на государственный бюджет.

---

<sup>128</sup> China Law Translate, «National Intelligence Law of the P.R.C. (2017),» *China Law Translate*, <https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/>.

<sup>129</sup> Liu, Coco. «BT, Vodafone Need 5 Years to Replace Huawei Without Blackouts.» *South China Morning Post*, July 9, 2020. <https://www.scmp.com/tech/gear/article/3092551/bt-vodafone-need-5-years-replace-huawei-without-blackouts>.

В 2024 году, по оценкам Федеральной комиссии по связи США, полный демонтаж небезопасного оборудования может обойтись в 4,98 млрд долларов. Однако ранее Конгресс одобрил программу «удаления и замены» оборудования лишь на 1,9 млрд долларов, что не может покрыть предполагаемые расходы<sup>130</sup>

Отказ от иностранного оборудования возможно в будущем будет отражать глобальный тренд на технологическую независимость<sup>131</sup>.

Так КНР столкнувшись с необходимостью тотального импортозамещения, китайские компании совершили резкий скачок в создании автономной технологической экосистемы, менее зависимой от западных компонентов. В результате Китай теперь предлагает странам региона не только экономически выгодные, но и более предсказуемые и устойчивые в условиях санкционного давления решения

Опыт технологически и экономически развитых стран, пытавшихся отказаться от китайского оборудования и опыт КНР в создании технологического суверенитета, продемонстрировали всю сложность этой задачи

Если ранее китайские технологии позиционировались как «дешевая альтернатива», то теперь они предлагаются как «надежная и санкционно-устойчивая» экосистема.

В итоге санкционная политика Запада, направленная на изоляцию Китая, достигла противоположного эффекта-это привело к усилению позиции КНР в Центральной Азии.

Однако для стран Центральной Азии, имеющих ограниченные бюджеты и ресурсы, полная замена инфраструктуры, подобно той, с которой столкнулись Великобритания, Канада и США, может быть неподъемной.

Эта ситуация создает серьезные геоэкономические риски для региона, поскольку страны могут быть вынуждены выбирать между модернизацией инфраструктуры и другими критически важными расходами.

### Риски централизации данных

Для полного запуска таких масштабных проектов сотрудничества с Китаем страны Центральной Азии начали создавать собственные базы данных: например, Узбекистан с 2011 года перешел на биометрические паспорта, к 2017 году охватив ими около 80% населения<sup>132</sup>. Подобные инициативы

---

<sup>130</sup> Shepardson, David. «US House to Vote to Provide \$3 Billion to Remove Chinese Telecoms Equipment.» Reuters, December 8, 2024. <https://www.reuters.com/world/us/us-house-vote-provide-3-billion-remove-chinese-telecoms-equipment-2024-12-08/>.

<sup>131</sup> SecurityLab.ru, «Обзор: Доклад Cloudflare о растущей зависимости мира от импортных технологий,» SecurityLab.ru, 29 марта 2024 г., <https://www.securitylab.ru/news/554672.php>.

<sup>132</sup> Digital Report. «В Узбекистане введут биометрические загранпаспорта с 1 января 2019 года.» Digital Report, 18 августа 2017 г. <https://digital.report/vuzbekistane-vvedut-biometricheskie-zagranpasporta-s-1-yanvary-a-2019-goda/>.



позже появились и в Таджикистане (2014), Кыргызстане (2021) и Казахстане (с 2021 года постепенно и на добровольной основе).

Внедрение биометрических программ ускорило цифровизацию государственных услуг и объединение различных баз данных. Однако, централизованное хранение биометрических данных создало огромные цифровые профили граждан, доступ к которым представляет собой серьезную угрозу для национальной безопасности.

В период с 2017 по 2025 годы законодательство стран Центральной Азии претерпело значительные изменения в сфере регулирования обработки и защиты персональных данных, в частности, в отношении требования о локализации данных - обязанности иностранных компаний хранить и обрабатывать данные граждан на серверах, физически расположенных в пределах национальных границ. Этот подход, призванный усилить суверенитет над данными и обеспечить их защиту, был принят не всеми государствами региона одинаково.

Регулирование хранения персональных данных в Центральной Азии представлено тремя основными подходами. Узбекистан придерживается самой жесткой модели тотальной локализации, обязывая хранить данные граждан исключительно на территории страны<sup>133</sup>. Казахстан выбрал гибридный подход: он обеспечивает суверенитет и доступность данных через обязательное внутреннее хранение, но при этом позволяет передавать данные за рубеж, если обеспечен достаточный уровень защиты и получено согласие субъекта, что способствует поддержанию международных бизнес-процессов<sup>134</sup>.

Однако эти две модели приводят к парадоксальным, результатам-когда правительство страны Центральной Азии, следуя своему закону, нанимает иностранную компанию для создания и обслуживания инфраструктуры, где будут храниться все персональные данные граждан, оно фактически консолидирует наиболее чувствительную национальную информацию в единый репозиторий. Этот репозиторий, в свою очередь, находится под управлением компании, которая юридически обязана сотрудничать и подчиняться прямо законам своей страны.

Проблема усугубляется тем, что страны Центральной Азии не имеют достаточного опыта и знаний для самостоятельной разработки безопасных систем хранения и обработки больших объемов данных. Это означает, что даже если серверы физически находятся в стране, контроль над техническим обслуживанием, обновлениями программного обеспечения и потенциальным доступом к скрытым каналам (бэкдорам) остается в руках

---

<sup>133</sup> Закон Республики Узбекистан от 02.07.2019 г. № ЗРУ-547 «О персональных данных», LEX.UZ, <https://lex.uz/docs/4396428>.

<sup>134</sup> Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите», в ред. от 16.09.2025, ИПС «Әділет», <https://adilet.zan.kz/rus/archive/docs/Z1300000094/16.09.2025>.

иностранных поставщиков. Таким образом, суверенитет над данными и их безопасность подвергаются риску.

Централизация данных, помимо внешних геополитических рисков, несет в себе и внутренние угрозы. Во-первых, крупные, объединенные базы данных становятся привлекательной и легкой целью для хакеров, так как одна успешная атака может привести к утечке личной информации огромного количества людей. Во-вторых, централизованные системы открывают возможности для злоупотреблений со стороны государства и нечестных чиновников, начиная от незаконной слежки за политическими противниками и заканчивая торговлей личными данными. В-третьих, в странах Центральной Азии, где отсутствует должный общественный контроль и независимый надзор за использованием централизованных баз данных, создаются условия для использования цифровых технологий в авторитарных целях.

Этот дефицит независимого контроля усугубляется тем, что систему цифровой безопасности выстраивает само государство в лице уполномоченных органов, часто аффилированных с силовыми структурами. Все страны региона имеют законодательную основу для регулирования информационной сферы (Законы «О кибербезопасности» и «О защите информации»). Однако практический аудит и контроль сосредоточен в руках государственных органов. Такая централизация обеспечивает государственный контроль, но не гарантирует независимой и прозрачной оценки рисков, особенно когда речь идет о технологиях, закупаемых для нужд самого государства.

При этом роль независимой экспертизы и гражданского общества остается крайне ограниченной. Организации, подобные ЦАРКА (Центр анализа и расследования кибератак), фокусируются на техническом анализе, в то время как общественный диалог о рисках и прозрачности в большинстве стран практически отсутствует. Подобный дисбаланс между степенью государственного регулирования и уровнем общественного контроля может приводить к недостаточной прозрачности при внедрении крупных технологических инициатив.

В отличие от этих двух стран Кыргызстан, Таджикистан и Туркменистан выбрали модель регулирования трансграничной передачи, где акцент делается не на обязательном внутреннем хранении, а на контроле условий перемещения данных. Защита в этих странах обеспечивается либо через

получение согласия субъекта, либо через гарантии адекватной защиты при обмене данными<sup>135,136,137</sup>

Предлагаемая модель, хоть и снижает риск геополитической централизации, создает не менее серьезную проблему для государств: постоянную потерю суверенитета и юрисдикции над данными. Это происходит из-за свободного трансграничного перемещения и хранения информации граждан в разрозненных потоках, которые национальные органы не в состоянии эффективно контролировать.

Анализ двух моделей показывает, что они имеют свои сильные и слабые стороны.

Модель жесткой локализации может создавать иллюзию суверенитета при сохранении технологической зависимости от иностранных поставщиков и концертирует риски, тогда как модель свободной трансграничной передачи данных, хотя и распределяет риски, но затрудняет контроль над данными со стороны государства.

## Рекомендации по политике

Рекомендации разработаны для минимизации негативного влияния выявленных рисков (неравенство, зависимость, правовые коллизии) и формирования стабильных основ для обеспечения цифрового суверенитета на национальном и региональном уровнях.

### *Обеспечение технологического суверенитета в регионе*

Для постепенного обретения технологической независимости в жизненно важных сферах (государственное управление, финансы, телекоммуникации) необходимо ввести обязательные квоты для отечественных поставщиков в системе государственных закупок, необходимо запустить долгосрочную программу поддержки национальных IT-компаний. Это должно включать налоговые льготы, гранты на разработку, что будет способствовать развитию национальных технологических компетенций.

Снизить монопольную зависимость, обеспечить устойчивость к внешним санкциям (опыт США/ЕС) и создать здоровую конкуренцию, используя

---

<sup>135</sup> Закон Республики Таджикистан от 3 августа 2018 года №1537 «О защите персональных данных», Национальный центр законодательства при Президенте Республики Таджикистан, <https://ncz.tj/content/%D0%BE-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5-%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85>.

<sup>136</sup> Закон Туркменистана от 22 марта 2017 года «Об информации и ее защите», Уполномоченный по правам человека в Туркменистане (Омбудсмен), доступ 3 октября 2025 г., [https://ombudsman.gov.tm/doc/ru/%D0%BE%D0%B1\\_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8\\_%D0%B8\\_%D0%B5%D1%91\\_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5.rtf](https://ombudsman.gov.tm/doc/ru/%D0%BE%D0%B1_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8_%D0%B8_%D0%B5%D1%91_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5.rtf).

<sup>137</sup> Закон Кыргызской Республики от 14 апреля 2023 года № 85 «О персональных данных», Центральный банк данных правовой информации Кыргызской Республики, <https://cbd.minjust.gov.kg/3-48/edition/35412/ru>.

инвестиционные предложения от альтернативных доноров (EC/Global Gateway, Япония, Южная Корея).

*Развитие регионального сотрудничества и независимый аудит.*

Для эффективного противодействия технологическим угрозам странам Центральной Азии необходимо создать региональный центр по кибербезопасности и сертификации технологий, который бы проводил тот самый независимый аудит для всех стран-участниц. В том числе это позволит координировать усилия, обмениваться опытом, развивать цифровую грамотность и проводить общественные обсуждения, опираясь на общие исторические связи и схожие модели государственного управления.

*Усиление защиты персональных данных и кибербезопасности*

Для эффективной защиты личной информации граждан и обеспечения безопасности в киберпространстве необходимо значительно ужесточить наказания за нарушения в этой сфере. Увеличение штрафов повысит ответственность всех участников: от государственных учреждений и бизнеса до рядовых граждан

Многие из этих политических инициатив уже обсуждаются и реализуются в Центральной Азии. Реализация предложенной трехуровневой стратегии потребует значительных инвестиций и политической воли. Однако в условиях глобальной техно-геополитической конкуренции это не вопрос выбора, а необходимое условие для сохранения реального суверенитета в цифровую эпоху.

## **Заключение**

Проведенное исследование подтверждает, что цифровое неравенство в Центральной Азии является не просто социальной проблемой, а ключевым элементом геополитической стратегии технологического контроля, реализуемой через формирование структурной зависимости от конкретных платформ и стандартов. Это достигается путем формирования зависимости пользователей от конкретных технологических платформ и продуктов. Результаты исследования указывают на то, что:

*Цифровое неравенство- фактор, определяющий геополитическое влияние*

Недостаток цифровой грамотности и инфраструктуры превращает их в поставщиков данных, открывая двери для внешнего влияния. В условиях геополитической борьбы за данные, эта внутренняя слабость становится критическим фактором. Привлекательность китайских «умных городов» для местных элит обусловлена не только экономическими преимуществами, но и политической целесообразностью.

*Структурная технологическая зависимость.* Центральная Азия демонстрирует высокую степень технологической интеграции с китайскими технологическими компаниями в таких областях, как телекоммуникации, безопасность и цифровое управление. Однако это привело к зависимости, поскольку замена китайского оборудования и программного обеспечения на альтернативные решения требует значительных инвестиций, что создает экономические трудности для стран региона.

*Правовые коллизии и экстерриториальность.* Сочетание национальных законов о локализации данных с китайским Законом о национальной разведке 2017 года создает парадоксальную ситуацию: меры, направленные на защиту национальных данных, фактически могут упрощать доступ к ним. Экстерриториальное действие китайского законодательства создает потенциальные правовые конфликты для стран-реципиентов технологической помощи.

*Разные модели сотрудничества.* Сравнительный анализ подходов КНР, ЕС и США выявил фундаментальные различия в стратегиях преодоления цифрового неравенства. Китайская модель демонстрирует превосходство в скорости реализации и финансовой доступности, но создает долгосрочные зависимости. Европейская модель, несмотря на соответствие высоким стандартам и прозрачность, оказывается менее конкурентоспособной в условиях необходимости быстрой модернизации.

*Риск централизации данных.* Централизация биометрических и государственных данных в системах, находящихся под контролем иностранных подрядчиков, поднимает вопросы о потенциальном их использовании для различных целей.

## Список литературы

- Addition of Entities to the Entity List. (2019, May 21). *Federal Register*, 84(98).  
<https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>
- Antipov, A. (2025, August 4). Кибера́така на Huawei оставила целую страну без связи и тревог [Cyberattack on Huawei left an entire country without communication and alarms]. *SecurityLab.ru*.  
<https://www.securitylab.ru/news/562044.php>
- ASIA-Plus. (2023, December 13). Служба связи Таджикистана и «Хуавэй Таджикистан» подписали Меморандум о сотрудничестве [Tajikistan's Communications Service and Huawei Tajikistan signed a Memorandum of Cooperation]. *ASIA-Plus*.  
<https://www.asiaplustj.info/ru/news/tajikistan/society/20231213/sluzhba-svyazi-tadzhikistana-i-huavei-tadzhikistan-podpisali-memorandum-o-sotrudnichestve>
- Bitdefender. (2025, July 30). *Vulnerabilities identified in Dahua Hero C1 smart cameras*. <https://www.bitdefender.com/en-us/blog/labs/vulnerabilities-identified-in-dahua-hero-c1-smart-cameras>
- Boyarkina, A. V. (2020). Китайская инициатива «Пояс и путь» в контексте концепции Си Цзиньпина «Сообщество единой судьбы человечества» [China's Belt and Road Initiative in the context of Xi Jinping's concept of a Community with a Shared Future for Mankind]. *Theories and Problems of Political Studies*(9), 120–126.
- Chén Kǎi Shuō. (2025, June 19). 中国大手一挥, 15 亿无偿送给中亚, 双方一致同意, 再签一项新条约 [China makes a big move, giving 1.5 billion to Central Asia for free; both parties agree to sign a new treaty]. *Baidu Baijiahao*.  
<https://baijiahao.baidu.com/s?id=1835320437599696014&wfr=spider&for=pc>
- China Law Translate. (n.d.). *National Intelligence Law of the P.R.C. (2017)*.  
<https://www.chinalawtranslate.com/national-intelligence-law-of-the-p-r-c-2017/>
- Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- Dahua International. (2022, January 12). *DHCC-SA-202201-001: Security advisory—Access control vulnerability found in some Dahua products*.  
<https://www.dahuasecurity.com/aboutUs/trustedCenter/details/602>
- DataReportal. (2025, January). *Digital 2025: Global overview report*.  
<https://datareportal.com/reports/digital-2025-global-overview-report>
- Digital Report. (2017, August 18). В Узбекистане введут биометрические загранпаспорта с 1 января 2019 года [Uzbekistan will introduce biometric passports from January 1, 2019]. *Digital Report*.



- <https://digital.report/vuzbekistane-vvedut-biometricheskie-zagranpasporta-s-1-yanvarya-2019-goda/>
- Digital Report. (2017, June 5). Обзор Телеком Рынка Таджикистана: Фиксированная, Мобильная и Международная Связь [Tajikistan Telecom Market Overview: Fixed, Mobile and International Communications]. *Digital Report*. <https://digital.report/tadzhikistan-svyaz/>
- Enelane, N. (2019). Kak Rabotaet Proekt 'Sergek' [How the Sergek Project works]. *Informbiuro*. <https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html>
- European Commission. (2025, April). *EU-Central Asia factsheet*. [https://ec.europa.eu/commission/presscorner/api/files/attachment/881028/EU-Central%20Asia\\_Factsheet\\_2025-04.pdf](https://ec.europa.eu/commission/presscorner/api/files/attachment/881028/EU-Central%20Asia_Factsheet_2025-04.pdf)
- GDPR-info.eu. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved September 3, 2025, from <https://gdpr-info.eu/>
- Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Milanović, N., & Meijers, E. (2007). *Smart cities—Ranking of European medium-sized cities* (Working Paper). Vienna University of Technology.
- Gissonna, N. (2025, September 12). Great Firewall. In *Encyclopedia Britannica*. <https://www.britannica.com/topic/Great-Firewall>
- Huawei. (2022, May 17). Huawei prodoljaet razvivat' 5G v Uzbekistane [Huawei continues to develop 5G in Uzbekistan]. *Huawei*. <https://www.huawei.com/uz/news/uz/2022/huawei-prodoljaet-razvivat-5g-v-uzbekistane>
- Huawei. (n.d.). *Local states*. <https://www.huawei.com/uz/corporate-information/local-states>
- Huawei Cyber Security Evaluation Centre Oversight Board. (2019). *HCSEC Oversight Board report 2019*. Gove.uk. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/790270/HCSEC\\_OversightBoardReport-2019.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf)
- Informatsionnoe agentstvo Kazinform. (2023, May 19). Китай предоставит странам Центральной Азии грант в размере 1,5 млрд юаней [China will provide Central Asian countries with a grant of 1.5 billion yuan]. *Inform.kz*. <https://www.inform.kz/ru/kitay-predostavit-stranam-tsentralnoy-azii-grant-v-razmere-15-mlrd-yuaney-84dc6a/>
- International Telecommunication Union. (2020, December 1). More urgent than ever: Universal connectivity to bring 3.7 billion people online. *International Telecommunication Union*. <https://www.itu.int/hub/2020/12/more-urgent-than-ever-universal-connectivity-to-bring-3-7-billion-people-online/>
- Invest in Uzbekistan. (n.d.). *Huawei and ZTE contract with Uzbekistan is worth more than \$500 million*. Retrieved September 3, 2025, from <https://invest-in-uzbekistan.org/uz/novosti-uzbekistana/en-huawei-and-zte-contract-with-uzbekistan-is-worth-more-than-500-million/>

- Izimov, R. Yu., & Muratalieva, Z. T. (2018). Центральноазиатский трек инициативы «Пояс и путь»: возможности и риски [The Central Asian track of the Belt and Road Initiative: Opportunities and risks]. *Vestnik mezhdunarodnykh organizatsii*, 13(3), 128–142. <https://doi.org/10.17323/1996-7845-2018-03-08>
- Jardine, B. (2019, November 15). China's surveillance state has eyes on Central Asia. *Foreign Policy*. <https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-centralasia/>
- Law of the Republic of Kazakhstan No. 94-V. (2013, May 21; amended 2025, September 16). Закон Республики Казахстан «О персональных данных и их защите» [Law of the Republic of Kazakhstan on Personal Data and Their Protection]. *Әділет*. <https://adilet.zan.kz/rus/archive/docs/Z1300000094/16.09.2025>
- Law of the Kyrgyz Republic No. 85. (2023, April 14). Закон Кыргызской Республики «О персональных данных» [Law of the Kyrgyz Republic on Personal Data]. *Central Bank of Legal Information Data of the Kyrgyz Republic*. <https://cbd.minjust.gov.kg/3-48/edition/35412/ru>
- Law of the Republic of Tajikistan No. 1537. (2018, August 3). Закон Республики Таджикистан «О защите персональных данных» [Law of the Republic of Tajikistan on the Protection of Personal Data]. *National Center for Legislation under the President of the Republic of Tajikistan*. <https://ncz.tj/content/%D0%BE-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5-%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85>
- Law of Turkmenistan. (2017, March 22). Закон Туркменистана «Об информации и ее защите» [Law of Turkmenistan on Information and Its Protection]. *Ombudsman of Turkmenistan*. Retrieved October 3, 2025, from [https://ombudsman.gov.tm/doc/ru/%D0%BE%D0%B1\\_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8\\_%D0%B8\\_%D0%B5%D1%91\\_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5.rtf](https://ombudsman.gov.tm/doc/ru/%D0%BE%D0%B1_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8_%D0%B8_%D0%B5%D1%91_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5.rtf)
- Law of the Republic of Uzbekistan No. ZRU-547. (2019, July 2). Закон Республики Узбекистан «О персональных данных» [Law of the Republic of Uzbekistan on Personal Data]. *LEX.UZ*. <https://lex.uz/docs/4396428>
- Liu, C. (2020, July 9). BT, Vodafone need 5 years to replace Huawei without blackouts. *South China Morning Post*. <https://www.scmp.com/tech/gear/article/3092551/bt-vodafone-need-5-years-replace-huawei-without-blackouts>

- Manson, K., & Aglionby, J. (2018, January 29). African Union tries to expunge Chinese cyber-snooping. *Financial Times*.  
<https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5>
- Ministry of Foreign Affairs of the People's Republic of China. (2013, September 7). Состоялась встреча Си Цзиньпина и Н. Назарбаева [Meeting between Xi Jinping and N. Nazarbayev took place]. *Ministry of Foreign Affairs of the PRC*.  
[https://www.mfa.gov.cn/rus/zxxx/201309/t20130911\\_766180.html](https://www.mfa.gov.cn/rus/zxxx/201309/t20130911_766180.html)
- Resolution of the Government of the Republic of Kazakhstan No. 56. (2020, January 14). Постановление Правительства Республики Казахстан «О заключении Соглашения между Правительством Республики Казахстан и Правительством Китайской Народной Республики об оказании безвозмездной помощи по проекту «Оборудование и материалы для создания суперкомпьютерного центра» [On the conclusion of an Agreement between the Government of the Republic of Kazakhstan and the Government of the People's Republic of China on the provision of gratuitous assistance for the project Equipment and materials for the creation of a supercomputer center].  
<https://adilet.zan.kz/rus/docs/P2000000056>
- SecurityLab.ru. (2024, March 29). Обзор: Доклад Cloudflare о растущей зависимости мира от импортных технологий [Review: Cloudflare report on the world's growing dependence on imported technologies]. *SecurityLab.ru*.  
<https://www.securitylab.ru/news/554672.php>
- Shepardson, D. (2024, December 8). US House to vote to provide \$3 billion to remove Chinese telecoms equipment. *Reuters*.  
<https://www.reuters.com/world/us/us-house-vote-provide-3-billion-remove-chinese-telecoms-equipment-2024-12-08/>
- Sherman, J. (2019, May 28). What's the deal with Huawei and this African Union headquarters hack? *New America*.  
<https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/whats-the-deal-with-huawei-and-this-african-union-headquarters-hack/>
- South China Morning Post. (2017, October 16). China to build giant facial recognition database to identify anyone. *South China Morning Post*.  
<https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any>
- 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].
- Suchkov, M. A. (2022). «Геополитика технологий»: международные отношения в эпоху Четвертой промышленной революции [Geopolitics of technologies: International relations in the era of the Fourth Industrial Revolution]. *Vestnik Sankt-Peterburgskogo universiteta. Mezhdunarodnye otnosheniya*, 15(2), 138–157. <https://doi.org/10.21638/spbu06.2022.202>

- Sukhankin, S. (2021, February 11). Tracking the digital component of the BRI in Central Asia, Part One: Exporting 'Safe Cities' to Uzbekistan. *China Brief*, 21(3). Jamestown Foundation. <https://jamestown.org/program/tracking-the-digital-component-of-the-bri-in-central-asia-part-one-exporting-safe-cities-to-uzbekistan/>
- Tsz Yau Yan. (2019, August 7). Smart cities or surveillance? Huawei in Central Asia: Chinese surveillance technologies are popular among Central Asia's governments. *The Diplomat*. <https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/>
- Umarov, T. (n.d.). *China looms large in Central Asia*. Carnegie Moscow Center.
- United Nations. (2024). *Global digital compact*. <https://www.un.org/ru/summit-of-the-future/global-digital-compact>
- United Nations Development Programme. (2022). *Цифровая стратегия 2022–2025* [Digital strategy 2022–2025]. [https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-ABRIDGED-VERSION-PRINT\\_RU\\_Interactive.pdf](https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-ABRIDGED-VERSION-PRINT_RU_Interactive.pdf)
- University of Sheffield. (n.d.). *Clive Humby*. Retrieved September 3, 2025, from <https://sheffield.ac.uk/cs/people/academic-visitors/clive-humby>
- U.S. Agency for International Development. (n.d.). *Our mission*. Retrieved September 3, 2025, from <https://oig.usaid.gov/mission>
- Van Deursen, A. J. A. M., & Van Dijk, J. A. G. M. (2019). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *New Media & Society*, 21(2), 354–375.
- Van Dijk, J. A. G. M. (2006). Digital divide research, achievements and shortcomings. *Poetics*, 34(4–5), 221–235.
- Vitkine, B., & Leblond, J. (2018, January 26). À Addis-Abeba, le siège de l'Union africaine espionné par les Chinois [In Addis Ababa, the headquarters of the African Union spied on by the Chinese]. *Le Monde*. [https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois\\_5247521\\_3212.html](https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html)
- Vsemirnyj bank. (2024, January 12). Всемирный банк предоставляет дополнительную поддержку для цифровой трансформации Кыргызской Республики [World Bank provides additional support for the digital transformation of the Kyrgyz Republic] [Press release]. <https://www.vsemirnyjbank.org/ru/news/press-release/2024/01/12/world-bank-provides-additional-support-for-the-kyrgyz-republic-s-digital-transformation>
- The White House. (2025, January 1). *Presidential memorandum on reevaluating and realigning United States foreign aid* [Presidential Actions]. <https://www.whitehouse.gov/presidential-actions/2025/01/reevaluating-and-realigning-united-states-foreign-aid/>

Zhànshù Yǎnhuà. (2025, June 20). 15 亿白送? 中国与中亚的'硬核扶贫'背后真相揭秘 [1.5 billion for free? The truth behind China's hardcore poverty alleviation in Central Asia revealed]. *Baidu Baijiahao*.  
<https://baijiahao.baidu.com/s?id=1835350871890629685&wfr=spider&for=pc>