Digital Silk Road in Central Asia: Present and Future

NARGIS KASSENOVA & BRENDAN DUPREY

JUNE 2021

Davis Center FOR RUSSIAN AND EURASIAN STUDIES

NARXOZ UNIVERSITY

SKRI SUSTAINABLE KAZAKHSTAN RESEARCH INSTITUTE

FRIEDRICH EBERT STIFTUNG

Digital Silk Road in Central Asia: Present and Future

Nargis Kassenova & Brendan Duprey, Editors

JUNE 2021

Digital Silk Road in Central Asia: Present and Future is a project of the Davis Center for Russian and Eurasian Studies at Harvard University, and the Sustainable Kazakhstan Research Institute, Narxoz University, with support from Friedrich Ebert Foundation in Kazakhstan.

Cataloging-in-Publication data

ISBN: 978-0-578-93435-8

Please direct inquiries to:

Nargis Kassenova
Kathryn W. and Shelby Cullom Davis Center for Russian and Eurasian Studies
Harvard University
1730 Cambridge Street, Suite S301
Cambridge, MA 02138
Phone: 617.496.5684
Fax: 617.495.8319
nkassenova@fas.harvard.edu

The full text of this report can be accessed at https://daviscenter.fas.harvard.edu/digital-silk-road. Limited print copies are also available.

Contents

Acknowledgements

We would like to thank the Friedrich Ebert Foundation in Kazakhstan for providing moral and financial support to the project. Without the encouragement and help of Christoph Mohr and Medet Suleimen, this report would not have seen the light of the day.

We are grateful to Aida Aidarkulova, Bota Ayazbayeva, Aliya Sharipbayeva, Shamil Ibragimov, and Ilhom Abdulloev for sharing their knowledge of the budding digital rights field in Central Asia with us.

Our big thanks go to those who contributed to the report for their timely submissions and readiness to revise their texts. It was a great pleasure to jointly develop this project with them. We also owe our gratitude to Andrii Paziuk and Azamat Burzhuev who generously shared their expertise as well.

The report would have been less readable without the corrections from our editor, Eric Newman.

Last but not least, many thanks to Sarah Failla and Mary McGreal, the wonderful Communications team of the Davis Center for Russian and Eurasian Studies, for designing the report and adding the final touches.

Introduction

Dear Reader!

This report is the product of the joint project carried out by Harvard Davis Center for Russian and Eurasian Studies and the Sustainable Kazakhstan Research Institute at Narxoz University. It was triggered by our shared interest in the processes of digitalization and growing digital connectivity in Central Asia, and the role that China and Chinese information communication technology (ICT) companies play in them. We wanted to understand how various projects carried out by Chinese and Central Asian partners fit into both the Digital Silk Road (DSR), part of China's Belt and Road Initiative (BRI), and into the national digitalization policies developed by Central Asian states, what incentives they respond to, what opportunities they create, what challenges they face, and what implications they carry.

We used the notion of DSR to refer to all types of cooperation in the digital sphere. It is important to note, however, that the expansion of Chinese ICT companies to Central Asia preceded by many years the announcement of the DSR in 2015. Besides, China was not the first to combine digitalization and the Silk Road. In 2002, NATO launched the Virtual Silk Highway, a computer networking project for academic institutions in the Caucasus and Central Asia. China also does not have a monopoly on the term. In 2017, Kazakhstan adopted a "Digital Kazakhstan 2020" strategy that had the development of the Digital Silk Road as one of its components.

We chose to look at the DSR-related developments in Central Asia through the lens of governance and consider them at three levels: national, regional, and global. We could tackle this ambitious goal with the help of an excellent group composed of Central Asian and international experts. The Davis Center focused on studying digitalization and digital connectivity in the context of state–society relations and a focus on norms, regulations and capacities that determine the implementation of norms and regulations. The team from Narxoz University focused on the use of big earth data for improving systems thinking and Central Asia's performance in regards to sustainable development.

Given the increasing role digitalization plays in all aspects of our lives, governance of the digital sphere has become central for shaping our future. What kind of digital infrastructure is being built in Central Asian countries, and why? What technical specifications and standards does it have, and what dependencies does this create? Is there capacity to manage this new digital technology? How are regulations shaped and practiced? What are the prospective implications of further integration of plans and projects of Central Asian stakeholders into the Digital Silk Road? Here we offer an in-depth analysis of two cases: Kazakhstan and Turkmenistan. These Central Asian countries are at the opposite sides of the spectrum when it comes to being open or closed and having more capacity or less capacity.

The questions that we asked ourselves were: What does this new digital technology adopted by governments do to relations between the state and society? Who is empowered, and who might be disempowered as a result? In this regard, the trend of using surveillance technologies, growing in the region and globally, is of particular salience.

Central Asian governments have been enthusiastically importing and installing surveillance tech, primarily from China. As in the case of China, their initial motivation was to improve the problematic situation with traffic on the roads, and thereby enhancing public safety. However, they might also follow the big eastern neighbor into using the surveillance and big data technology to establish comprehensive control of the citizenry.

China is not the only source of inspiration and supplier of digital control and surveillance technologies. Russia, the traditional great power and model for Central Asians, also plays a role. A part of our report focuses on similarities and differences between the approaches adopted by the Russian and Chinese governments, their cooperation, and the impact on Central Asia. We also discuss their joint efforts to promote "digital sovereignty" and shape global digital governance. Central Asian governments have supported some of these efforts.We will continue to keep a close eye on the unfolding contestation over the norms of global digital governance.

All of the foregoing questions are critical to better understand the complex interactions between the digitalization of regional geopolitical strategies like the BRI, their interlinkages with national policies, and their subsequent outcomes for society. From a broader conceptual lens we must also analyze how digitalization can affect cooperation and joint decision making on global and regional challenges that Central Asian governments face, like climate change and human migration.

In this regard, the latter part of this book analyzes governance for the implementation of the Sustainable Development Goals (SDGs) in Central Asia. In 2015, governments around the world passed the SDGs as the overarching road map for human development focusing on its three core aspects: social, environmental, and economic. The digital revolution has provided policymakers and academics with a greater ability than at any other time in human history to understand the complex interactions between these areas on a regional and global scale. Big earth data deriving from earth-observation systems and ground-based observations, among others, can be analyzed to obtain an improved understanding of regional and global issues like climate change, human migration, and land-use patterns. In this context, the Big Earth Data Science Plan was established under the BRI to obtain big earth data in an organized way and accelerate the use of that data for its practical application in support of the implementation of the SDGs in countries participating in the BRI. The "Role of Big Earth Data for Governance for Sustainable Development" section explores ongoing environmental, social, and economic challenges facing Central Asia in the context of the implementation of the SDGs. Moreover, this section identifies some of the initiatives related to ongoing big earth data projects in Central Asia and potential interlinkages with the big earth data platform of the BRI.

This information is by no means meant to be an exhaustive list of topics linked with Central Asia's participation in the DSR Initiative. The authors' goal is to expand and update the book's content based on the ever-growing list of new developments in the digitialization process and the DSR Initiative. This book should be considered a live document that will grow and expand with new developments in the field of research.

We would like to thank the Friedrich Ebert Foundation (FES) in Kazakhstan for making this project possible. We hope this report and its findings will contribute to the public discourse on the role of Central Asia in the DSR Initiative. The authors foresee the content being used by a broad scope of stakeholders ranging from academics to civil servants in order to broaden their knowledge base in support of informed decision making regarding governmental policies and future academic endeavors. The interconnectedness between the digital world and social development will only continue to grow in the coming years. With this in mind, it is important to better understand and predict its consequences.

Nargis Kassenova and Brendan Duprey
22 June 2021

Executive Summary

Since its announcement in 2015, Digital Silk Road (DSR), aimed at "building a community with a shared future in cyberspace," has become an increasingly important part of the BRI agenda. It is composed of wide-ranging government announcements, state and private funding, and business ambitions. The DSR encompasses digital economy, artificial intelligence, nanotechnology, quantum computing, big data and cloud computing, and smart cities.

While infrastructure such as new railroads and ports visibly change the geography and the economy of BRI countries, the impact of a "Chinese Internet" that extends from infrastructure to hardware to software and services is less visible and harder to analyze. Is China creating a separate Sino-centric Internet among its neighbors and BRI clients? Will the world be divided into different Internets? Does the DSR, and the BRI generally, represent a unified strategy, or are they a series of ad hoc projects that fall under the same ideological umbrella, but with very different scope, actors, and goals?

Chinese companies and financing are strongly intertwined with those of other companies, in particular American and local ones. At the level of digital services such as e-commerce, the typical strategy of Chinese companies is to form local partnerships and leverage the existing digital ecosystem to enter a market and then establish their own presence. AliExpress is a good example of such flexible nature of the Chinese ICT industry's outward expansion, within and outside the DSR framework.

The DSR is likely to take very different shapes in different countries, with a mix of infrastructures, hardware, software, and services that will reflect pre-existing ecosystems and regional preferences. The "Chinese Internet" will be exported to BRI countries, but it will be absorbed into and become adapted by local realities, much as AliExpress is deploying diverse strategies and creating different partnerships in different countries.

China has been making efforts to shape global Internet governance. Russia is its key partner in this undertaking, and Central Asian governments occasionally play a supportive role. Over the past two decades Beijing and Moscow have been promoting a concept of Internet (digital) sovereignty that rejects the multi-stakeholder model of Internet governance, which they see as Western-dominated. China and Russia want governments to have greater control over digital infrastructure and content within their borders and play the dominant role in making global Internet policy.

The two governments share the goal, but they differ in their tactics. The Kremlin employs digital tools in an effort to undermine Western governments, sowing discord through social media platforms and spreading biased or fake news. These campaigns undercut Beijing's interest in stability and predictability, both in real life and on the Web. With a large financial stake in cybertechnologies and services, China also strives to maintain access to international markets for its core assets (e.g., Huawei, ZTE, Alibaba). These commercial considerations account for China's muted position (when compared with Russia's stance on key issues) and could eventually cause cracks in the partnership.

Moscow and Beijing regularly work together to advance cybersovereignty and state-centric Internet governance through the United Nations and regional organizations with varying degrees of success. The UN and its specialized agency the International Telecommunication Union (ITU) serve as forums of choice. In fact, Beijing and Moscow seek to transfer Internet governance from the Internet Corporation for Assigned Names and Numbers (ICANN) to the UN's ITU. Russia and China have twice proposed a resolution on an International Code of Conduct for Information Security to the United Nations General Assembly (UNGA). The initiative was supported by Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan but failed to gain traction in the UNGA. However, these states were successful in creating an UN Open-ended Working Group (OEWG) on cyber issues that boosted their status in global Internet policy making.

Multilateral cooperation efforts through regional organizations, such as SCO, EEU, and the BRICS, have been less fruitful. The inward-focused culture that pervades most CIS security services may act as a barrier to information sharing and supranational cooperation on the tactical level.

Surveillance Technology in Central Asia: Sources and Implications

Central Asia is rapidly developing its surveillance capacity by cooperating with Chinese ICT companies to create "Safe City projects." These companies largely work within the DSR framework and are active throughout much of the developing world. Safe City projects use facial recognition cameras, data management systems, and control centers to monitor the activity of citizens and levy fines. These projects promise to drastically improve domestic governance, which explains their popularity both within Central Asia and in the larger developing world, but they also dramatically increase the state's surveillance capacity as well. The reliance on Chinese ICT companies is also problematic because of the high risk of long-term reliance on China for further technological development and losing data sovereignty by allowing the Chinese government to access domestic information networks.

Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan all developed different Safe City projects within the past few years. Each utilizes facial recognition technology, biometric registries, and data management centers. Each country cooperated and continues to cooperate with Chinese ICT companies to create these systems, with several Chinese companies operating in multiple countries simultaneously. Notably, the timelines for development in each country are remarkably similar, and the changes in each country's regulatory environment are also similar. In effect, each country dramatically improved its surveillance networks within a short period of time, but in terms of regulations and data protections, no country in the region adequately protects either its own data sovereignty from foreign interference or its own citizenries from government overreach.

This is mirrored throughout the developing world and best demonstrated by the development of surveillance capacity in Ecuador. Ecuador's may have been one of the first pilot programs for Chinese ICT companies to see if exporting surveillance technology was a viable financial enterprise. In Ecuador, Chinese ICT companies have built a vast surveillance network called ECU-911 that includes thousands of cameras throughout the country, drones, facial recognition software, and a command center in which Chinese contractors work side by side with Ecuadorian government officials. The scope, scale, and sophistication of ECU-911 indicate the potential trajectory for other developing countries, including those in Central Asia, that are relying on Chinese ICT companies to develop safe city projects. The effect of domestic governance may be a positive for these countries, but the drawbacks are severe and include the strengthening of authoritarian tendencies throughout the developing world.

While Chinese companies are leading suppliers of surveillance technology, they do not keep full monopoly in the Central Asian market. Russian companies have carved a niche for themselves. Russia is also a model for policies and legislation for Central Asian states. These two countries and their companies play the most important role in shaping the digital governance landscape in Central Asia.

Sino-Russian digital relations feature a complex ecosystem with emulation and cooperation, as well as competition and suspicion. China functions predominantly as a supplier, exporting technology products and services and Internet control and surveillance models to Commonwealth of Independent States (CIS) countries. Russia, in contrast, both produces and consumes products and policy. The Russian government has signed lucrative contracts for Chinese information communications technology (ICT) and surveillance hardware and is increasingly implementing aspects of China's digital control methods.

Chinese and Russian leaders use digital information technology for surveillance and control. Each pursues its own breed of "digital authoritarianism." The differences are partially a relic of the particular ideological trajectories that guided the regimes and the historical circumstances facing the two states during the commercial Internet's birth. These legacies inform both states' current methods for filtering, censorship, and even surveillance. Russia relies on a lower-tech approach that promotes self-censorship, selective filtering, and more traditional telecommunications surveillance, all of which is backed by law. China's techniques are tech-heavy, employing artificial intelligence and impressive manpower to remove content and track citizens systematically. Understanding the two approaches is crucial to analyzing what drives ICT policy diffusion (or lack thereof) in Central Asia.

Digitization in Kazakhstan and Turkmenistan: Policies and Constraints

Kazakhstan has been at the forefront of digital transformation in Central Asia. Its first Public Service Centers and the e-gov portal (eGov.kz) were established in 2005–2007, aiming at improving the quality of public services and reducing pervasive corruption. They brought significant benefits to citizens by making procedures easier and cutting the waiting time. In 2017 the government introduced "Digital Kazakhstan," a national digitization/digitalization plan until 2020, modeled after the Singaporean Smart Nation initiative. It outlines four key areas of the long-term objectives to transform: economy, state, infrastructure, and human capital.

While significant progress is undeniable, Kazakhstan's digitalization agenda and implementation feature a number of shortcomings. The strategy is underdeveloped, and its implementation is not thought through. The emphasis is on introducing technologies fast and getting quick quantitative results to be reflected in various international indices and rankings. The government has assumed a more aggressive, nontransparent, and rapid approach to digitization of public services, neglecting a proper analysis of long-term benefits and side effects for the people, their freedoms, and trust in government. Not enough attention is paid to the provision of security, making the new systems vulnerable to data leaks and cyber-attacks. It remains unclear who has access to and controls the security of collection, processing, and storage of personal information. The government and other stakeholders need to practice a secure-by-design and secure-by-default approach to introducing new digital technology.

Instead of the security of data, Kazakhstan's government has been focusing on controlling the content of the Internet. Citizens are more worried about state surveillance than they are about the use and misuse of their private data by private companies. The current state-centric approach needs to change and put center stage the

personal data protection and the democratizing potential of the digitalization. The government needs to pay more attention to shaping digitization/digitalization culture, promoting cyber hygiene and digital literacy among its citizens.

The introduction of surveillance technology needs to be accompanied by strategic thinking. All digital plans and programs should build a healthy cyber ecosystem with credible legal norms and safety regulations, aimed at boosting economic welfare and developing new social rights. And if the Kazakh government could succeed in introducing strategic culture into its digitization efforts without surveillance stigmatization, it would receive higher support and better results in the long run.

Turkmenistan is lagging behind its neighbors in the region. In 2018 the government announced the Concept of the development of digital economy in Turkmenistan for 2019–2025. Prior to that there had been underdeveloped sector-focused (e.g., healthcare, tourism, etc.) digitization initiatives. The Concept bound them together, setting a unifying and ambitious target: the radical transformation of all economic sectors, social sphere, and public governance through the uptake of digital technologies.

These efforts all together are yielding some visible, albeit still modest, progress in the country's digital development. The Turkmen segment of the Internet is steadily expanding: Turkmen banks and financial institutions, state enterprises, and private companies are developing their own websites and expanding their e-services to citizens and businesses. The government's policy approach, however, has noticeable shortcomings. It focuses on digitalization as a tool to enhance the competitiveness of the national economy and neglects facilitating good governance and catalyzing social growth. No attention is paid to bridging the digital divide or developing digital literacy and cyber-hygiene skills among citizens.

The policy implementation leaves much to be desired. It is characterized by a general lag in quality, hastiness and disorganization, and lack of clearly identified priorities and interim objectives in e-governance. The governmental web portals, including the e-government platform, appear underdeveloped and visually outdated and have limited functional capacity, providing only a handful of e-services.

In the meantime, the Turkmen government has been strengthening repressive cyber capabilities. It blocks access to foreign media outlets, almost all social media platforms, and video hosting sites. The government also uses a wide range of tactics, such as DNS spoofing, HTTP Host Header Inspection and IP blocking, disruption of Internet service, and monitoring and eavesdropping, to detect and intimidate activists who post critical commentary about the government online. It is not surprising that Ashgabad is eager to develop cooperation with like-minded technology-exporting states, Russia and China, to improve its surveillance capacity.

The Role of Big Earth Data in Governance for Sustainable Development

The digital revolution has provided policymakers and academics with a greater ability than at any other time in human history to understand the complex interactions between social, environmental, and economic developments on a regional and global scale. Big Earth Data deriving from Earth observation systems and ground-based observations, among others, can be analyzed to obtain an improved understanding of issues like climate change, human migration, and land-use patterns, among others. In this context, the Big Earth Data Science Plan was established under the umbrella of the BRI to obtain big earth data in an organized way and accelerate the use

of that data for its practical application in support of the implementation of the SDGs (Sustainable Development Goals) in countries participating in the BRI. One of the core aspects of the Science Plan is the creation of a big earth data platform. Its overarching goal is to develop itself as a platform that will facilitate the sharing of Earth observation technologies and information services across Belt and Road countries.

Infrastructure projects and other investments deriving from the BRI can have both positive and negative impacts on the environment. Without comprehensive and integrated data on environmental and social impacts on these investments, however, mitigation and adaptation measures cannot be effectively enacted. Participation in and contribution to the big earth data platform of the Digital Belt and Road Program (DBAR) by Central Asian countries can have a variety of positive effects, including: building trust and improved collaboration between Central Asian countries, supporting the implementation of the SDGs on a regional level, building capacities and improving knowledge of Central Asian experts, and improving technological advancements.

The challenges of the effective implementation of the platform in Central Asia range from general mistrust between partners, insufficient human capacities, and lack of technological resources to conduct data collection. To overcome this mistrust, it is necessary to ensure the reliability of data included in the platform and address concerns over how the data will be used. Importantly, the big earth data system will be open source, providing users with free access to data. The acceptance of the platform would be enhanced if the FAIRness framework (where data must be Findable, Accessible, Interoperable, and Reusable) were enacted. Security and ethical concerns of stakeholders and society as a whole must also be taken into consideration.

It is important to raise awareness and build capacity in Central Asia. Most experts we addressed in the context of our research were not familiar with the Science Plan and had little understanding of its scope and implications. Setting up one or several International Centers for Excellence in Central Asia would be a step forward. Such center/s could provide on-the-ground support to the Initiative, as well as identify synergies and opportunities for collaboration.

The Puzzle of the Digital Silk Road

Elisa Oreglia, Hongyi Ren, and Chia-Chi Liao

When Xi Jinping announced the One Road One Belt Initiative in 2013, he outlined the idea of a newly reconstituted Silk Road, based on regional political and economic cooperation, improved road connectivity and trade, better monetary convertibility, and increasing understanding among people over an area that at the time was limited to China and Central Asia.[1] The speech was long in vision but short on details. It took two years before an Action Plan was issued to define the content of the by then renamed Belt and Road Initiative (BRI). In this plan, investments and projects related to the digital realm played a significant part. The "improved connectivity" of the original 2013 speech was expanded to include the construction of communication networks through "cross-border optical cable networks . . . transcontinental submarine optical cable projects . . . [and] spatial (satellite) information passageways."[2] The Information Silk Road, which later became the Digital Silk Road (DSR), was born. The digital component became an increasingly important part of Xi Jinping's speeches on the BRI and soon came to include the digital economy, artificial intelligence, nanotechnology, quantum computing, big data and cloud computing, and smart cities—all with the goal of "building a community with a shared future in cyberspace."[3]

It took a while for these guidelines to morph into concrete projects, but in the past two years the DSR seems to have gained momentum—or at least newspaper headlines that highlight how it could be a means to export the "Chinese Internet" into BRI countries.[4] Examples of projects linked to the DSR include the laying of fiber optic cables in BRI countries, the commercialization of smartphones with the Android operating system but with Chinese apps installed as default, agreements with BRI governments to use Beidou (the Chinese version of GPS) for military and civilian purposes, and the acquisition and localization of e-commerce websites.[5]

---

[1] "Promote Friendship Between Our People and Work Together to Build a Bright Future," Speech by Xi Jinping at Nazarbayev University, Astana, Kazakhstan, September 7, 2013, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1078088.shtml.

[2] National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of The People's Republic of China, "Action Plan on the Belt and Road Initiative," March 28, 2015, http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm.

[3] Sun Jingxin, "Post COVID19, the Value of the Digital Silk Road Will Be Even More Conspicuous" (*Hòu yìqíng shídài, shùzì sīchóu zhī lù jiàzhí jiāng gèng wèi zhāngxiǎn*), *China Today*, August 13, 2020, http://www.chinatoday.com.cn/zw2018/bktg/202008/t20200813_800217554.html.

[4] A 2018 article from *Foreign Affairs* synthetizes well what has become a common refrain in more recent English-language headlines; an Internet more dominated by Chinese hardware and software "will be less global and less open. A major part of it will run Chinese applications over Chinese-made hardware. And Beijing will reap the economic, diplomatic, national security, and intelligence benefits that once flowed to Washington" (Segal, 2018).

[5] Examples of concrete projects related to the Digital Silk Road include China Mobile's stepping up the deployment of the China-developed 4G/5G TD-LTE standard in BRI countries, Alibaba's building of data centers in key BRI countries (see Shen, 2018), the Pakistan-China Fiber Optic project (see Bhutta, 2018), the acquisition of the Burmese e-commerce platform shop.com.mm by Alibaba, and the localization of the online steel trading platform zhaogang.com through the opening of foreign branches and sales offices in BRI countries (see Thompson Chau, 2018).

How can we see the effects of the Digital Silk Road?

So far, the DSR has been a typically ambiguous assemblage of wide-ranging government announcements, state and private funding, and business ambitions that are reminiscent of various plans that China has been deploying since the early 2000s to "informatize" its economy and society.[6] One of the goals is to shape the digital worlds of BRI countries in multiple and often unseen ways.[7] It is not only providing the infrastructural backbone to extend fast internet to underserved areas but also making available the more mundane devices and services people rely on when using their phones or connecting to the Internet.

Yet while infrastructure such as new railroads and ports visibly changes the geography and the economy of BRI countries, the impact of a "Chinese Internet" that extends from infrastructure to hardware to software and services is less visible and harder to analyze. Even though seven years have passed since the announcement of this political vision, it is still unclear what it is exactly, beyond the headlines and announcements of projects that may or may not be realized. Is China creating a separate Sino-centric Internet among its neighbors and BRI clients? Will the world be divided into different Internets? Does the DSR, and the BRI generally, represent a unified strategy or are they a series of ad hoc projects that fall under the same ideological umbrella, but with very different scope, actors, and goals? And finally, how do we study the Digital Silk Road and its effects, given the complexity and layers that make up the "Internet," or, even more vaguely, the "digital world"?

Projects such as the Australian Strategic Policy Institute's *Mapping China's Tech Giants* and the U.S.-based Center for Strategic & International Studies' *Reconnecting Asia* provide a necessary first step to mapping companies and projects connected to the BRI and the DSR.[8] Their focus on Chinese investments and activities, however, leaves out the greater context of digital connectivity in different countries and makes it difficult to see whether and how it is changing. Despite an increasing Chinese presence at different points of the digital world of BRI (and other) countries, Chinese companies and financing are strongly intertwined with those of other companies, in particular American and local ones. At the level of digital services such as e-commerce, often the strategy of Chinese companies is to form local partnerships and leverage the existing digital ecosystem to enter a market and then establish their own presence, as we will see in the next section.

A Case Study in Flexibility: AliExpress

AliExpress, a cross-border e-commerce platform owned by Alibaba, is a good example of a Chinese company's deploying very flexible localization strategies to achieve global expansion. AliExpress is at the center of a very complex ecosystem that starts within China. In 2015, the Chinese government issued an "Internet Plus" plan that advocated the use of digital technologies for the development of traditional industries.[9] Shortly thereafter, Alibaba implemented its own "Internet Plus Foreign Trade" strategy, which consisted of a series of agreements with local

[6] Important national plans related to IT include the "National Informatization Development Strategic Plan 2006-2020," the "Framework for National Agriculture and Rural Informatization 2007–2015," the "Made in China" and "Internet Plus" plans launched in 2015.

[7] For an analysis of the motivations behind the Digital Silk Road, see Basu Das, 2017; Brown, 2017; Shen, 2018.

[8] ASPI's Mapping China's Tech Giants (https://chinatechmap.aspi.org.au) focuses on monitoring investments and projects by Chinese tech companies, while CSIS's Reconnecting Asia (https://reconasia.csis.org/) monitors infrastructural projects carried out by Chinese companies in different sectors, including IT.

[9] State Council, "The State Council's Guiding Opinions on actively promoting the 'Internet plus' action," July 1, 2015, http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm.

towns in China to set up cross-border industrial zones, where local industries could receive extra support and training from AliExpress to sell on international markets using the company's e-commerce facilities (AliExpress, 2020).[10] In 2019, AliExpress announced a new "Local to Global" strategy and began to sign agreements with a number of countries so that small and medium companies located in these countries could use the AliExpress network to sell their products in China and, in some cases, in third countries. To date, AliExpress has signed agreements with Russia, Turkey, Spain, Italy, and France.[11]

AliExpress's strategy is one of centralized control and local agreements in the domains of logistics, payments, and marketing. In terms of logistics, AliExpress's distribution network is managed by another subsidiary of Alibaba called Cainiao, which has developed two main distribution strategies with the aim of speeding up transportation and delivery. The first consists of creating directly owned AliExpress global warehouses to which goods are shipped from China and then distributed through local transport companies. Currently, there are AliExpress warehouses in twenty-four countries in North and South America, Europe, the Middle East, Africa, and Asia. These warehouses also support services for sellers, such as storage and handling of customer returns.

The second strategy consists of signing distribution agreements with logistics companies, both Chinese and international, which then handle the rest of the process. Payments are also dealt with in a similar way, through direct handling or through agreements with international or local companies. Direct handling is done through another subsidiary of Alibaba, Ant Financial, which owns the mobile money app Alipay. This can be used directly in a number of countries where Ant Financial has signed agreements with local banks or has pursued other partnerships. For example, in Cambodia AliExpress users can use the Alipay wallet through a partnership with the Cambodian payment company PiPay (Xinhua, 2017). In other countries, Ant Financial has invested in popular local mobile payment apps,[12] or has signed agreements with companies such as Visa, Mastercard, or other local financial companies whose payment methods are already widely used.[13]

Finally, in terms of marketing, AliExpress is developing extremely flexible localization strategies that leverage Chinese, international, and local marketing companies, tools, and partners. AliExpress actively cooperates with local companies to take advantage of their own local networks and know-how.

Central Asia represents a particularly interesting case study of AliExpress foreign expansion tactics. The region is central to the BRI project for historical, geographical and strategic reasons, and while the Chinese government has stretched the reach of its re-imagined Silk Road to include countries all around the world, many of the earlier logistics and transportation projects tied to the BRI were built in the region.[14]

From a digital perspective, Central Asia is at the crossroads of different digital ecosystems all coexisting in a tenuous balance. Russia is still an important influence, especially in terms of policies and in terms of Russian companies' market reach. At the same time, U.S. tech companies such as Instagram, Facebook, and Google

[10] See AliExpress Industrial Special Zones (https://sell.aliexpress.com/zh/__pc/2019_industry.htm?spm=5261.11333555.100.6.30b32fe0ULkaE8) and List of Logistics Schemes (https://sale.aliexpress.com/zh/__pc/seller/shipping_methods_list.htm?spm=5261.8174434.0.0.77653cc1ee6eSA).

[11] See Hai Xianhui, "AliExpress allows foreign retailers to sell," Sohu, October 5, 2019, last accessed on September 11, 2020. https://www.sohu.com/a/313197280_368681.

[12] For example, in Myanmar AntFinancial is investing in the mobile money app WaveMoney. See Miguel Cordon, "Ant Financial to pour $73.5m into Myanmar fintech firm Wave Money," Techinasia, May 18, 2020, https://www.techinasia.com/ant-financial-pour-73m-myanmar-fintech-wave-money.

[13] For example, in Kazakhstan people can pay on AliExpress using VISA, Mastercard, or local companies QiWi and Webmoney.

[14] See projects listed in CSIS's Reconnecting Asia map, https://reconasia.csis.org/map/. See also the historical and strategic analysis of the importance of Central Asia in Fatima Zhakypova et al. (2020) *Analysis of China's Economic Strategy and Foreign Policy in Kazakhstan*. Nur-Sultan: TALAP Center for Applied Research and Konrad Adenauer-Stiftung.

dominate the market in many Central Asian countries, and financial companies such as Visa and Mastercard play an important role in e-commerce. China is a latecomer but is making up for lost time through a mix of state-backed loans and agreement, big corporations' investments, and small traders' cross-border commercial activities.

AliExpress competes and collaborates with all these existing players at once, and in user-facing services, logistics, and payments alike. Part of its goal is to challenge Amazon's dominance in the business-to-consumer space.[15] For example, in order to manage its Central Asian marketing and business partnerships, in 2018 AliExpress set up the joint venture *AliExpress Russia* with Megafon, Mail.ru, and Russian Direct Investment Fund, companies that have a significant presence in Central Asian markets and understand both customer needs and local government requirements.[16] On the other hand, AliExpress encourages and trains Chinese companies to partner with local online influencers, in order to gain customers.[17]

To encourage buyers in different Central Asian countries, AliExpress leverages whichever social media networks are popular in the specific country, regardless of whether they are Russian, Chinese, American, or local. In Kazakhstan, AliExpress users can create an account on the platform using e-mail, or their login credentials from Apple, Facebook, Instagram, Google, Vkontakte, and ok.ru, these last two both owned by Mail.ru.[18] A platform-agnostic sign-in system simplifies the procedure of creating a new account and helps gain first-time users. Instagram, Facebook, YouTube, and Google Analytics are all used by Chinese sellers to advertise their AliExpress businesses and understand customers' behaviors, even though these websites are all banned in China.

Alibaba's experience in China has taught the company that it needs to grow the number of sellers alongside the number of buyers, and through AliExpress it is replicating this model in a handful of countries. In Kazakhstan, it launched a "School of Internet Exporter" (possibly modeled on its various e-commerce training schools and initiatives in China) in collaboration with local partners, to train local entrepreneurs to sell on AliExpress. The most promising participants were rewarded with a "Golden Supplier" icon on AliExpress, which allows the seller's mini-site, among other things, to be promoted among the top search results on AliExpress.[19] Becoming a "Golden Supplier" is not cheap. Among the 43 such suppliers registered so far, five obtained the highest supplier seal, which is subject to an annual fee of US$4,900, whereas the rest obtained the basic icon, which costs US$1,900. AliExpress made a total of 38.3 million *tenge* (approximately US$88,000) from Kazakh sellers' registration fees.[20] The results and uptake of the program are mixed, but other partnerships between Chinese and Kazakh educational institutions on one side, and Chinese tech companies including Tencent and JD.com on the other, are being developed. The international business is not only e-commerce, but also training to do international business on Chinese e-commerce platforms.

---

[15] James Kynge, "Alibaba Steps Up Competition with Amazon in Global Ecommerce Market." *Financial Times*, May 8, 2019, https://www.ft.com/content/3d25007c-713d-11e9-bbfb-5c68069fbd15.

[16] Alibaba, "RDIF, Alibaba Group, MegaFon and Mail.ru Group Launch New Social Commerce Joint Venture in Russia and the CIS," September 11, 2018, accessed September 5, 2020, https://www.alibabagroup.com/en/news/article?news=p180911.

[17] AliExpress, "List of Logistics Schemes," 2020, accessed August 28, 2020, https://sale.aliexpress.com/zh/__pc/seller/shipping_methods_list.htm?spm=5261.8174434.0.0.77653cc1ee6eSA.

[18] See AliExpress mobile app for Kazakhstan.

[19] For an in-depth description of various initiatives, including how they are perceived by Kazakh entrepreneurs, see Fatima Zhakypova et al. (2020), section 2.5, "Digitalization of Relations: Introducing Chinese Technology Giants Into the Kazakh Market."

[20] This is according to data issued by the Kazakh Embassy in China, reported on the Chinese Ministry of Commerce website: "Top 10 Kazakhstan "Gold Suppliers" on Alibaba Platform (Alibabaāpíngtái shàng de shí dà hasàkè sitan "jinpái gongyìng sheng)," http://kz.mofcom.gov.cn/article/fb/202010/20201003007950.shtml.

Payment for online purchases is another area that requires a great flexibility, to accommodate consumers who are already embedded in specific financial arrangements or do not have credit cards, a common situation in many BRI countries. AliExpress cooperates with local and international companies to adapt its payment conditions to local preferences, and supports eleven international credit card groups, in addition to having cooperation agreements with thirty-eight local payment channels around the world, including native mobile payment systems such as MPesa in Kenya.[21] In Central Asia, AliExpress clients can use Visa and Mastercard, but also QIWI and WebMoney, widespread Russian digital payment platforms. QIWI Wallet on AliExpress.com is built on the API of Alipay, China's leading third-party online payment platform—a clear example of the tension between collaboration and competition that exists among Russian and Chinese companies in the area.[22] Another example of localization in central Asia comes from Kazakhstan, where in 2017 AliExpress issued a credit card offering a 1.5 percent cash-back for purchases on its site and other benefits, in collaboration with Kazpost JSC, the national postal service, which serves also as a bank and a logistics company, and which is actively engaged in developing e-commerce in the country.[23]

Conclusion

AliExpress is a good example of the extremely flexible nature of the Chinese IT industry's outward expansion, within and outside the Digital Silk Road framework. Broad globalization strategies, pushed by both the Chinese government and by companies' headquarters, go hand-in-hand with highly tailored localization strategies that aim to secure market share through multi-pronged partnerships, investments, and tools. This central strategy, followed by flexibility with and adaptability to local circumstances in its actuation, mirrors what has happened with China's internal informatization plans discussed earlier: a strategy document and set of general guidelines coming from the central government, followed by creative and flexible implementation plans carried out by local governments and companies, including the re-labeling or re-orienting of existing projects to fit central plans.

Much still needs to be studied about the Digital Silk Road, but it seems likely that it will end up taking very different shapes in different countries, with a mix of infrastructures, hardware, software, and services that will reflect pre-existing eco-systems and regional preferences. The "Chinese Internet" will be exported to BRI countries but will be absorbed into and become adapted by local realities, much as AliExpress is deploying diverse strategies and creating different partnerships in different countries.

Bibliography

21st Century Business Herald. "A Further Upgrade in Russia's Logistics, AliExpress Deepens Ties with the European Market" (Èluósī wùliú zài shēngjí sù mài tōng shēngēng ōuzhōu shìchǎng.), December 26, 2019. Accessed March 13, 2021. http://www.21jingji.com/2019/12-26/0NMDEzODFfMTUyMzk0NA.html.

---

[21] "A further upgrade in Russia's logistics, AliExpress deepens ties with the European market" (Èluósī wùliú zài shēngjí sù mài tōng shēngēng ōuzhōu shìchǎng) *21st Century Business Herald* https://kuaibao.qq.com/s/20191226AZP65G00

[22] "QIWI Offers Russian Online Shoppers Local Payment Options on AliExpress.com," *QiWi Wallet*, 2012, https://investor.qiwi.com/index.php/news-releases/news-release-details/qiwi-offers-russian-online-shoppers-local-payment-options.

[23] See the different AliExpress-branded KazPost credit card at https://post.kz/.

Alibaba. "RDIF, Alibaba Group, MegaFon and Mail.ru Group Launch New Social Commerce Joint Venture in Russia and the CIS," September 11, 2018. Accessed September 5, 2020. https://www.alibabagroup.com/en/news/article?news=p180911.

AliExpress. "Industrial Special Zones," 2019. Accessed August 28, 2020. https://sell.aliexpress.com/zh/__pc/2019_industry.htm?spm=5261.11333555.100.6.30b32fe0ULkaE8.

AliExpress. "List of Logistics Schemes," 2020. Accessed August 28, 2020. https://sale.aliexpress.com/zh/__pc/seller/shipping_methods_list.htm?spm=5261.8174434.0.0.77653cc1ee6eSA.

Bhutta, Zafar. "Optic Fibre Cable Connecting Pakistan, China to Be Inaugurated Today," The Express Tribune, July 13, 2018. Accessed March 13, 2021. https://tribune.com.pk/story/1756458/2-optic-fibre-cable-connecting-pakistan-china-inaugurated-today.

Brown, Rachel. *Beijing's Silk Road Goes Digital*. Council on Foreign Relations, 2017. Accessed July 20, 2020. https://www.cfr.org/blog/beijings-silk-road-goes-digital.

Cordon. Miguel. "Ant Financial to Pour $73.5m into Myanmar Fintech Firm Wave Money." *Techinasia,* May 18, 2020. Accessed September 1, 2020. https://www.techinasia.com/ant-financial-pour-73m-myanmar-fintech-wave-money.

Das, Sanchita Basu. *OBOR's Digital Connectivity Offers Both Benefits and Risks*. ISEAS Yusof Ishak Institute, 2017. Accessed March 13, 2021. http://hdl.handle.net/11540/7454.
Economic and Commercial Section of the Embassy of the Republic of Kazakhstan. 2020. "Top 10 Kazakhstan 'Gold Suppliers' on Alibaba Platform (Alibaba píngtái shàng de shí dà hasàkè sitan "jinpái gongyìng sheng"). Accessed November 2, 2020. http://kz.mofcom.gov.cn/article/fb/202010/20201003007950.shtml.

Hai, Xianhui. "AliExpress Allows Foreign Retailers to Sell." Sohu, October 5, 2019. Accessed September 3, 2020. https://www.sohu.com/a/313197280_368681.

Kynge, James. "Alibaba Steps Up Competition with Amazon in Global Ecommerce Market." *Financial Times*, May 8, 2019. Accessed November 3, 2020. https://www.ft.com/content/3d25007c-713d-11e9-bbfb-5c68069fbd15.

Ministry of Foreign Affairs of the PRC. "Promote Friendship Between Our People and Work Together to Build a Bright Future." Speech by Xi Jinping at Nazarbayev University, Astana, Kazakhstan, September 7, 2013. Accessed July 25, 2020. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1078088.shtml.

National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of the People's Republic of China. "Action Plan on the Belt and Road Initiative," March 30, 2015. Accessed March 13, 2021. http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm.

Segal, Adam. "When China Rules the Web: Technology in Service of the State." *Foreign Affairs* 97:10, 2018.

Shen, Hong. "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative." *International Journal of Communication* 12, 2018, pp. 2683–2701.

State Council. "The State Council's Guiding Opinions on Actively Promoting the 'Internet Plus' Action" (Guówùyuàn guānyú jījí tuījìn "hùliánwǎng +" xíngdòng de zhǐdǎo yìjiàn), 2018. Accessed March 13, 2021. http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm.

Thompson Chau, Thiha Ko Ko. "Alibaba Secures Foothold in Myanmar Market, Growth in e-Commerce Expected." *Myanmar Times*, May 22, 2018.

QiWi Wallet. "QIWI Offers Russian Online Shoppers Local Payment Options on AliExpress.com," May 5, 2012. Accessed: 3 November 2020. https://investor.qiwi.com/index.php/news-releases/news-release-details/qiwi-offers-russian-online-shoppers-local-payment-options.

Xinhua. "China's Alipay Signs Partnership Deal with Cambodia's Pi Pay." *China Daily*, December 21, 2017. Accessed September 5, 2020. http://www.chinadaily.com.cn/a/201712/21/WS5a3b184ca31008cf16da295f.html.

Zhakypova, Fatima., et al. *Analysis of China's Economic Strategy and Foreign Policy in Kazakhstan.* Nur-Sultan: TALAP Center for Applied Research and Konrad Adenauer-Stiftung, 2020.

Sino-Russian Advocacy for "Internet Sovereignty" and State-Led Internet Governance

Miranda Lupion[1]

Moscow and Beijing often invoke the concept of national sovereignty to justify domestic governing decisions that contradict Western norms, such as a broad interpretation of human rights. Over the past two decades, Russia and China have sought to extend this historical claim to the digital sphere, advocating for Internet sovereignty. Also known as digital sovereignty, Internet sovereignty rejects the multi-stakeholder model of Internet governance, which Russia and China see as Western-dominated, to give governments (1) greater control over digital infrastructure and content within their borders and (2) the dominant role in making global Internet policy.[2] The two countries' digital authoritarian policies and shared goal of regime stability drive cooperation over Internet issues.[3] Moscow and Beijing regularly work together to advance cyber sovereignty and state-centric Internet governance through the United Nations and regional organizations with varying degrees of success.

The Logic and Limits of Cyber Alignment

Experts trace recent Sino-Russian cooperation to 2014. In the wake of the Crimean annexation, the European Union and the United States sought to isolate Russia economically and diplomatically. In response, Russia "pivoted to the East."[4] Moscow embarked on a campaign to expand economic, energy, and political ties with Beijing.[5] At the same time, the Internet's center of gravity was also shifting east. China and Russia began to claim more of the World Wide Web's users and demand a greater say in the way it is run.[6] Joint advocacy for mutually beneficial Internet governance policies followed. The new-found partnership, however, is asymmetric. Beijing sees Moscow as a declining power and not a rising hegemon.[7] China is Russia's largest trading partner, but Russia does not make China's top ten.[8]

---

[1] Research carried out as part of a Title VI–funded Innovation Fellowship at, and on behalf of, the Davis Center for Russian and Eurasian Studies.

[2] Dennis Broeders, Liisi Adamson, and Rogier Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace" (The Hague Program for Cyber Norms Policy Brief, November 2019); Alexander Gabuev, "Digital Bromance: The Sino-Russian Partnership Racing Ahead," Carnegie Moscow Center, December 7, 2015, https://carnegie.ru/2015/12/07/digital-bromance-sino-russian-partnership-racing-ahead-pub-62253.

[3] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace," 5.

[4] Gabuev, "Digital Bromance."

[5] Alexander Gabuev, "The Pandemic Could Tighten China's Grip on Eurasia," Carnegie Moscow Center, April 24, 2020, https://carnegie.ru/2020/04/24/pandemic-could-tighten-china-s-grip-on-eurasia-pub-81635.

[6] Julien Nocetti, "Contest and Conquest: Russia and Global Internet Governance," *International Affairs* 91, no. 1 (2015): 111.

[7] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace," 7.

[8] Ibid., 5.

Absent any major disputes, Sino-Russian cooperation is likely to continue in the near-to-medium-term. The countries hold similar although not identical positions on critical digital questions: they oppose the "denationalized liberalism" and norms of free speech and Internet freedom that came with the Web's early development. Considering online information potentially destabilizing, the regimes reject these norms. They seek to challenge the resulting non-hierarchical multi-stakeholder governance model, which gives companies, nonprofits, engineers, and states a say in running the Internet.[9] They also both fear cyber conflict.[10]

The states do differ in their tactics for achieving change. The Kremlin employs digital tactics in an effort to undermine Western governments, sowing discord through social media platforms and spreading biased or fake news. These campaigns undercut Beijing's interest in stability and predictability, both in real life and on the Web.[11] (Although, with the onset of the COVID-19 pandemic, China may be adopting Russia's playbook.[12]) With a large financial stake in cybertechnologies and services, China also strives to maintain access to international markets for its core assets (i.e., Huawei, ZTE, Alibaba).[13] Tencent and Alibaba invest in startups in the United States and the European Union.[14] These commercial considerations account for China's comparatively muted position (when compared with Russia's stance on key issues) and could eventually cause cracks in the partnership. They explain why Russia often leads in Internet sovereignty efforts.[15]

Bilateral Treaties and Talks

China and Russia cooperate to advance the Internet sovereignty agenda, working on both bilateral and multilateral levels. Heralded by some as a cyber "nonaggression pact" and unprecedented in its detail, the May 2015 agreement on information security codifies joint beliefs and grounds bilateral cooperation.[16] It explicitly affirms that sovereignty and related international norms apply to the Internet and expresses "concern" about the use of Internet technology to undercut state security and influence internal affairs. "International information security" is highlighted as a key element of security. Article 2 defines the main threats to international information security, including those that "destabilize the internal political and socio-economic" orders. Article 3 outlines areas of Sino-Russian cooperation. These include technology and expert exchanges, cooperation on issues within the framework of international governmental organizations (IGOs), joint training, confidence-building measures,

---

[9] Nocetti, "Contest and Conquest: Russia and Global Internet Governance," 117.

[10] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace," 1.

[11] Broeders, Adamson, and Creemers, 7.

[12] Jessica Brandt and Torrey Taussig, "The Kremlin's Disinformation Playbook Goes to Beijing," *Brookings* (blog), May 19, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.

[13] Ibid., 3–4.

[14] Kieron O'Hara and Wendy Hall, "Four Internets: The Geopolitics of Digital Governance" (Centre for International Governance Innovation, December 2018).

[15] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace," 3.

[16] Elaine Korzak, "The Next Level For Russia-China Cyberspace Cooperation?," Council on Foreign Relations, *Net Politics* (blog), August 20, 2015, https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation.

information sharing for law enforcement purposes, and even coordinated responses to cyberthreats.[17] Some experts see Article 4 as a cyber non-aggression pact. The parties plan to implement these measures through two consultation meetings each year.[18]

Russia and China followed up this agreement with bilateral talks and high-level meetings. At the 2015 World Internet Conference in Wuzhen, then–Prime Minister Dmitry Medvedev met with Alibaba CEO Jack Ma.[19] In a 2016 joint statement, Russia and China affirmed that non-interference, as defined in the UN Charter, applies in cyberspace. The statement also called on the entire international community to avoid conflict in cyberspace.[20]

Most recently, the media reported that China and Russia planned to sign an "agreement on illegal online content." The 2019 document was slated to have treaty status. Roskomnadzor claimed it would sign the agreement along with its counterpart on October 20. China, however, has yet to comment on the agreement.[21] The text is not publicly available, and it is unclear if both parties actually concluded the agreement.

Mixed Results at the UN and ITU

Russia and China promote these ideas through global IGOs as well. The United Nations and its specialized agency, the International Telecommunication Union (ITU), serve as forums of choice. In fact, Beijing and Moscow seek to transfer Internet governance from the Internet Corporation for Assigned Names and Numbers (ICANN) to the UN's ITU.[22] Under a U.S. Department of Commerce contract, ICANN allocates Internet Protocol (IP) addresses globally and manages parts of the Domain Name System (DNS). Although ICANN features representatives from industry (Internet service providers, engineers), civil society (NGOs), and governments around the world, Russia and China see the organization as privileging the United States.[23] At a 2010 ITU meeting in Guadalajara, the states proposed to give ". . . a specially-constituted group within ITU with the authority to veto decisions adopted by the ICANN Board of Directors."[24] This move was particularly brazen, given that ICANN lacks an ITU representative and thus was unable to respond directly to the proposal. Although the ITU scrapped the veto scheme, China later used its ITU chairship to push for measures allowing "government micromanagement" of the Internet.[25]

---

[17] "On Signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in Ensuring International Information Security," Pub. L. No. No. 788-p, 1 (2015), https://www.documentcloud.org/documents/2076545-5amaccs7mslxgbff1ua785wwmwcabdjw.html.

[18] Korzak, "The Next Level For Russia-China Cyberspace Cooperation?"

[19] Gabuev, "Digital Bromance."

[20] Lincoln Davidson, "Despite Cyber Agreements, Russia and China Are Not as Close as You Think," Council on Foreign Relations, *Net Politics* (blog), June 30, 2016, https://www.cfr.org/blog/despite-cyber-agreements-russia-and-china-are-not-close-you-think.

[21] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace," 5–6; "Russia and China to Sign Agreement on Combating Illegal Online Content," The Moscow Times, October 8, 2019, https://www.themoscowtimes.com/2019/10/08/russia-and-china-to-sign-agreement-on-combating-illegal-online-content-a67640.

[22] Gabuev, "Digital Bromance."

[23] Nocetti, "Contest and Conquest: Russia and Global Internet Governance," 117.

[24] Gregory Francis, "Plutocrats and the Internet," Circle ID, October 4, 2010, http://www.circleid.com/posts/20101004_plutocrats_and_the_internet/.

[25] O'Hara and Hall, "Four Internets: The Geopolitics of Digital Governance," 8.

Despite ICANN's dominance, the two states continue to work through the UN. They have twice proposed a resolution on an International Code of Conduct for Information Security to the United Nations General Assembly (UNGA). In 2011, Tajikistan and Uzbekistan joined China and Russia in endorsing the resolution. In 2015, Russia submitted the updated version on behalf of the Shanghai Cooperation Organization (SCO), which includes Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.[26] The agreement consisted of twelve voluntary commitments that stressed the right of states to determine Internet policy.[27] The resolution called on governments to "curb the dissemination of information that incites terrorism, secessionism, or extremism, or that undermines other countries' political, economic, and social stability, as well as their spiritual and cultural environment."[28] Critics claimed this clause would, in practice, legitimize Internet filtering—particularly of anti-regime content. It also sought to establish a non-aggression norm, asking states not to use ICT to undermine "international stability and security" and infrastructure.[29] The Code of Conduct failed to gain traction in the UNGA.

In November 2018, however, Russia and China advanced their agenda with the creation of a UN Open-ended Working Group (OEWG) on cyber issues. Previously, China and Russia participated in the nonbinding UN Group of Government Experts (GGE). The group met annually for discussion. In 2017, the UN GGE failed to achieve consensus and did not issue policy recommendations. The United States and its Western allies voted for a new round of GGE meetings, while Russia, with Chinese support, proposed a separate OEWG. Both resolutions passed, and the competing groups began work in 2019. The existence of a parallel expert body legitimizes Russia's and China's Internet sovereignty goals and boosts their status in global Internet policy making.[30]

The year 2019 brought an additional victory for Sino-Russian cyber efforts. In December, the NGA voted 79 to 60 (with 33 abstentions) to establish a committee of experts to draft a new cybercrime treaty. In its resolution, Russia argued that the 2004 Budapest Convention was outdated and violated principles of sovereignty and non-interference. Experts consider the resolution's language on ICT use for "criminal purposes" to be vague; the clause could give governments cover to censor or prosecute opposition members.[31] The intergovernmental committee was supposed to meet in August 2020 to begin work on a new treaty, but the session was postponed because of the COVID-19 pandemic. Russia and China issued a joint statement reaffirming their commitment to this treaty and planning for a committee meeting no later than March 2021.[32]

---

[26] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace," 3.

[27] Nocetti, "Contest and Conquest: Russia and Global Internet Governance," 123.

[28] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3826.

[29] Nocetti, "Contest and Conquest: Russia and Global Internet Governance," 123.

[30] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace," 11–12.

[31] Joyce Hakmeh and Allison Peters, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet," *Net Politics* (blog), January 13, 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

[32] "Draft decision entitled, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (A/74/L.84)," The United Nationals General Assembly, August 14, 2020, https://www.un.org/pga/74/wp-content/uploads/sites/99/2020/08/rev_PGA-LETTER-ON-CONCLUSION-OF-SP-ON-A-74-L.84-CYBERCRIME-1.pdf.

Much Ado About Nothing: Advocacy Through Regional Organizations

Multilateral cooperation efforts through regional organizations, such as SCO, EEU, and the BRICS, have been less fruitful. The inward-focused culture that pervades most CIS security services may act as a barrier to information sharing and supranational cooperation on the tactical level.[33]

The lack of concrete and long-term progress on these issues is particularly evident in SCO and Collective Security Treaty Organization (CSTO) projects. The SCO, whose members China, Russia, India, Pakistan, Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan, advocates for "protective integration against international norms."[34] While the organization projects outward unity in cyber affairs, its members have achieved little material gain. In 2009, the parties signed a cooperation agreement on international information security, which came into force in 2011.[35] A summit in 2012 followed, where member states committed their secret services to vague joint measures against terrorist activity on the Internet.[36] These measures fell short of what Kazakhstan's former President Nursultan Nazarbayev had proposed. He had sought an alliance-wide cyber police force that would legally codify digital sovereignty and borders.[37] This example reflects the way SCO activity more often legitimizes members' domestic digital control policies than leads to robust and deep coordination.

Sometimes called the "NATO of the East," the CSTO is a military alliance composed of former Soviet countries Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, and Tajikistan.[38] In response to the Arab Spring Protests and Color Revolutions, the organization developed a unified system for fighting "threatening digital content."[39] Under operation PROKSI (sometimes transliterated as PROXI), CSTO countries cooperated to take down 2,000 websites that they assessed were spreading damaging information.[40] In Russia alone, 216 websites went dark, supposedly in connection with these efforts.[41] The project was short-lived, apparently quietly abandoned in 2010.[42] The organization has also postponed other efforts, such as establishing a joint information security center called CISCERT, indefinitely.[43] Similar proposals, like the creation of a CIS Center for Cybersecurity and a 2017 plan for a BRICS (Brazil, Russia, India, China, and South Africa) Internet have also fallen through.[44]

---

[33] Andrei Soldatov and Irina Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You," WIRED, 2012, https://www.wired.com/2012/12/russias-hand/.

[34] Nocetti, "Contest and Conquest: Russia and Global Internet Governance," 124.

[35] Ibid., 124.

[36] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3826.

[37] Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

[38] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3825.

[39] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3825.

[40] Ibid.

[41] Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

[42] Ibid.

[43] Ibid.

[44] Adee, "The Global Internet Is Disintegrating. What Comes Next?"; Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3824.

The Road Ahead: An Alliance of Convenience and the Endurance of the Multi-stakeholder Model

Although China and Russia share digital governance goals, this new Sino-Russian "alliance" will not undermine multi-stakeholder Internet governance, at least in the medium-term. First, cooperation over cyber issues does not signal a permanent alliance or even temporary alliance in the traditional sense of the term; China eschews long-term alliances and permanent partnerships. Instead, the linkup is an additional mechanism for counterbalancing perceived U.S. hegemony, especially on issues of Internet freedom.[45] (The COVID-19 pandemic, however, has deepened Sino-Russian relations and temporarily lessened the partnership's asymmetry, as China depends more on Russia for trade.[46])

Second, while Beijing and Moscow do join forces to advocate for Internet sovereignty and state-centered Internet governance, their efforts have yielded mixed results at best. Russia and China likely recognize that overturning ingrained Internet freedom and governance norms at the global level is unattainable. Their advocacy activities actually serve two different purposes; they (1) provide a pretext for their domestic control policies and (2) help other hybrid and authoritarian states justify adopting similar regimes. Russia and China already practice filtering and exert *de facto* sovereignty over their respective cyberspaces. The multi-stakeholder governance model does not significantly impede their work.

Bibliography

Adee, Sally. "The Global Internet Is Disintegrating. What Comes Next?" BBC, May 14, 2019. https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

Broeders, Dennis, Liisi Adamson, and Rogier Creemers. "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace." The Hague Program for Cyber Norms Policy Brief, November 2019.

Creemers, Rogier. "The International and Foreign Policy Impact of China's AI and Big Data Strategies." In *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas Wright, 112–27. Strategic Multilayer Assessment (SMA) Periodic Publication. Department of Defense, 2018.

Davidson, Lincoln. "Despite Cyber Agreements, Russia and China Are Not as Close as You Think." Council on Foreign Relations. *Net Politics* (blog), June 30, 2016. https://www.cfr.org/blog/despite-cyber-agreements-russia-and-china-are-not-close-you-think.

Francis, Gregory. "Plutocrats and the Internet." Circle ID, October 4, 2010. http://www.circleid.com/posts/20101004_plutocrats_and_the_internet/.

[45] Davidson, "Despite Cyber Agreements, Russia and China Are Not as Close as You Think."

[46] Gabuev, "The Pandemic Could Tighten China's Grip on Eurasia."

Gabuev, Alexander. "Digital Bromance: The Sino-Russian Partnership Racing Ahead." Carnegie Moscow Center, December 7, 2015. https://carnegie.ru/2015/12/07/digital-bromance-sino-russian-partnership-racing-ahead-pub-62253.

———. "The Pandemic Could Tighten China's Grip on Eurasia." Carnegie Moscow Center, April 24, 2020. https://carnegie.ru/2020/04/24/pandemic-could-tighten-china-s-grip-on-eurasia-pub-81635.

Hakmeh, Joyce, and Allison Peters. "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet." *Net Politics* (blog), January 13, 2020. https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

Kerr, Jaclyn. "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region." *International Journal of Communication* 12 (2018): 3814–34.

Korzak, Elaine. "The Next Level For Russia-China Cyberspace Cooperation?" Council on Foreign Relations. *Net Politics* (blog), August 20, 2015. https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation.

Nocetti, Julien. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* 91, no. 1 (2015): 111–30.

O'Hara, Kieron, and Wendy Hall. "Four Internets: The Geopolitics of Digital Governance." Centre for International Governance Innovation, December 2018.

On signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security, Pub. L. No. No. 788-p, 1 (2015). https://www.documentcloud.org/documents/2076545-5amaccs7mslxgbff1ua785wwmwcabdjw.html.

The Moscow Times. "Russia and China to Sign Agreement on Combating Illegal Online Content," October 8, 2019. https://www.themoscowtimes.com/2019/10/08/russia-and-china-to-sign-agreement-on-combating-illegal-online-content-a67640.

Soldatov, Andrei, and Irina Borogan. "In Ex-Soviet States, Russian Spy Tech Still Watches You." WIRED, 2012. https://www.wired.com/2012/12/russias-hand/.

Taussig, Jessica Brandt and Torrey. "The Kremlin's Disinformation Playbook Goes to Beijing." *Brookings* (blog), May 19, 2020. https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/.

Uchill, Joe. "Russia and China Get a Big Win on Internet 'Sovereignty.'" Axios, November 21, 2019. https://www.axios.com/russia-china-united-nations-internet-sovereignty-3b4c14d0-a875-43a2-85cf-21497723c2ab.html.

https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.

Digital Silk Road and Surveillance Technology in Central Asia

Cian Stryker[1]

Modern surveillance technology has allowed states to surpass the traditional limitations of suppression. States across the globe utilize technology to monitor domestic activity in every way possible. Governments screen emails, listen in on phone calls, collect purchasing-history data, and use facial recognition technology (FRT) to monitor behavior in public spaces. The power balance between governments and people has historically been defined by the capacity of governments to control their citizens, but digital surveillance has the potential to radically increase this capacity and thus adversely affect overall state–societal relations. This trend is not unique to the developed world. The rapid growth of digital surveillance in Central Asia demonstrates the profound impact this trend will have on state–societal relations globally.

Central Asia comprises five post-Soviet republics that are all developing states and are either fully authoritarian or, at best, semi-democratic. They have histories of domestic suppression, and each regime has incentives for pursuing more sophisticated digital surveillance technology. The region is a major target of China's Belt and Road Initiative (BRI), which means it has also become a participant to many of BRI's digital enterprises. Chinese Information and Communication Technology (ICT) companies have begun exporting mass surveillance systems globally through BRI's subsidiary the Digital Silk Road, and Central Asia has become a frequent client.[2] Central Asian states are actively pursuing advanced surveillance technology supposedly to improve domestic governance, but an important byproduct is the large increase in suppressive capacity.

This paper analyzes the range of the digital mass surveillance in the region with attention paid to the technologies involved, foreign companies present, changes in legislation, and adaptations in governance. I provide a regional overview with economic climate, regime type, and indicators of governance depicted through descriptive statistics and visualizations.[3] The economic climate is portrayed with GDP data from the World Bank.[4] Regime descriptions rely on the Freedom House's "Freedom in the World" index, which is measured on a 100-point scale.[5] Governance draws on the "Rule of Law" and "Government Effectiveness" indicators calculated by the World Bank project on governance, both of which are also measured on a 100-point scale.[6] After the regional overview, each country is analyzed individually, but every country section is broken down into three parts: country profile, digital infrastructure, and regulatory environment.

---

[1] Research carried out as part of a Title VI–funded Innovation Fellowship at, and on behalf of, the Davis Center for Russian and Eurasian Studies.

[2] 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/.

[3] All visualization code can be found at https://github.com/CianStryker/Thesis_Project.

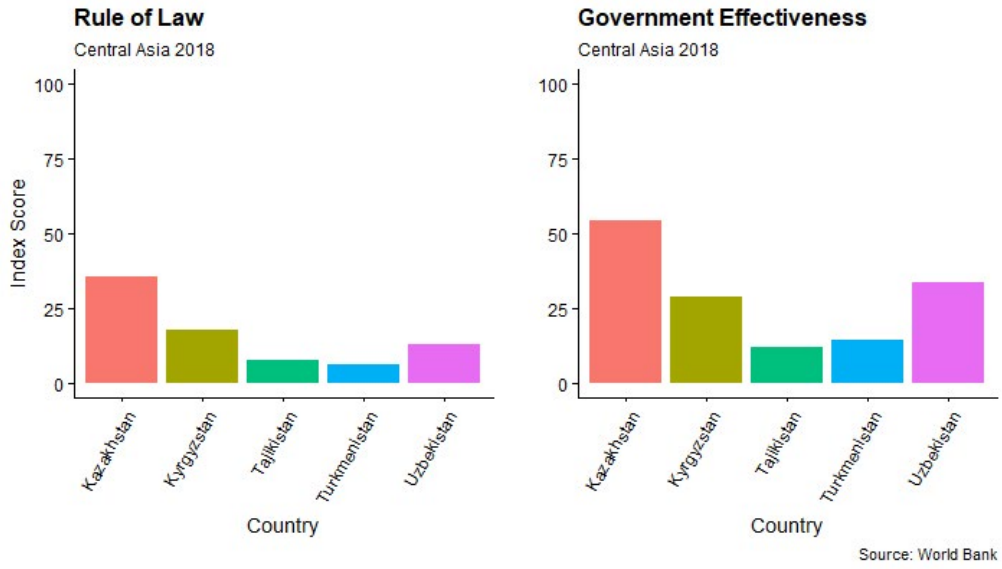
[4] "World Bank Open Data | Data," World Bank, accessed May 15, 2020, https://data.worldbank.org/.

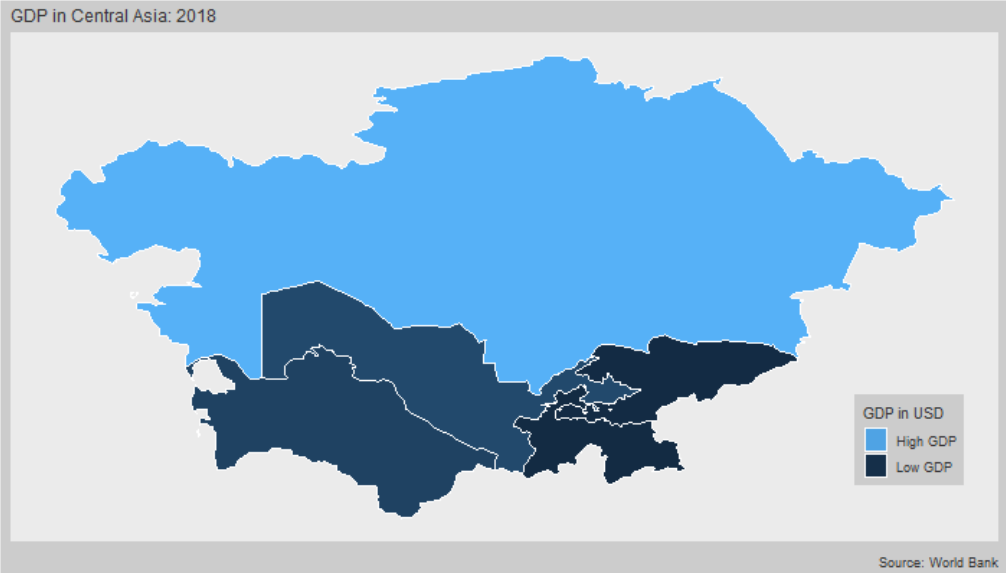
[5] "Freedom in the World," Freedom House, accessed May 15, 2020, https://freedomhouse.org/report/freedom-world.

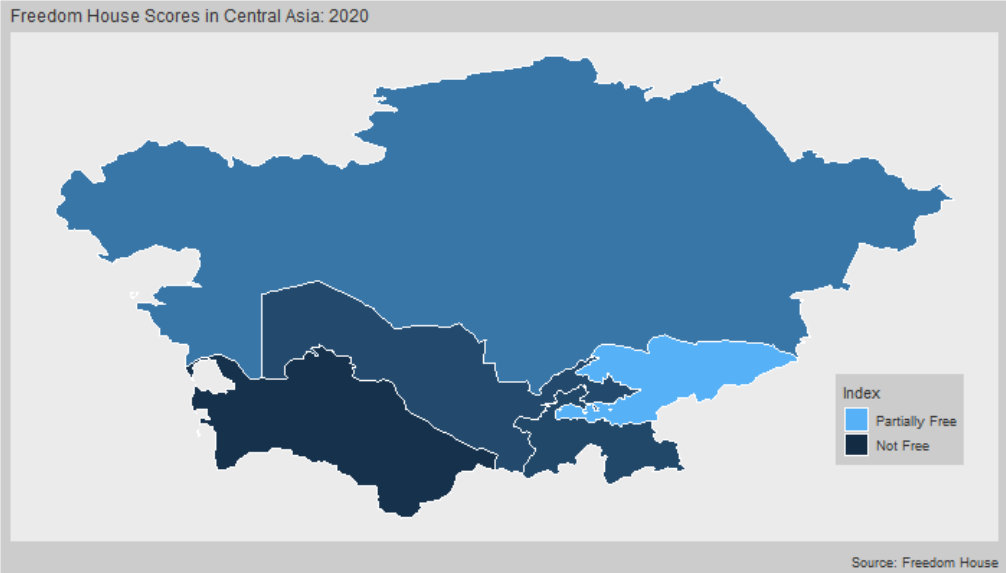
[6] "WGI 2019 Interactive > Documentation," World Bank, accessed May 15, 2020, https://info.worldbank.org/governance/wgi/Home/Documents.

Regional Overview

	Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan
Technology	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers	• Internet • Biometric Database • Safe City Projects • Facial Recognition	• Internet • Biometric Database • Safe City Projects • Facial Recognition
Foreign Companies Involved	• Huawei • HikVision • Dahua • CETC	• CEIEC • Huawei • IZP Group • Shenzhen Sunwin Intelligent • Vega (Russian)	• Huawei	• Huawei • CITIC • COSTAR • ZTE
Domestic Companies Involved	• IPAY • Sergek	• Government	• Government	• Government
Data Privacy Legislation	Yes	Yes	Yes	Yes
Known Data Privacy Scandals	Yes	Yes	No	No



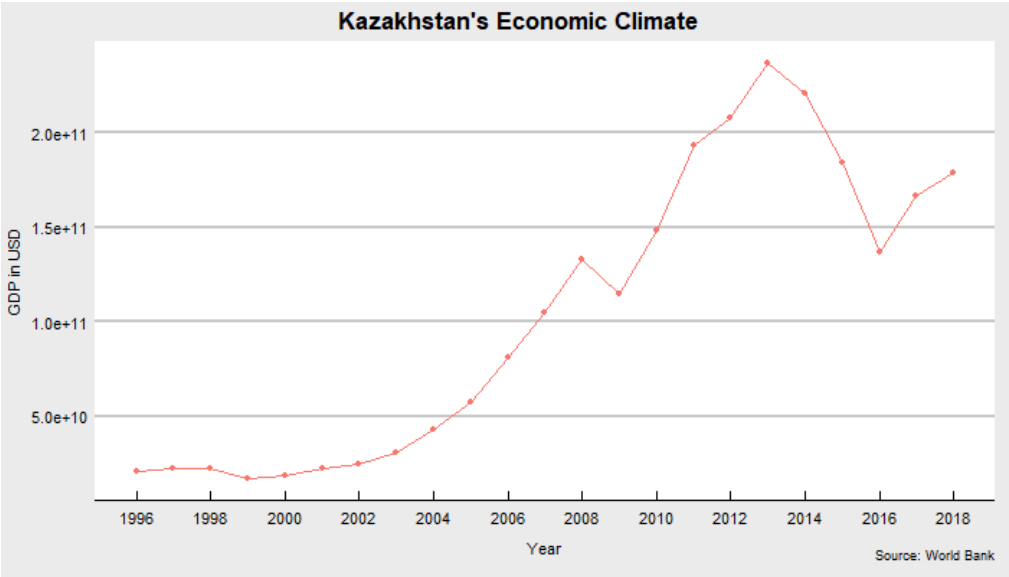

GDP in Central Asia: 2018
GDP in USD
High GDP
Low GDP
Source: World Bank

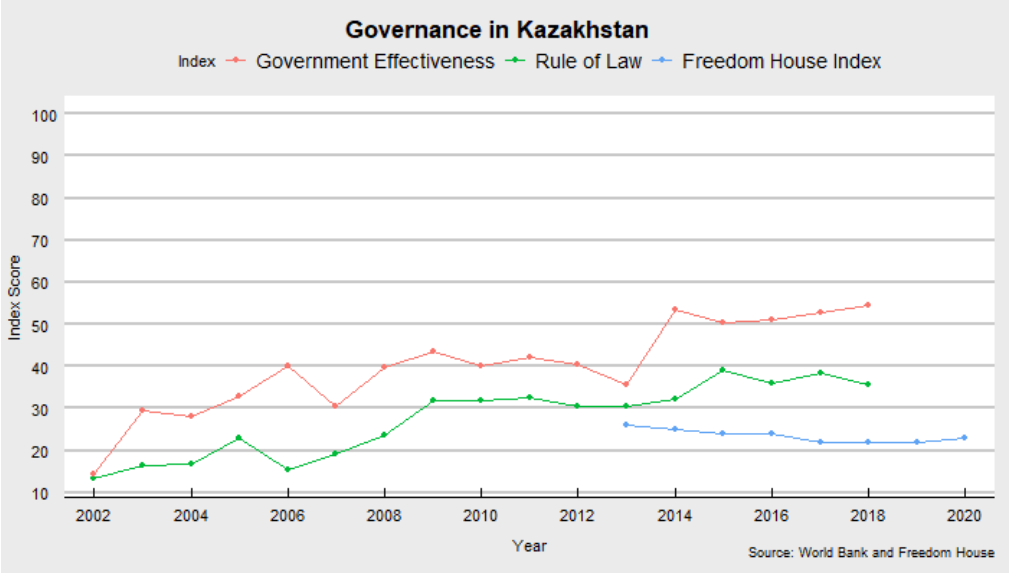

Freedom House Scores in Central Asia: 2020
Index
Partially Free
Not Free
Source: Freedom House

Country Profile: Kazakhstan

Technology	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers
Foreign Companies Involved	• Huawei • HikVision • Dahua • CETC
Domestic Companies Involved	• IPAY • Sergek
Data Privacy Legislation	Yes
Known Data Privacy Scandals	Yes

Kazakhstan consistently has the largest GDP in the region. It has also typically scored the best in terms of the World Bank's "Rule of Law" and "Government Effectiveness" governance indicators in comparison to the rest of the region. These two indicators are measured on a 0 to 100 scale. The "Rule of Law" indicator captures the perceptions of the extent agents have confidence in and abide by the rules of society, which includes the quality of contract enforcement, property rights, the police, the courts, and the likelihood of crime and violence. The "Government Effectiveness" indicator captures perceptions of the quality and relative political independence of public services and civil service. It also captures the quality of policy formulation, implementation, and the credibility of the government's commitment to such policies. In terms of regime type, Kazakhstan has consistently scored low on Freedom House's "Freedom in the World" index, which is also measured on a scale between 0 to 100 and has been determined to be "Not Free." Overall, Kazakhstan is an authoritarian state with the strongest economy and the best governance in the region, but still relatively low per global standards.





The wealthiest and most developed state within Central Asia has been aggressively improving its digital surveillance capacity for some years. It has done this largely through cooperation with Chinese ICT companies. This is unsurprising given that China has been one of the most important trade partners for Kazakhstan throughout the post-independence period. In fact, President Xi decided to officially announce the Belt and Road Initiative in Astana in September 2013. Despite this growing partnership, Kazakhstan, more so than any other regional state, has attempted to balance Chinese involvement in digital surveillance by pushing for domestic control of most systems. However, while the Kazakh government promises that Kazakh data is securely in Kazakh hands, the extent of Chinese involvement signals that complete domestic autonomy is unlikely.

The technologies in question that are essential for consideration are the Internet, a biometric database, Safe City projects that involve facial recognition technology, and finally data management centers. For the vast majority of these technologies, Chinese ICT companies are deeply involved, such as Huawei, Hik Vision, Dahua, and CETC. Local domestic companies play a dominant role however, which namely includes Sergek, but others such as IPAY have begun to integrate these technologies into their operations as well. Understanding the scope of each of these technologies and the role of relevant companies will describe the overall state of digital surveillance in Kazakhstan.

Kazakhstan's Digital Infrastructure

The Internet is more widely available in Kazakhstan than in any other Central Asian republic with around 75 percent of the population having access.[7] Although originally under state monopoly, the Kazakh government pursued market liberalization in 2004, which led to greater competition among multiple licensed operators.[8] The Internet in Kazakhstan is provided by a combination of domestic mobile Internet providers and cooperation with foreign companies, which include fiber optic landline and submarine routes to China.[9] The government has also granted itself a significant degree of access to the Internet sphere of its citizenry as shown by its creation of a system for "Automated monitoring of the national space" in 2017 for analyzing domestic digital data.[10]

Kazakhstan began to develop its biometric registry in 2009, when the government announced the creation of biometric passports that would include basic information such as a digital signature, photograph, and the like.[11] This registry was then expanded in 2016 when the Interior Ministry announced plans to create by 2021 a national fingerprint database that would include all citizens.[12] This has since expanded again in 2019 when the government began to launch pilot programs of using biometric data to deliver public services and would allow access by simply scanning fingerprints or allowing a facial scan.[13] Biometric registries are common globally, but their expansion is a requirement of developing greater surveillance capacity. The biometric database of Kazakhstan is what has allowed the Safe City projects to be implemented in the first place.

Safe City projects began to be implemented as early as 2017 in Astana (now Nur-Sultan) when an agreement between domestic IT companies and the government was signed for developing video surveillance systems with facial recognition capabilities.[14] This pilot project was under the jurisdiction of a domestic company named

---

[7] Kunagorn Kunavut, Atsuko Okuda, and Dongjung Lee, "Belt and Road Initiative (BRI): Enhancing ICT Connectivity in China–Central Asia Corridor," *Journal of Infrastructure, Policy and Development* 2, no. 1 (February 27, 2018): 116, https://doi.org/10.24294/jipd.v2i1.164.

[8] Ibid

[9] Ibid

[10] Daniiar Moldabekov, "Evraziiskii kibersoiuz: Istoriia o nesamostoiatelʹnosti Kazakhstana v oblasti kiber-bezopasnosti" [Eurasian Cyber Union: A Story of Kazakhstan's Dependence in Cyber Security], *Vlast.kz*, February 19, 2019, https://vlast.kz/obsshestvo/31791-evrazijskij-kibersouz.html.

[11] Aktan Rysaliev, "Kazakhstan Introducing Compulsory Fingerprinting Program," *Eurasianet*, November 15, 2016, https://eurasianet.org/kazakhstan-introducing-compulsory-fingerprinting-program.

[12] Ibid

[13] Inga Selezneva, "Kazakhstan Launches Pilot Programme Using Biometric Data to Deliver Public Services," *The Astana Times*, January 24, 2019, sec. Nation, https://astanatimes.com/2019/01/kazakhstan-launches-pilot-programme-using-biometric-data-to-deliver-public-services/.

[14] Ibid

"Sergek," and it was one of the most expensive public–private partnership projects in Kazakhstan.[15] Sergek has plans to install around 13,000 modern surveillance cameras in Nur-Sultan, all of which will be tied into a greater surveillance system. According to the Astana Police Department, from January to November 2018, 831,000 traffic violations were identified by Sergek.[16] This system can monitor an entire city from a single operational center.[17] Sergek has since expanded operations to Almaty and Shymkent, although Nur-Sultan remains the core of Kazakhstan's facial recognition system development. Sergek is not the only Kazakh experimentation with Safe City projects. In 2018 a different smart city pilot program was launched in the much smaller city of Akqol called "Smart Akqol" to study the effectiveness of Safe City projects in a smaller case study.[18]

The use of facial recognition technology has only expanded further as of 2020. Recently a local company called IPay in Nur-Sultan announced that it would use FRT for public transportation in the capital.[19] Further, the Kazakh government in 2020 drafted a law that introduced the concept of developing a "National Video Monitoring System" (Национальная Система Видеомониторинга), which demonstrates its eagerness to expand Sergek's work throughout the country.[20] Sergek's success in Nur-Sultan and early success in Almaty and Shymkent has proven to the Kazakh government the benefits of Safe City surveillance systems. Its system is generally easy to implement within Kazakhstan's digital infrastructure, and the technology to develop and manage these systems has largely been bought from foreign companies. An important note, however, is how the data from these systems is stored. Little is known about data storage practices outside of official legislation which promises that Kazakh data is stored domestically within Kazakhstan, but even this legislation has stipulations. Sergek, for example, has not publicized its data storage locations or practices. What is known, however, is that an unnamed Chinese company began building a large data storage center in the Baiterek district of Kazakhstan.[21] Also, another, larger data center is being built by the Chinese company CETC near Nur-Sultan.[22] This suggests that Chinese ICT companies are playing a larger role in Kazakhstan's digital surveillance apparatus than has been officially reported.

As stated earlier, much of the information surrounding Chinese ICT involvement in Kazakh domestic surveillance is not available, but a few key facts are well documented. First of all, Kazakh Internet providers Kazakhtelecom, Kcell, Beeline, and Tele2 work closely with Huawei for developing, providing, and producing Internet and/or telecommunications technology.[23] Sergek has disclosed that they heavily relied upon the Chinese

---

[15] Nikolai Enelane, "Kak Rabotaet Proekt 'Sergek'"[How the 'Sergek' Project Works], Informbiuro, 2019, https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html.

[16] Ibid

[17] Ibid

[18] ăChto Slozhnee ăSozdat «umnyi Gorod» Ili Nauchitsia v Nem Zhit?" [What is More Difficult – to Create a "Smart City" or to Learn to Live with it?], *Bluescreen*, accessed May 27, 2019, https://bluescreen.kz/digital-kazakhstan/chto-slozhnee-sozdat-umnyj-gorod-ili-nauchitsja-v-nem-zhit/.

[19] Chris Rickleton, "Kazakhstan Embraces Facial Recognition, Civil Society Recoils," *Eurasianet*, October 17, 2019, https://eurasianet.org/kazakhstan-embraces-facial-recognition-civil-society-recoils.

[20] Tatiana Trubacheva, "Bolshoi Brat: Kak Budet Rabotat Natsionalnaia Sistema Videomonitoringa v Kazakhstane" [Big Brother: How the National Video Monitoring System Will Work in Kazakhstan], *Forbes*, 2020, https://forbes.kz//process/technologies/bolshoy_brat_po-kazahski_1582187734/.

[21] Lukpan Akhmediarov, "Kitaiskaia kompaniia stroit v ZKO tsentr khraneniia informatsii" ["A Chinese Company is Building an Information Storage Center in WKO], Uralăkaia Nedelia, 2019, https://www.uralskweek.kz/2020/02/12/kitajskaya-kompaniya-stroit-v-zko-centr-xraneniya-informacii/.

[22] Nazerke Syundyukova, "Data Center to Be Built in Nur Sultan," *The Qazaq Times*, September 12, 2019, https://qazaqtimes.com/en/article/69113.

[23] 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/.

company Dahua to develop their surveillance network.[24] President Tokayev made a public trip to HikVision's headquarters in China where he praised the facial recognition software he saw and that HikVision supplies cameras to Kazakh cities including Almaty and Shymkent.[25] HikVision is an ICT company specifically sanctioned by the United States for its role in helping with the persecution of Uyghurs in western China.[26] Finally, CETC is involved with building data storage systems within Kazakh territory. What links these ICT companies have to the Chinese government is another pressing question.

Huawei is one of the largest Internet companies in the world and a leading producer of 5G technology that has repeatedly been tied directly to the Chinese government.[27] Dahua is a partially state-owned Chinese company that has become one of the largest providers of video surveillance in the world.[28] They are also the primary company involved with repressive activities against the Uyghurs and have had a back door in their hardware that was discovered to be leaking data to the Chinese government.[29] Finally, CETC (China Electronics Technology Group Corporation) is a state-owned company that produces and manages digital equipment, communications devices, software development, and asset management for civil applications and has been tasked with developing software to identify terrorists using data on jobs, hobbies, habits, and behavior.[30] The nature of these companies suggests direct Chinese government involvement in their projects. It is also documented that Chinese ICT companies have had access to the data systems they helped install elsewhere in the world. For example, it was reported in 2018 that China was routinely accessing confidential data from the IT network of the Chinese-built African Union headquarters.[31] Even more surprising is that the African Union was supposedly aware of China's access to their confidential data network but unwilling to risk relations with China and so decided to ignore the insecurity. The level of Chinese ICT company involvement in Kazakh surveillance is not clear, but it is seemingly more substantial than officially reported by the Kazakh government, and geopolitically these connections have resulted in data access channels for the Chinese government.

Kazakhstan's Regulatory Environment

Examining what legislation exists regarding personal data can demonstrate what limitations might exist for government penetration into personal privacy. In terms of legislation that addresses Internet surveillance practices, the government retains the right to monitor Internet activity in the interests of national security as detailed by a

---

[24] Nikolai Enelane, "Kak Rabotaet Proekt 'Sergek'"[How the 'Sergek' Project Works], *Informbiuro*, 2019, https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html.

[25] Asemgul Mukhitkyzy, ăRaspoznaet Dazhe v Maskakh». Nuzhny Li Kazakhstanu Kamery Hikvision?" [Recognizes Even in Masks ". Does Kazakhstan Need Hikvision Cameras?], *Radio Azattyk*, 2019, https://rus.azattyq.org/a/kazakhstan-china-survelliance-camera/30210035.html.

[26] Bradley Jardine, "China's Surveillance State Has Eyes on Central Asia," *Foreign Policy*, November 15, 2019, https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/.

[27] Murakami David Wood, "The Global Turn to Authoritarianism and After," *Surveillance & Society* 15, no. 3/4 (2017): 357–70.

[28] Nikolai Enelane, "Kak Rabotaet Proekt 'Sergek'"[How the 'Sergek' Project Works], *Informbiuro*, 2019, https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html.

[29] Zak Doffman, "Warning as Millions of Chinese-Made Cameras Can Be Hacked to Spy on Users: Report," *Forbes*, accessed March 28, 2020, https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/.

[30] Shai Oster, "China Tries Its Hand at Pre-Crime," *Bloomberg*, March 3, 2016, https://www.bloomberg.com/news/articles/2016-03-03/china-tries-its-hand-at-pre-crime.

[31] Mailyn Fidler, "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts," *Council on Foreign Relations*, March 7, 2018, https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

1995 law.[32] Also, in an act officially implemented in 2019, the Kazakh government requires all ISPs to force their users to install a root certificate into their devices. This essentially allows the government to carry out man-in-the-middle attacks on Kazakh Internet traffic.[33]

Regarding overall personal data, however, in 2013 Kazakhstan created a law on "Personal Data and Their Protection."[34] The stated purpose of the law is to protect human rights during the collection and processing of personal data. It applies to both the private and public sectors. Its regulations mandate that database operators and information collectors be transparent and get consent from individuals before collecting personal data. It did not, however, create a data protection authority. Each state agency is required to develop and supervise data protection within the industry/section of society over which it has authority.[35] It defines personal data into two categories. The first is public data, or data such as biographical directories, addresses, telephone books, public information resources, and similar resources. The second is personal data, which is not available to the public under Kazakh law, such as workplace, identity card, and personal cell phone number.[36]

This 2013 law was amended in January 2016 to require the "localization" of data. Businesses have to store personal data of Kazakh citizens within the territory of Kazakhstan. This includes servers, physical documents, data media, or even clouds. Regarding Internet sources, the related hardware and software must be physically present in the territory of Kazakhstan.[37] Finally, there are exceptions to when personal data is allowed to be distributed because the government has the right to access personal data in the interest of national security, intelligence, security measures, or counterintelligence.[38] This law states that personal information must be stored in Kazakhstan, but it does not say that duplicate versions of that data cannot be stored outside the country. This is permitted, most notably, when the data is being transferred to jurisdictions with adequate levels of data protection—"adequate," however, as defined by the government.

It is clear that legislation in Kazakhstan has been modeled on the personal data legislation of other countries, most notably the European Union's GDPR, but throughout Kazakh data protection laws the government is granted legal access for national security reasons. We also see that while there are regulations that Kazakh data should be stored domestically, it has exceptions for duplications. The key to understanding the usefulness of legislation is to recognize that legislation can signal state intention, but this does not guarantee state compliance. Kazakh legislation regarding the Internet and personal data signals a large amount of access that it has granted itself within

---

[32] "Zakon Respubliki Kazakhstan Ot 21 Dekabria 1995 Goda № 2710 «Ob Organakh Natsionalnoi Bezopasnosti Respubliki Kazakhstan» (s Izmeneniiami i Dopolneniiami Po Sostoianiiu Na 10.01.2020 g.)" "Law of the Republic of Kazakhstan dated December 21, 1995 No. 2710 "On the National Security Bodies of the Republic of Kazakhstan" (with Amendments and Additions as of 10.01.2020)], *Informatsionnaia sistema PARAGRAF,* accessed March 28, 2020, //online.zakon.kz/Document/?doc_id=1005971.

[33] Catalin Cimpanu, "Kazakhstan Government Is Now Intercepting All HTTPS Traffic," ZDNet, accessed March 28, 2020, https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/.

[34] "Zakon Respubliki Kazakhstan Ot 21 Maia 2013 Goda № 94-V «O Personalnykh Dannykh i Ikh Zashchite» (s Izmeneniiami i Dopolneniiami Po Sostoiăniiu Na 28.12.2017 g.)" [The Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V" On Personal Data and Their Protection "(with Changes and Additions as of December 28, 2017)], *Informatsionnaia sistema PARAGRAF*, accessed March 28, 2020, //online.zakon.kz/Document/?doc_id=31396226.

[35] Ibid

[36] Ibid

[37] Ibid

[38] Ibid

the digital sphere. Also, these regulations do not guarantee security if safe practices are not adopted. In 2020 a database with about 11 million people's data, almost the entire population of the country, was leaked in a massive data scandal.[39] This evinces the insecurity of Kazak personal security despite seemingly strong legislation.

Overall, the eagerness of the Kazakh government to develop its surveillance capacity is clearly visible. It has announced its large-scale plans for greatly expanding facial recognition surveillance systems nationwide. It has pursued this policy while promising both that domestic companies have full autonomy over Kazakh data and that legislation exists to protect citizens' rights to privacy. In terms of legislation, this promise is hollow considering the state's legal right to examine personal data without consent. In terms of domestic autonomy, this is even less clear. Chinese ICT involvement in this sphere suggests levels of access and cooperation between the Chinese government and domestic IT companies that are counter to the official governmental stance. That being said, however, in comparison to those of other Central Asian republics, the Kazakh government has been the most successful in balancing foreign involvement within their domestic surveillance network.

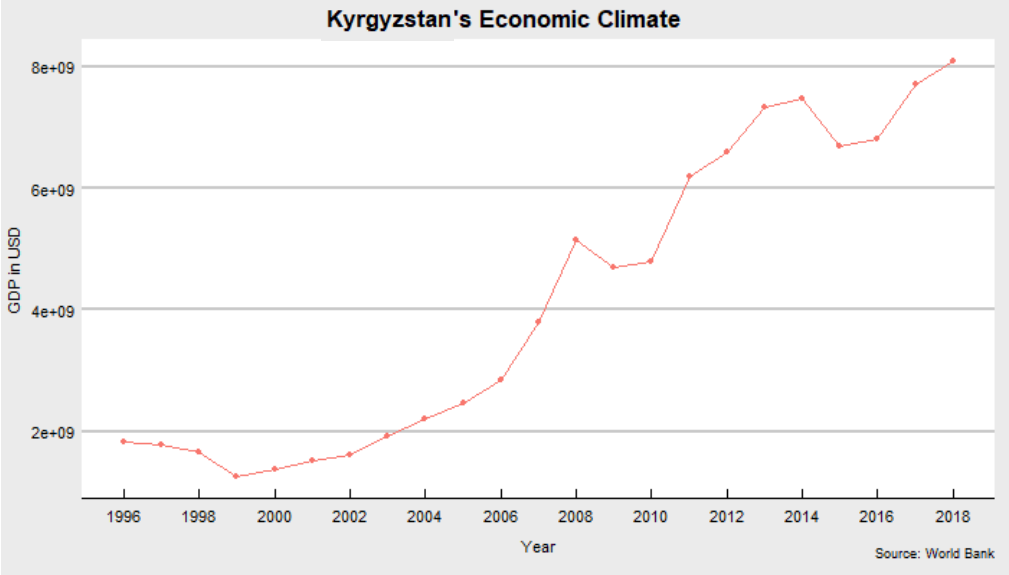
Country Profile: Kyrgyzstan

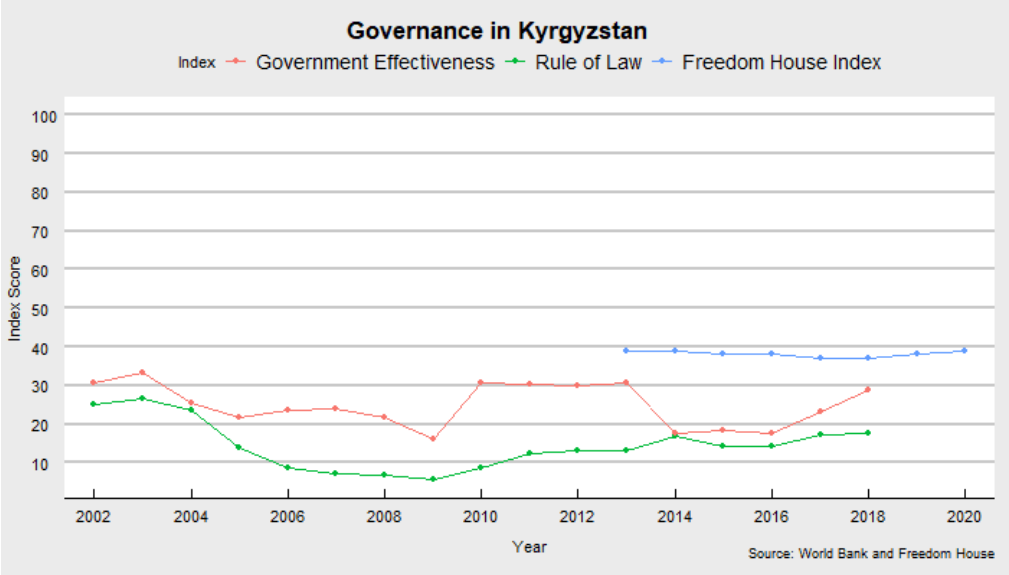
Technology	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers
Foreign Companies Involved	• CEIEC • Huawei • IZP Group • Shenzhen Sunwin Intelligent • Vega (Russian)
Domestic Companies Involved	• Government
Data Privacy Legislation	Yes
Known Data Privacy Scandals	Yes

Kyrgyzstan has the second-lowest GDP of the region, only ahead of Tajikistan in terms of economic output. It performs poorly in terms of both "Rule of Law" and "Government Effectiveness," although it does have the second highest "Rule of Law" score in the region, behind Kazakhstan. In terms of regime type, however,

[39] "Zloumyshlenniki vylozhili v set dannye millionov kazakhstantsev" [Attackers Have Posted the Data of Millions of Kazakhstanis on the Network], *Kursiv - Delovye Novosti Kazakhstana*, April 7, 2019, https://kursiv.kz/news/obschestvo/2019-07/zloumyshlenniki-vylozhili-v-set-dannye-millionov-kazakhstancev.

Kyrgyzstan has the highest score in terms of Freedom House's "Freedom in the World" index and is considered the sole democracy within the region. Freedom House, however, considers Kyrgyzstan to be only "Partially Free," which means the country is better considered to be semi-democratic or authoritarian leaning per global standards. Overall, Kyrgyzstan is the most liberal state in the region, but it still has poor governance and a very weak economic climate.





As stated before, Kyrgyzstan is Central Asia's only democratic state, although this label is often misleading as the state is better described as semi-democratic because of its fundamental issues with political rights and civil society.[40] That being said, however, Kyrgyzstan's democratic tendencies make its relationship with surveillance technology interesting for making comparisons to other semi-democratic states. Overall, Kyrgyzstan is the region's second-poorest state and was one of the first to cooperate with BRI. China is Kyrgyzstan's most

[40] "World Report 2020: Rights Trends in Kyrgyzstan," Human Rights Watch, December 10, 2019, https://www.hrw.org/world-report/2020/country-chapters/kyrgyzstan.

important economic partner, and the government has been eager to sign on to projects.[41] Kyrgyzstan has made some attempts to balance Chinese ICT involvement in its digital surveillance sphere but has generally been less successful than Kazakhstan. Local IT companies play little role in Safe City projects, and debt to China suggests long-term dependency issues. Also despite its being a democratic state, the lack of transparency and extent of digital surveillance development indicates that the Kyrgyz government is moving toward greater illiberal practices.

Kyrgyzstan's Digital Infrastructure

The technologies of interest in Kyrgyzstan are similar to those of Kazakhstan and other Central Asian states. The Internet, biometric registry, and developing Safe City projects constitute the country's digital surveillance system. Unlike in Kazakhstan, however, no domestic companies are closely involved. Instead, these systems are developed and managed entirely through government cooperation with foreign ICT companies, mostly from China. Chinese companies involved in Kyrgyzstan's digital surveillance sector include Huawei, CEIEC, and IZP Group. Interestingly, Kyrgyzstan has also worked with a Russian ICT company, Vega, which it had originally awarded a contract to over Huawei. While this might suggest a degree of balance, a Chinese ICT company was chosen to integrate Vega's work into Kyrgyzstan's overall Safe City project, rendering Vega's involvement less effective in terms of balancing China's role.

Internet is much less widely available in Kyrgyzstan than it is in Kazakhstan, with less than 35 percent of the population having access.[42] The Internet in Kyrgyzstan is provided through access to satellite backbone communication lines with links to Russia, Germany, Ukraine, and Kazakhstan, although there are also terrestrial links between China and Kyrgyzstan with more currently under construction.[43] Similar to Kazakhstan, domestic Internet providers in Kyrgyzstan are divided among multiple licensed operators, some of which are subsidiaries of foreign companies. Kyrgyzstan's Internet infrastructure overall is not considered adequately secured from either private cybercrime or state actions.[44] The government has a large degree of access to all communications networks and has a known history of wiretapping.[45] Also, as with any country that relies on Internet routed through other countries, there is a risk of foreign filtering.

Kyrgyzstan began to implement in 2014 a wide-ranged biometric database with the introduction of a biometric data registration program.[46] Legislators announced the plans to expand this system nationwide for the 2015 elections. By 2018 more than 80 percent of the population was included in the registry, which includes fingerprints, photo identification, and various biometric data, which the Kyrgyz government hopes to use for

---

[41] Roman Mogilevskii, "Kyrgyzstan and the Belt and Road Initiative" (Bishkek, Kyrgyzstan: University of Central Asia: Graduate School of Development, 2019).

[42] Kunagorn Kunavut, Atsuko Okuda, and Dongjung Lee, "Belt and Road Initiative (BRI): Enhancing ICT Connectivity in China–Central Asia Corridor," *Journal of Infrastructure*, *Policy and Development* 2, no. 1 (February 27, 2018): 116, https://doi.org/10.24294/jipd.v2i1.164.

[43] Kunagorn Kunavut, Atsuko Okuda, and Dongjung Lee, "Belt and Road Initiative (BRI): Enhancing ICT Connectivity in China–Central Asia Corridor," *Journal of Infrastructure, Policy and Development* 2, no. 1 (February 27, 2018): 116, https://doi.org/10.24294/jipd.v2i1.164.

[44] "Kyrgyzstan: State of Affairs report," *Digital Report*, April 18, 2018, https://digital.report/kyrgyzstan-state-of-affairs-report/.

[45] "Kyrgyzstan: State of Affairs report," *Digital Report*, April 18, 2018, https://digital.report/kyrgyzstan-state-of-affairs-report/.

[46] Dasha Kondrateva, "Kyrgyzstanis Skeptical about Government Biometric Data Drive · Global Voices,ăGlobal Voices, November 24, 2014, https://globalvoices.org/2014/11/24/kyrgyzstanis-skeptical-about-government-biometric-data-drive/. .

expanding its eGovernance initiatives, which will include an electronic voting platform.[47] There have been delays, however, in fully integrating the biometric registry with actual passports, and the Kyrgyz government hopes to begin granting biometric passports to citizens in 2021.[48]

While biometric passports may be lagging behind schedule, the integration of this biometric registration into functioning facial recognition Safe City projects is not. Kyrgyzstan was initially interested in developing a Safe City system in 2011 with Russian company Stilsoft, but the deal fell through for unknown reasons.[49] Then in 2018 they tried again and began a bidding war between Chinese ICT company Huawei and the Russian ICT company Vega.[50] At first the Kyrgyz government secured a $60 million contract with Huawei to create a Smart City project that would include a control center and would bring coverage to both Bishkek and Osh.[51] Negotiations with Huawei to install hardware fell through without explanation, and instead Kyrgyzstan granted a $33 million project to Vega to install traffic cameras.[52] The following year, however, the Chinese defense equipment supplier CEIEC began to install a network of facial recognition cameras and to create a police command center in Bishkek apparently free of cost.[53] While the system began functioning in 2019, there has been no information provided about where the data will be stored or who has access.[54] The second phase of the Safe City project, which includes the installation of thousands of new cameras throughout the country, began in 2019.[55] The data storage side of this equation is particularly interesting because of the lack of information provided by either the Kyrgyz government or the ICT companies involved. Another Chinese ICT company called IZP Group built and operates a data center in Kyrgyzstan, but its relationship, if any, to Bishkek's Safe City project is unknown.[56]

Much as with Kazakhstan, the amount of unknown information outweighs what is known, especially regarding data management practices. What is known, however, is that the bulk of Kyrgyzstan's surveillance network has been implemented using foreign ICT companies that partner directly with the Kyrgyz government as opposed to local companies. Huawei, much as in all Central Asian republics, plays a large role in Kyrgyz telecommunications companies, providing 90 and 70 percent of the hardware for top providers Sky Mobil and Alfa Telecom,

---

47 Aziza Umarova, "Why Kyrgyzstan Uses Biometrics in Its Voting System," *GovInsider*, June 29, 2018, sec. Connected Gov, https://govinsider.asia/connected-gov/kyrgyzstan-uses-biometrics-voting-system/.

48 Negmat Giiasov, "Grazhdane Kyrgyzstana Poluchat Biometricheskie Zagranpasporta Lish k 2021 Godu" [Citizens of Kyrgyzstan Will Receive Biometric Passports Only by 2021], *Aziia* TV, May 8, 2019, http://asiatv.kg/2019/08/05/%D0%B3%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%D0%B5-%D0%BA%D1%8B%D1%80%D0%B3%D1%8B%D0%B7%D1%81%D1%82%D0%B0%D0%BD%D0%B0-%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B0%D1%82-%D0%B1%D0%B8%D0%BE%D0%BC%D0%B5%D1%82/.

49 Temur Umarov, "China Looms Large in Central Asia," *Carnegie Moscow Center,* accessed April 2, 2020, https://carnegie.ru/commentary/81402.

50 Tsz Yau Yan, "China Taking Big Brother to Central Asia," *Eurasia.net*, accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia.

51 "V Bishkeke budet ustanovlena sistema raspoznavaniia lits v ramkakh proekta Smart City" [A Face Recognition System Will be Installed in Bishkek as Part of the Smart City project], *Karavansarai*, February 9, 2018, https://central.asia-news.com/ru/articles/cnmi_ca/newsbriefs/2018/02/09/newsbrief-02.

52 Tsz Yau Yan, "China Taking Big Brother to Central Asia," *Eurasia.net*, accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia.

53 Bermet Zhumakadyr kyzy, "Right to Privacy in Kyrgyzstan," *EUCAM*, January 21, 2020, sec. Commentaries, https://eucentralasia.eu/2020/01/right-to-privacy-in-kyrgyzstan/.

54 Daria Timofeeva, "Na ulitsakh Bishkeka poiavilis kamery raspoznavaniia lits. Kitai ustanovil ikh besplatno" [Face Recognition Cameras Appeared on the Streets of Bishkek. China Installed Them for Free], Nastoiashchee Vremia, 2019, https://www.currenttime.tv/a/30246828.html.

55 Temur Umarov, "China Looms Large in Central Asia," *Carnegie Moscow Center,* accessed April 2, 2020, https://carnegie.ru/commentary/81402.

56 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/.

respectively.[57] Vega, the Russian company, which won a contract to install traffic cameras over Huawei, specializes in military and surveillance systems.[58] The China National Electronics Import and Export Corporation (CEIEC) is a state-owned enterprise that delivers defense and security solutions to foreign markets. Shenzhen Sunwin Intelligent is another Chinese ICT company that is involved with the development of Safe City projects and other aspects of digital security, but it has historically operated only domestically in China.[59] Finally, IZP Group is a big-data company that has created a business network covering more than 104 countries. One of their main goals is to complement the Belt and Road Initiative by creating a network of international datacenters that would create a precise international supply chain system for China called the "Silk Road Station" project.[60] IZP Group has seen a drop in stock, however, after its CEO, who was once a highly ranked Chinese politician, was put under investigation for corruption and who promptly disappeared.

Similar to Kazakhstan, the nature of these companies in combination with the lack of transparency regarding the Safe City project suggests a high degree of Chinese penetration into Kyrgyzstan's domestic digital sphere. Legislation regarding personal privacy does promise a wide range of protections for citizens based on two major laws. The first is the 2014 law on biometric data, defined as the physiological and biological characteristics based upon which one can establish identity.[61] It includes clauses that mandate the collection and promise transparency and protection of the data. Data includes signatures, images of face, fingerprints, passports, birth certificates, gender, birth, place of residence, and similar details. Of specific note would be Article 6, which describes the protections for biometric data. It promises that the database is the property of Kyrgyz republic and that it is subject to legislation concerning personal information, field of informatization, and the protection of state secrets.[62] It also states that all procedures for ensuring the security of the database (i.e., collection, processing, storage, and use) are determined by the government. In Article 7, the law mandates that the gathering and use of biometric data require the consent of the individual, except under circumstances where the government needs to use said data to administer justice, handle issues of national security, combat terrorism or corruption, or in any specific cases determined by legislation of the Kyrgyz republic.[63]

Kyrgyzstan's Regulatory Environment

The other key piece of legislation is the 2008 law regarding personal data that created a state policy toward data management and collection.[64] Of particular note are Articles 25 and 27, which discuss the transfer of personal data. Article 25 states that the government cannot collect personal data without consent except when it is necessary for state bodies, local authorities, and established legislation. Personal data held by corporations can be transferred when they have an "urgent" need to protect the interests of the subject, but only after requesting permission from

---

[57] Ibid

[58] Ibid; "About," *Vega.su*, accessed April 1, 2020, http://vega.su/en/about/.

[59] "300044.SZ - Shenzhen Sunwin Intelligent Co., Ltd. Profile, " *Reuters*, accessed April 2, 2020, https://www.reuters.comundefined.

[60] Wu Yujian et al., "How Did an Ambitious Cross-Border Settlement Firm's Dream Turn Sour?," *Caixin Global*, accessed April 1, 2020, https://www.caixinglobal.com/2017-09-18/how-did-an-ambitious-cross-border-settlement-firms-dream-turn-sour-101146346.html.

[61] "Zakon KR" [Law of the Kyrgyz Republic], *Gosudarstvennaia Registratsionnaia Sluzhba*, accessed April 1, 2020, https://grs.gov.kg/ru/documents/laws/29-Zakon-KR-O-biomietrichieskoi-rieghistratsii-ghrazh/.

[62] Ibid

[63] Ibid

[64] "Zakon KR ot 14 Aprelia 2008 Goda № 58 'Ob Informatsii Personalnogo Xaraktera'" [Law of the Kyrgyz Republic of April 14, 2008 No. 58' On Personal Information], Ministerstvo Iustitsii Kyrgyzskoi Respubliki, April 1, 2020, http://cbd.minjust.gov.kg/act/view/ru-ru/202269.

state authorities. Also, regarding the cross-border transfer of data, the government provides legal protection for the process. Data will not be transferred to countries that do not provide adequate levels of protection without the consent of the subject unless it is necessary to protect the interests of the subject or if personal data is contained in a publicly accessible array. What "adequate levels of protection" means, however, is undefined.[65] Article 27 discusses the storage of personal data but simply says that it should not be stored longer than necessary. There is no mention of how the data should be stored or what protections it should be granted.

Kyrgyzstan's legislation regarding personal data seems robust, but the level of access granted to the government is large. Similarly, little legislation exists that promises citizens' data is not managed, accessed, or otherwise held by foreign companies. This is of course assuming the government adheres to its own legislation, but two data-related scandals occurred that suggest otherwise. In 2019 it became apparent that the government had been selling citizens' data to financial organizations, telecommunications companies, and banks since 2017.[66] Another notable scandal took place in 2017, when it was uncovered that then–Presidential candidate Jeenbekov used citizens' private data to win the 2017 election. Hackers found that a little-known real estate website called "Samara" was hosting the personal data including PINs, passport numbers, and phone numbers of 2 million citizens from the server of the State Registration Service.[67]

Overall, Kyrgyzstan has been less successful than Kazakhstan in balancing foreign involvement in its digital surveillance network but has been pursuing its development just as quickly. Given it is the most democratic state in the region, one would expect greater measures for transparency regarding this system. Kyrgyzstan, however, has weaker legislation regarding personal privacy, has well-documented data-abuse scandals, has released less information regarding the degree of penetration enjoyed by Chinese ICT companies, and, in general, has become far more reliant on China for financial and technological support. Considering these dependency issues, the nature of the ICT companies involved with developing Kyrgyzstan's surveillance systems, and the overall unwillingness of the Kyrgyz government to either adhere to personal data legislation or reveal details regarding surveillance practices, it is likely that the Kyrgyz government is actively improving its suppressive capabilities at the cost of sharing domestic data with the Chinese government.

---

[65] Ibid

[66] Tatyana Kudryavtseva, "Passport Data of Kyrgyzstanis to Be Sold to Banks, Cellular Companies," *24.Kg,* November 6, 2019, sec. English, https://24.kg/english/134288__Passport_data_of_Kyrgyzstanis_to_be_sold_to_banks_cellular_companies/.

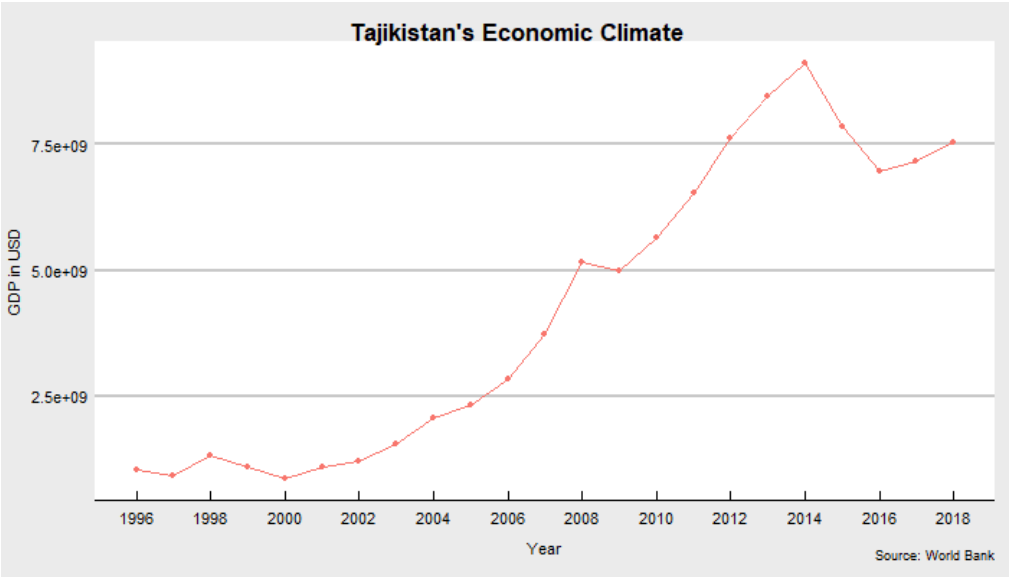
[67] Rinat Tukhvatshin, "Samarageti, epizod 1. Kak server pravitelstva Kyrgyzstana ispolzovali dlia popytki vliianiiă na prezidentskie vybory" [Samaragate, Episode 1. The Government of Kyrgyzstan was used as a Server to try to Influence the Presidential Elections], *KLOOP.KG - Novosti Kyrgyzstana*, October 26, 2017, https://kloop.kg/blog/2017/10/26/samara_elections_kg/.

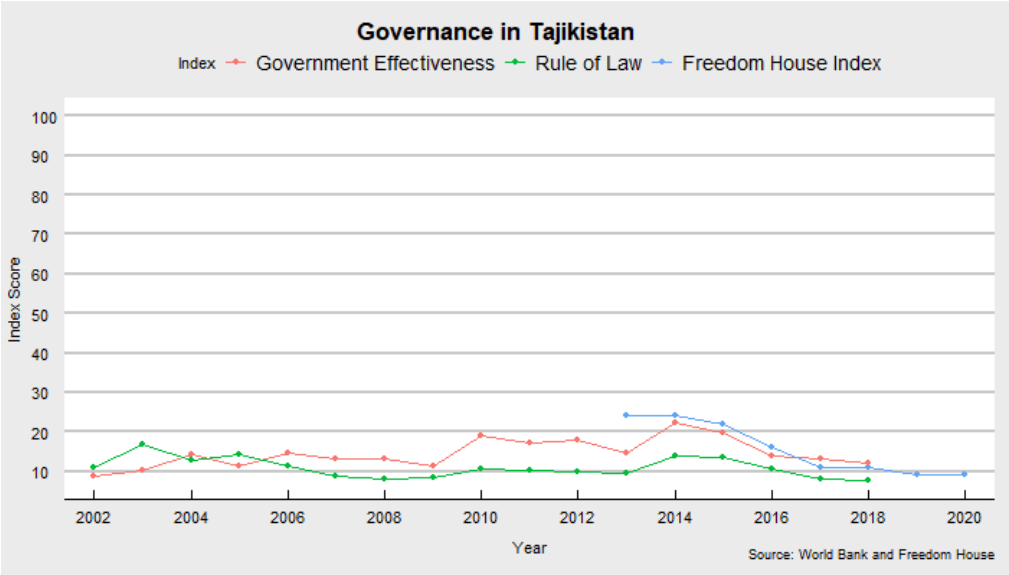
Country Profile: Tajikistan

Technology	• Internet • Biometric Database • Safe City Projects • Facial Recognition
Foreign Companies Involved	• Huawei
Domestic Companies Involved	• Government
Data Privacy Legislation	Yes
Known Data Privacy Scandals	No

Tajikistan is the poorest state in Central Asia and has one of the region's worst track records for human rights, political freedoms, and civil society.[68] Tajikistan has the lowest GDP in the entire region. Tajikistan's governance record is also worse than its neighbors', as it has also regularly scored the worst on both the "Rule of Law" and "Government Effectiveness" indexes. Finally, in terms of regime type, Tajikistan has one of the lowest ratings on Freedom House's "Freedom in the World" index and is considered "Not Free." Tajikistan's is an autocratic government with a poor governance record and weak economic environment in comparison to both the region and global standards. In recent years, Tajikistan's governance and autocratic tendencies have continued to deteriorate, which is unique in the region.

[68] "World Report 2020: Rights Trends in Tajikistan," *Human Rights Watch,* December 10, 2019, https://www.hrw.org/world-report/2020/country-chapters/tajikistan.





Tajikistan has been one of the major BRI target developmental projects, to which the Tajik government has been largely receptive. Tajikistan has paid for BRI projects through loans or by directly signing away land or mining rights.[69] This has resulted in large-scale dependencies issues for the country, and the sphere of digital surveillance is no exception to these problems. While only one foreign company, Huawei, is at play in Tajikistan, it has a near-monopoly on both the domestic Internet environment and the nascent sphere of digital surveillance. Regardless of the legislation that promises personal data protections, Tajikistan's record on human rights issues and the state's history of targeting political dissent suggest that its motivation for developing digital surveillance is first and foremost to improve the regime's authority over a country that saw a civil war only a few decades ago.

[69] Sam Reynolds, "For Tajikistan, the Belt and Road Is Paved with Good Intentions," *The National Interest* (The Center for the National Interest, August 23, 2018), https://nationalinterest.org/feature/tajikistan-belt-and-road-paved-good-intentions-29607.

Tajikistan's Digital Infrastructure

The domestic fixed communications market of Tajikistan is reasonably competitive with a variety of local companies that provide Internet service.[70] Of those companies, however, only the state-owned Tajiktelecom is operational throughout the entire country. Mobile communications is the faster-growing market and enjoys a relatively open and competitive market with domestic and foreign companies at play.[71] In terms of international Internet connectivity, Tajikistan is reliant on cable connections through Kyrgyzstan, Uzbekistan, and China, which raises network travel security issues.[72] Finally, more than 90 percent of Tajikistan's telecommunications hardware is supplied directly by Huawei, which also owns TK mobile, one of the largest telecommunications providers in the country.[73] Internet surveillance is very common in Tajikistan, where Internet access is routinely blocked or canceled depending on domestic circumstances.[74] Since 2001, the Tajik government has mandated that all companies install a system of operational search measures in their equipment to allow full government access to data.[75] Tajikistan's Internet market is therefore generally competitive but dominated by Huawei hardware and completely under the control of the Tajik government.

Tajikistan began creating a biometric data registry in 2010 when it announced that it would begin creating and issuing biometric passports that would contain citizens' digital photographs and fingerprints.[76] The Tajik government decided to expand this data system by mass fingerprinting citizens in 2016.[77] According to government sources in 2019, this effort was largely successful, and as of 2020 around 2.5 million citizens had biometric passports.[78] Although the government will continue issuing biometric passports to its citizens, the vast majority have had their biometric data included in the overall biometric registry.

The implementation of Tajikistan's Safe City project is more straightforward than those of other Central Asian republics' and also began somewhat earlier. Dushanbe's Safe City initiative began in 2013 after spending $22 million dollars for a Huawei contract.[79] Huawei installed hundreds of CCTV and traffic cameras around Dushanbe, but these cameras lacked the facial recognition systems that are more common with current Chinese

---

[70] "Obzor Telekom Rynka Tadzhikistana: Fiksirovannaia, Mobilnaia i Mezhdunarodnaia Sviaz" [Tajikistan Telecom Market Review: Fixed, Mobile and International Communications], *Digital Report,* June 5, 2017, https://digital.report/tadzhikistan-svyaz/.

[71] Ibid

[72] Ibid

[73] Abdullo Ashurov, "Smartfony Huawei v Tadzhikistane populiarny. A bezopasny li?" [Huawei Smartphones are Popular in Tajikistan. Are they Safe?], *Radio Ozodi*, 2019, https://rus.ozodi.org/a/29692588.html.

[74] "Obzor Telekom Rynka Tadzhikistana: Fiksirovannaia, Mobilnaia i Mezhdunarodnaia Sviaz" [Tajikistan Telecom Market Review: Fixed, Mobile and International Communications], *Digital Report*, June 5, 2017, https://digital.report/tadzhikistan-svyaz/.

[75] Ibid

[76] Galim Faskhumdinov, "Tadzhikistan podgotovil biometricheskie pasporta v Germanii," [Tajikistan Prepared Biometric Passports in Germany], *DW*, 02 2010, https://www.dw.com/ru/%D1%82%D0%B0%D0%B4%D0%B6%D0%B8%D0%BA%D0%B8%D1%81%D1%82%D0%B0%D0%BD-%D0%BF%D0%BE%D0%B4%D0%B3%D0%BE%D1%82%D0%BE%D0%B2%D0%B8%D0%BB-%D0%B1%D0%B8%D-0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5-%D0%BF%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%B0-%D0%B2-%D0%B3%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D0%B8/a-5198915.

[77] "V Tadzhikistane Prokhodit Massovaia Daktiloskopiia" [Mass fingerprinting is underway in Tajikistan]," *Molbulak.ru*, November 29, 2016, https://www.molbulak.ru/news/tadzhikistan/v-tadzhikistane-prokhodit-massovaya-daktiloskopiya/.

[78] Avaz Iuldashev, "Skolko Grazhdan Tadzhikistana Imeiut Biometricheskie Pasporta?" [How Many Tajik Citizens Have Biometric Passports?], *Novosti Tadzhikistana ASIA-Plus*, 2019, https://www.asiaplustj.info/ru/news/tajikistan/society/20190802/v-mid-soobtshili-skolko-grazhdan-tadzhikistana-imeyut-biometricheskie-pasporta.

[79] 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/.

Safe City projects. This system reportedly created more than $14 million in traffic fines in the fall of 2019 alone, which speaks to its overall effectiveness as a police tool.[80] This prompted the Tajik government to upgrade the original system in 2019 when it announced that new Huawei cameras, now equipped with facial recognition systems, would be installed not only throughout Dushanbe, the airport, shopping centers, parks, and markets, but also in every major city of Tajikistan.[81] The contract for this large-scale expansion of the Safe City network was granted entirely to Huawei with no domestic company involved whatsoever.

Interestingly, unlike in Kyrgyzstan and Kazakhstan, there have been no reports either directly by the government or indirectly by journalistic reports of data management centers. This suggests that either local journalists and experts have failed to recognize the construction of data management centers or that the data management of Tajikistan's Safe City project is being handled outside the country itself. Considering Huawei's size as a company and its relationship to the Chinese government, this might mean that most of the data storage is handled in Huawei servers, which could be located in any large Huawei data center. Similarly, considering that the Tajik government has already made a precedent of ceding over land, mineral rights, and domestic factories to Chinese companies in return for services, it does not seem impossible that domestic data is handled remotely by Huawei in a similar manner. In fact, this practice would be consistent with Chinese company activities in Tajikistan to this point as many Chinese projects in the country are managed, worked, and completed with Chinese labor and equipment.[82]

Tajikistan's Regulatory Environment

This practice would not be considered illegal per Tajik personal data privacy legislation. The most recent and comprehensive piece of privacy legislation is the 2018 law on the protection of personal data, which defines the legal basis for the collection, storage, and processing of personal data. This unifies and replaces the previous "scattered" pieces of legislations dealing with various aspects of data protection. The new law contains provisions on consent requirements, biometric data, and subject access requests.[83] This law also defines what constitutes data collection and processing personal data. Data collection is any action aimed at receiving personal data. Processing personal data is considered the recording, systematization, storage, amendment, replenishment, extraction, usage, spread, impersonation, blocking, or destruction of data that is taken from individuals.[84] The law states that the collection and processing of personal data are allowed when the subject gives consent, when the data processing is in compliance with the lawful aims of the data controller, when the processed information is accurate, when the subject has access to the data, and when the data collector has certified all equipment and facilities with the regulator.

---

[80] Tsz Yau Yan, "China Taking Big Brother to Central Asia," *Eurasia.net,* accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia.

[81] "V Tadzhikistane Prokhodit Massovaia Daktiloskopiia" [Mass fingerprinting is underway in Tajikistan]," *Molbulak.ru*, November 29, 2016, https://www.molbulak.ru/news/tadzhikistan/v-tadzhikistane-prokhodit-massovaya-daktiloskopiya/.

[82] Sam Reynolds, "For Tajikistan, the Belt and Road Is Paved with Good Intentions," *The National Interest* (The Center for the National Interest, August 23, 2018), https://nationalinterest.org/feature/tajikistan-belt-and-road-paved-good-intentions-29607.

[83] "Zakony Respubliki Tadzhikistan" [Laws of the Republic of Tajikistan], *Narodnaia Gazeta*, accessed April 1, 2020, http://www.narodnaya.tj/index.php?option=com_content&view=article&id=7232:2018-08-08-07-09-50&catid=69:zakoni&Itemid=171.

[84] Ibid

Article 11 stipulates, however, that access to personal data without receiving consent is allowed if it is necessary for governmental authorities to carry out their functions or when in the interests of protecting the rights and freedom of citizens.[85] Cross-border transfers are allowed if the government determines that the foreign body has sufficient protection for personal data, subject consent is obtained, and the transfer is necessary for the protection of citizens' rights, freedom, health, morality, or public order.

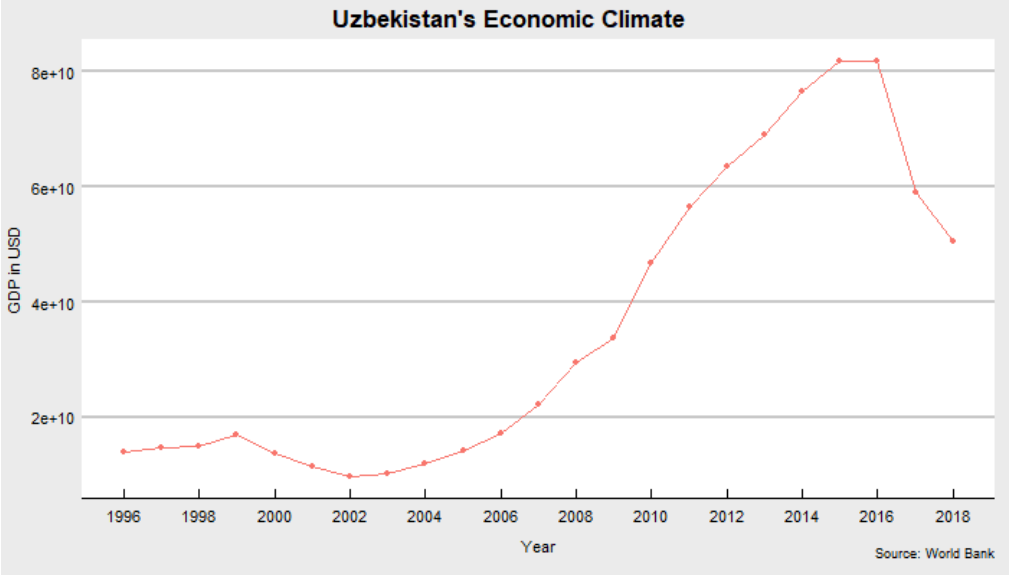
This legislation, like others in the region, is modeled on Europe's GDPR, but with even broader stipulations for when data can be collected or used without citizen consent. Considering the overall reputation and precedent that the Tajik government has for adhering to its own legislation and its track record on suppression regarding political dissent, this law signals only the awareness of the regime regarding global personal privacy norms. It does not demonstrate an adherence to its principles. Generally speaking, Tajikistan's is one of the clearest cases in Central Asia of an authoritarian regime that is actively seeking to improve its suppressive capacity regardless of foreign dependency. China, via Huawei, enjoys a near-monopoly both within Tajikistan's telecommunications hardware market and also its newly developing digital surveillance apparatus. Considering the land, mineral rights, and general operational autonomy that has already been granted to Chinese Belt and Road companies, it is likely that Tajik personal data is processed and stored in a variety of Huawei facilities that may or may not be located within the country itself. In this sense, Tajikistan is a direct case of an authoritarian regime trading domestic autonomy to a more powerful, foreign neighbor in exchange for improving its position over its own citizenry.

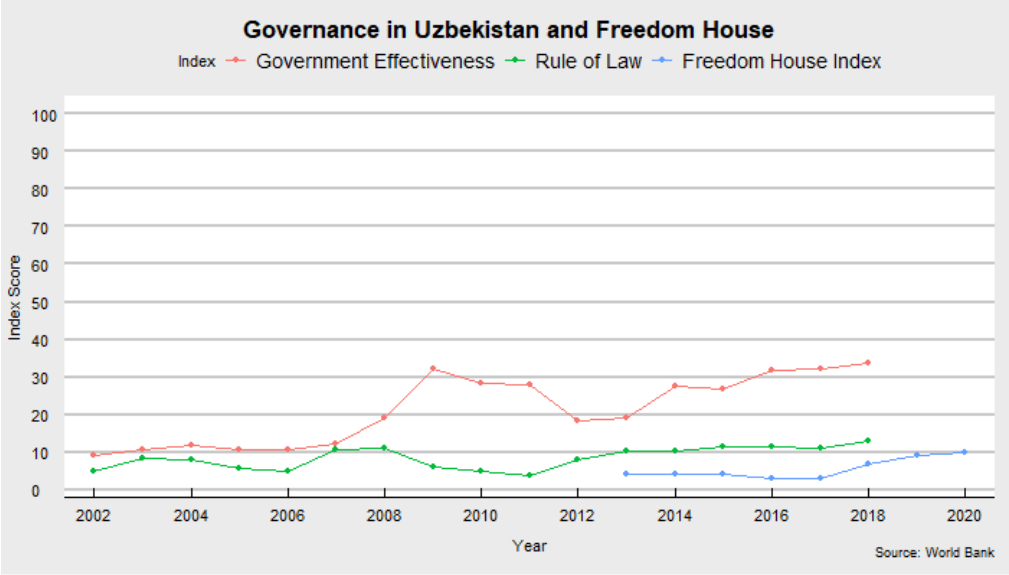
Country Profile: Uzbekistan

Technology	• Internet • Biometric Database • Safe City Projects • Facial Recognition
Foreign Companies Involved	• Huawei • CITIC • COSTAR • ZTE
Domestic Companies Involved	• Government
Data Privacy Legislation	Yes
Known Data Privacy Scandals	No

[85] Ibid

Uzbekistan has the largest population in the region and the second-largest economy, behind only Kazakhstan. In terms of governance, Uzbekistan has a poor record in comparison to global standards for both "Rule of Law" and "Government Effectiveness." That being said, Uzbekistan actually has the second-best "Government Effectiveness" score in the region, again behind only Kazakhstan. Finally, in regard to regime type, Uzbekistan has one of the lowest scores on the "Freedom in the World" index and is considered "Not Free." It is an authoritarian state with an overall poor governance record, but a stronger economic climate than most of its neighbors'. Uzbekistan's governance and "Freedom in the World" score, however, have both been improving since the death of the country's first President, Islam Karimov.





Similar to the other Central Asian states, Uzbekistan is an active partner of China's BRI and the Digital Silk Road. This includes cooperation with Chinese ICT firms to develop its overall digital sphere and to create and operate a large-scale surveillance network through Safe City projects. Uzbekistan has involved multiple foreign

ICT companies in this goal but has chosen not to involve domestic companies in the management. The foreign companies involved with Uzbekistan's developing surveillance network are Huawei, CITIC, COSTAR, and HikVision. They all partner directly with the Uzbek government.

Uzbekistan's Digital Infrastructure

Around 46 percent of Uzbekistan's population has access to the Internet of some variety.[86] Much of the telecommunications market is controlled by the state through the state-owned company Uztelecom. Uzbekistan has several landline routes through Kazakhstan, Kyrgyzstan, Tajikistan, and Afghanistan – it has been largely successful in diversifying its Internet access points.[87] Huawei is the most influential foreign telecommunications company in Uzbekistan. In 2008, Huawei modernized the Uzbek national telecommunications network for $21 million, and in 2011 Uzbekistan signed a $18 million technology purchasing deal using loans from the China Development Bank.[88] Huawei has already begun incorporating 5G technology into both Uzmobile and Ucel systems, which demonstrates the degree of access Huawei has in Uzbekistan's telecommunications sphere.

Surveillance and restrictions on Internet usage in Uzbekistan are still extensive. The government "Center for the Monitoring of the Mass Communications Sphere" is tasked with identifying online publications that are deemed a negative influence on society. In 2020 Uzbekistan announced that it will force the companies Facebook, Google, and Yandex to store the personal data of Uzbek users within Uzbek territory, which has been criticized as an attempt to impose greater control.[89] Overall, Uzbekistan enjoys extensive access to the Internet and domestic mobile communications. The state also periodically controls Internet access to suppress narratives it deems anti-government. While Skype, WhatsApp, and Viber's becoming available in 2018 suggests some liberal developments for Uzbekistan's Internet environment, the degree of surveillance and control practiced by the regime still classifies it as illiberal in nature.[90]

Uzbekistan created a comprehensive biometric registry in 2011 when it began transitioning to biometric passports that included biographical information, fingerprints, and photographs.[91] The government continued to promote the biometric passport and by 2017 around 80 percent of the population had one.[92] Recently the government

---

[86] "Refworld | Freedom on the Net 2018 - Uzbekistan," Refworld, accessed November 1, 2018, https://www.refworld.org/docid/5be16aed4.html.

[87] Kunagorn Kunavut, Atsuko Okuda, and Dongjung Lee, "Belt and Road Initiative (BRI): Enhancing ICT Connectivity in China-Central Asia Corridor," *Journal of Infrastructure, Policy and Development* 2, no. 1 (February 27, 2018): 116, https://doi.org/10.24294/jipd.v2i1.164.

[88] 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/.

[89] "Tashkent Forcing Internet Firms To Locate Uzbek User Data Within Uzbekistan," Radio Free Europe/Radio Liberty, February 21, 2020, https://www.rferl.org/a/internet-firms-user-data-within-uzbekistan/30447111.html.

[90] "Refworld | Freedom on the Net 2020, accessed March 5 2021, https://freedomhouse.org/countries/freedom-net/scores.

[91] "V Uzbekistane Vvedut Biometricheskie Zagranpasporta s 1 Ianvaria 2019 Goda" [Biometric Passports to Be Introduced in Uzbekistan from January 1, 2019], *Digital Report,* August 18, 2017, https://digital.report/v-uzbekistane-vvedut-biometricheskie-zagranpasporta-s-1-yanvarya-2019-goda/.

[92] "80% naseleniia Uzbekistana obespecheno biometricheskimi pasportami" [80% of the Population of Uzbekistan has been Provided Biometric Passports], *Digital Report*, April 12, 2017, https://digital.report/80-naseleniya-uzbekistana-obespecheno-biometricheskimi-pasportami/.

announced that only those with the biometric passport would be able to travel abroad and that ID cards would be acceptable only within the territory of Uzbekistan.[93] This system, similar to the other biometric registries in the region, provides the backbone for the nascent Safe City project to be implemented.

While traffic cameras began appearing in Tashkent in 2015, Uzbekistan's Safe City project officially began in 2018 and has so far been limited to just the capital of Tashkent.[94] Tashkent's project began with a surveillance system installed by Huawei and began operating in 2019. It has since expanded to include investments from CITIC and COSTAR, although the hardware for the system itself is still provided by Huawei.[95] CITIC and COSTAR became involved with the Safe City project after President Mirziyoyev signed a $1 billion agreement in Beijing.[96] The Uzbek government wants to further expand this system by including smart transport, smart education, smart healthcare, smart ride, smart water/sewage, and smart house capabilities.[97] Generally speaking, the Uzbek government wants to integrate artificial intelligence, digitization, and central control into most of the country's physical infrastructure and governance apparatuses. In 2019, for example, Huawei and another Chinese ICT company, ZTE, agreed to introduce surveillance technology to the Uzbek education system to monitor student attendance and teacher performance.[98] Uzbekistan's plans for expanding its Safe City Project into a countrywide Smart City system is the most ambitious of the region, and the government has already moved toward actualizing these goals. Much as with Tajikistan and Kyrgyzstan, however, information regarding management practices and data storage has not been released.

Examining the profiles of the companies involved, alongside existing legislation, may indicate insecurities and personal privacy concerns that the relevant parties have not discussed. Huawei's connections to the Chinese government are well documented, and it is a company active in every Central Asian state. China International Trust Investment Corporation (CITIC) is not an ICT company but instead a state-owned investment corporation with the goal to introduce advanced technologies.[99] COSTAR Group is another Chinese company that researches, manufactures, and markets optical elements, which includes monitoring systems.[100] Finally, ZTE is a leading Chinese ICT company that has been criticized for its close relationship to the Chinese government.[101] These

---

[93] "S 2021 Goda v Uzbekistane Vmesto Biometricheskogo Pasporta Budut Vydavatsia ID-Karty" [From 2021 in Uzbekistan ID-Cards will be Issued instead of a Biometric Passport], *Review.uz*, accessed March 9, 2020, https://review.uz/ru/post/s-2021-goda-v-uzbekistane-vmesto-biometricheskogo-pasporta-budut-vdavatsya-id-kart.

[94] Maksim Yeniseyev, "Tashkent 'Safe City' Project to Unify Security Information Systems," *Caravanserai*, September 20, 2017, https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2017/09/20/feature-01.

[95] 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/; Tsz Yau Yan, "China Taking Big Brother to Central Asia," Eurasia.net, accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia; Zhadmoliddin Turdimov, "Uzbekistan privlechet svyshe $1 milliarda kitaăkikh investitsii v razvitie tsifrovoi infrastruktury" [Uzbekistan will Attract over $1 Billion of Chinese investments in the Development of Digital Infrastructure], Kursiv - Delovye Novosti Kazakhstana, April 2019, https://kursiv.kz/news/ekonomika/2019-04/uzbekistan-privlechet-svyshe-1-milliarda-kitayskikh-investiciy-v-razvitie.

[96] Umida Hashimova, "China Dominates Digital Infrastructure in Uzbekistan," *The Diplomat,* June 28, 2019, https://thediplomat.com/2019/06/china-dominates-digital-infrastructure-in-uzbekistan/.

[97] "Uzbekistan to Develop Smart Cities," *Dentons.com*, January 28, 2019, https://www.dentons.com/en/insights/alerts/2019/january/28/uzbekistan-to-develop-smart-cities.

[98] Bradley Jardine, "China's Surveillance State Has Eyes on Central Asia," *Foreign Policy*, November 15, 2019, https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/.

[99] "CITIC Limited," CITIC.com, accessed April 2, 2020, https://www.citic.com/en/.

[100] "Costar Group Co Ltd - Company Profile and News," *Bloomberg.com*, accessed April 2, 2020, https://www.bloomberg.com/profile/company/002189:CH.

[101] Kevin Kelleher, "Trump, China and ZTE: An Explainer," *Fortune*, June 13, 2018, https://fortune.com/2018/06/13/zte-trump-china-heres-fuss-all-about/.

companies all have close ties to the Chinese government, which suggests yet again that Beijing has a degree of access to Uzbek personal data. The Uzbek government, however, has only recently passed legislation that creates any formal protections for Uzbek data.

Uzbekistan's Regulatory Environment

Uzbekistan's Law on Personal Data was adopted in 2019.[102] It defines special personal data as information on racial/social origin; political, religious, or ideological beliefs; political membership; and other factors. It defines biometric data as the anatomical or physiological characteristics of subjects and also defines genetic personal data as information related to inherited or acquired characteristics as pertaining to a biological sample. According to the law, the processing of personal data includes collection, systematization, storage, modification, addition, use, provision, dissemination, transfer, depersonalization, and destruction.[103] Processing is allowed under the following scenarios: upon consent, when the use is necessary to fulfill an agreement that includes the subject, when required to fulfill obligations of the owner and/or operator, when needed to protect the interests of the subject or others, when it is required to exercise the rights and legitimate interests of the owner and/or operator in order to achieve socially significant goals (provided the rights of the subject are not violated), when it's needed for research, or when it is taken from public sources.[104]

Personal data can be given to third parties when consent is given, when there is an agreement between the subject and the owner, and in cases as stipulated by law. Finally, and most interestingly, cross-border transfer of personal data is allowed when the foreign entity is considered to have "adequate" protection, but what constitutes adequate protection is not defined. Cross-border transfers of data are also allowed to non-"adequate" countries when the subject agrees, when it is stipulated by the international treaty of Uzbekistan, and when there is a "need" to protect the constitutional order of Uzbekistan, public order, rights/freedoms of citizens, and health or morality of the population. In general, much as in other Central Asian states, formal legislation modeled on GDPR exists, but the degree of access given to the regime is high. Also, similar to Tajikistan, general state Internet surveillance practices suggest that much of this legislation will not be adhered to by governing bodies.

Uzbekistan is similar to Tajikistan and Kyrgyzstan, therefore, in how it has approaches the development of its digital surveillance network. It has decided to rely entirely on Chinese ICT companies and has created public–private partnerships between the regime and these companies only to implement and manage Safe City projects. It has also not attempted to integrate domestic IT companies as Kazakhstan has done. More than any other state, however, the Uzbek government has the most ambitious plans for developing its surveillance system, hidden under official rhetoric for developing a nationwide smart governance system. Despite legislation, Uzbekistan's record on surveillance and personal data abuse suggests that Uzbekistan will use enhanced surveillance technologies to continue its repressive style of government, only more effectively. Much as with Tajikistan and Kyrgyzstan, there is little doubt that the Uzbek personal data is in the possession of the Chinese government, which further demonstrates that Central Asian governments are less concerned with full autonomy than they are with improving domestic suppressive capacity.

---

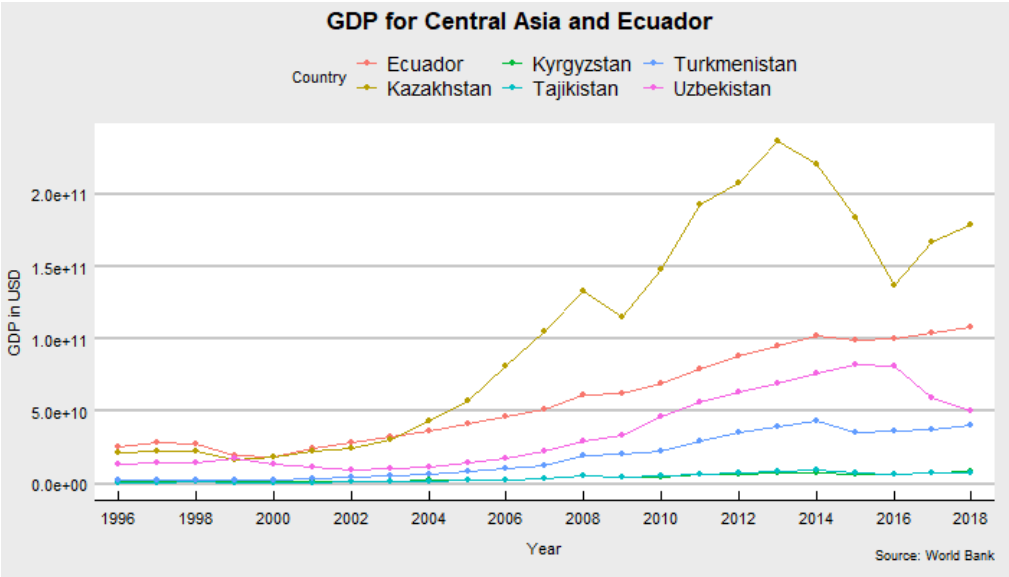
[102] "ZRU-547-Son 02.07.2019. O Personalnykh Dannykh" [ZRU-547-Son 02.07.2019. About Personal Data], *Lex.uz*, accessed April 2, 2020, https://lex.uz/docs/4396428.

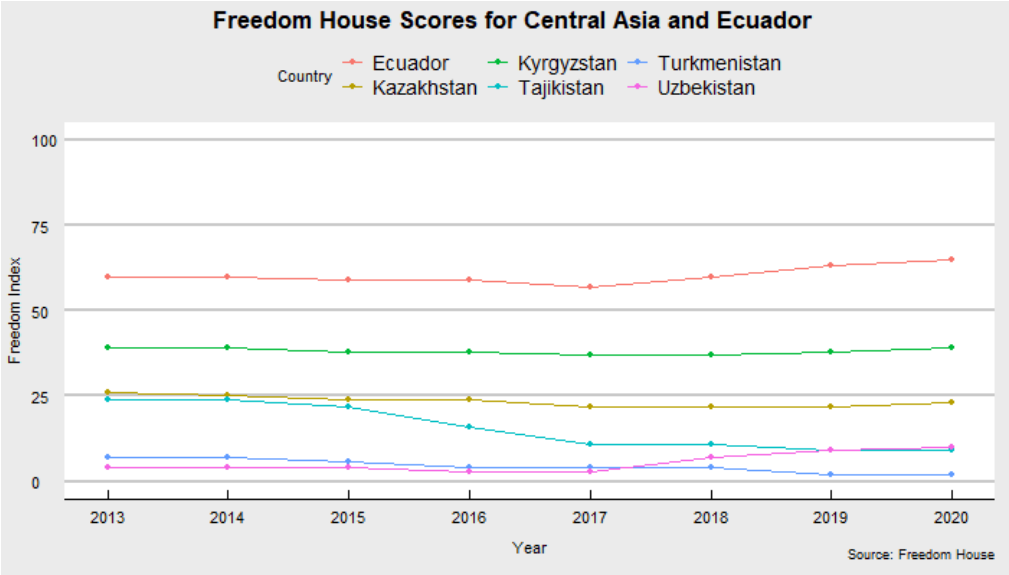
[103] Ibid

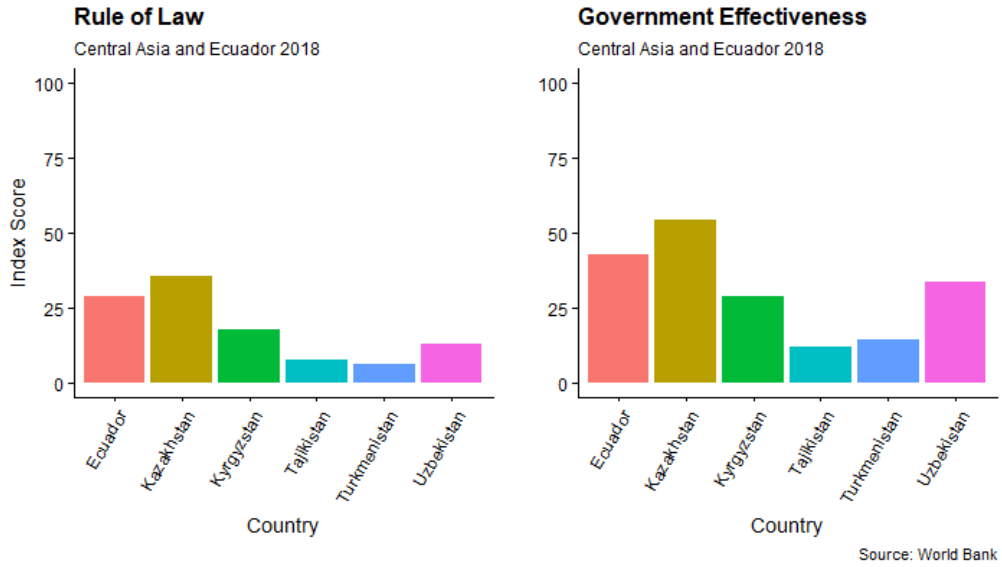
[104] Ibid

Comparative Overview: Ecuador

	Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan	Ecuador
Technology	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers	• Internet • Biometric Database • Safe City Projects • Facial Recognition	• Internet • Biometric Database • Safe City Projects • Facial Recognition	• Internet • Biometric Database • Safe City Projects • Facial Recognition
Foreign Companies Involved	• Huawei • HikVision • Dahua • CETC	• CEIEC • Huawei • IZP Group • Shenzhen Sunwin Intelligent • Vega (Russian)	• Huawei	• Huawei • CITIC • COSTAR • ZTE	• Huawei • CEIEC • ZTE
Domestic Companies Involved	• IPAY • Sergek	• Government	• Government	• Government	• Government • ECU 911
Data Privacy Legislation	Yes	Yes	Yes	Yes	Yes
Known Data Privacy Scandals	Yes	Yes	No	No	Yes


GDP for Central Asia and Ecuador
Country
Ecuador
Kazakhstan
Kyrgyzstan
Tajikistan
Turkmenistan
Uzbekistan
GDP in USD
2.0e+11
1.5e+11
1.0e+11
5.0e+10
0.0e+00
1996
1998
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
Year
Source: World Bank


Freedom House Scores for Central Asia and Ecuador
Country
Ecuador
Kazakhstan
Kyrgyzstan
Tajikistan
Turkmenistan
Uzbekistan
Freedom Index
100
75
50
25
0
2013
2014
2015
2016
2017
2018
2019
2020
Year
Source: Freedom House



Ecuador can be used as a comparative for Central Asian states for a number of reasons. Demographically, Ecuador has a population slightly larger than Kazakhstan's, but lower than Uzbekistan's.105 In terms of GDP, it is slightly below Kazakhstan, but overall comparable to the region. In terms of its government type, Ecuador is labeled as "Partly Free," similar to Kyrgyzstan, but Ecuador's scores are slightly higher on the "Freedom in the World" index. In terms of governance, Ecuador scores slightly lower than Kazakhstan on both the "Rule of Law" and "Government Effectiveness" indexes, but higher than all other Central Asian states. From a broad perspective, therefore, Ecuador is a developing, partially free country with comparable population sizes, governance record, and economic power to those of countries in Central Asia.

Country Profile: Ecuador

Ecuador is an even better case for comparison when looking at economic relations to China, especially in terms of Chinese ICT company involvement in digital surveillance. China expanded its role in South America around the 2008 financial crisis and began offering South American countries economic assistance in the form of loans.[106] This resulted in China's becoming South America's top trading partner.[107] Ecuador began signing deals with China in 2011 for infrastructure projects, often backed by Chinese loans, which it has continued to do since. In 2018, the government exchanged 80 percent of Ecuador's oil exports in return for around $19 billion in loans, which is only one of the many loan schemes the government has pursued with China.[108]

---

[105] "Population, Total - Tajikistan, Kyrgyz Republic, Ecuador, Turkmenistan, Uzbekistan, Kazakhstan | Data," World Bank, accessed April 12, 2020, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=TJ-KG-EC-TM-UZ-KZ.

[106] Nicholas Casey and Clifford Krauss, "It Doesn't Matter If Ecuador Can Afford This Dam. China Still Gets Paid," *New York Times*, December 24, 2018, https://www.nytimes.com/2018/12/24/world/americas/ecuador-china-dam.html.

[107] Ibid

[108] Ibid

One of the original Ecuadorian deals with China included the creation of a large-scale surveillance network that would be designed, built, and partially managed by Chinese ICT companies.[109] Ecuador's purchase of this system was in part inspired by an Ecuadorian delegation's tour of Beijing's surveillance system during the 2008 Olympic games. Since 2011, Ecuador's Chinese surveillance network has drastically expanded in size and was given the name ECU-911.[110] This system has been built and operated by two ICT companies: Huawei and CEIEC. ECU-911 now includes more than 4,000 cameras and 16 monitoring centers, employs more than 3,000 people, has thermal cameras for volcano monitoring, employs night vision drones, recently began incorporating facial recognition cameras along with an artificial intelligence research lab, and operates countrywide.[111] Its success supposedly inspired Venezuela, Bolivia, and Angola to purchase replica systems, which in turn sparked a wave of other developing countries' purchasing digital surveillance technology from China.

Ecuador is interesting because it purchased a complete digital surveillance system from Chinese ICT companies before almost any other country. China treated Ecuador as a flagship program to see how effective and profitable exporting digital surveillance could be and found a high demand from the developing world. This sparked the now-worldwide phenomenon of Chinese ICT companies exporting digital surveillance to developing countries, including those of Central Asia. Three of the Chinese ICT companies—Huawei, CEIEC, and Zeta—that are active in Ecuador are also operating in Central Asia to develop surveillance systems. While the use and implementation of FRT is as new to Ecuador as it is to Central Asia, the scale of ECU-911, the use of multiple types of technology, and the degree of Chinese ICT involvement in management is far greater as a result of Ecuador's having cooperated with China for a much longer period of time. Analyzing Ecuador's digital sphere, governance practices, and ECU-911 specifically will demonstrate the similarities between it and Central Asia. This will also indicate the probable trajectory for Central Asia. Ecuador, therefore, offers an insight into what Central Asia might look like in the coming years.

Ecuador's Digital Infrastructure and Regulatory Environment

In Ecuador, around 57 percent of the population has access to the Internet, which is considered partially free.[112] Ecuador's Internet was much more illiberal under the previous president Rafel Correa, but his successor President Lenin Moreno has taken steps to liberalize the Internet. Seven major ISPs are active in Ecuador along with hundreds of smaller ISPs. The fixed line market is dominated by the state-owned National Telecommunications Corporation (CNT), and the mobile Internet is dominated by a Brazilian company in addition to CNT's large market share.[113] There are multiple Internet routes to Ecuador that include the newest Pacific Caribbean Cable System—a high-speed fiber-optic cable—that was completed in 2015 by a consortium of companies.[114] Both wired and wireless Internet are widely available in the country, although there have been

---

[109] Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State - *The New York Times*," April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

[110] Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

[111] Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China," *Foreign Policy,* August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

[112] "Refworld | Freedom on the Net 2018 - Ecuador," Refworld, accessed November 1, 2018, https://www.refworld.org/docid/5be16b1d6.html.

[113] "Refworld | Freedom on the Net 2018 - Ecuador," Refworld, accessed November 1, 2018, https://www.refworld.org/docid/5be16b1d6.html.

[114] Ibid

difficulties in expanding Internet access to rural areas. A variety of international companies are involved with Ecuador's Internet sphere, including ZTE, which built a large-scale virtual IP Multimedia Subsystem in South America that includes Ecuador.[115] CNT also began launching a 5G network in cooperation with Huawei in 2019.[116]

Ecuador began creating its nationwide biometric database in 2012; it included photographs, personal information, employment information, financial records, and car ownership data.[117] This registration was used to issue Ecuadorian biometric passports that have chips containing facial data, fingerprints, and demographic information.[118] In 2019, however, the registration was the subject of a massive data breach due to an unsecured server, which resulted in more than 20 million Ecuadorians' having their personal data exposed.[119] Worryingly, while the biometric registry is not entirely secure, it has been instrumental in the creation and expansion of ECU-911.

ECU-911 began being built in 2011 and was designed by CEIEC, but it relies largely on hardware from Huawei. While it began from a $240 million loan and only in the capital, Quito, the system has been expanded upon since 2011, relying on additional Chinese loans.[120] CEIEC provided engineers and technicians who helped construct the system and who still currently work in the system's lab and command centers. Huawei provided the surveillance cameras, data storage systems, and a portable rapid deployment system.[121] This system has recently grown again by including thermal monitors, drones, and facial recognition cameras.[122] Before 2016, ECU-911 relied entirely on CCTV cameras and the use of sixteen regional response centers where government employees would physically monitor the camera feeds to identify criminal activity.[123] In 2016, however, reports began emerging that thousands of ECU-911 cameras were beginning to test facial recognition software. This was coupled with the creation of a research lab in 2016 that was inaugurated with a visit from President Xi. It was reported that in this research lab CEIEIC engineers worked "day and night" to develop intelligent video analysis to allow ECU-911 to begin integrating facial recognition.[124] In 2019 it was officially announced that FRT would be used in Ecuador's airports and in major cities.[125]

---

[115] "Telefonica, ZTE Deploy VIMS in LatAm Ahead of VoLTE Rollout," December 20, 2016, https://www.commsupdate.com/articles/2016/12/20/telefonica-zte-deploy-vims-in-latam-ahead-of-volte-rollout/.

[116] "Huawei Zhuli Eguaduoer Kaiqi 5G" [Huawei Helps Ecuador Turn on 5G], Huawei, July 18, 2019, https://www.huawei.com/cn/press-events/news/2019/7/huawei-ecuador-5g.

[117] James Stickland, "Ecuador Data Breach: An Entire Nation's Data Exposed," *Veridium*, October 2, 2019, https://veridiumid.com/ecuador-data-breach-an-entire-nations-data-exposed/.

[118] "Ecuador Incorporates 32 Historical Figures to the Electronic Passport," – *Ministerio de Relaciones Exteriores y Movilidad Humana*, May 27, 2018, https://www.cancilleria.gob.ec/en/ecuador-incorporates-32-historical-figures-to-the-electronic-passport/.

[119] James Stickland, "Ecuador Data Breach: An Entire Nation's Data Exposed," *Veridium*, October 2, 2019, https://veridiumid.com/ecuador-data-breach-an-entire-nations-data-exposed/.

[120] Frank Fang, "China Provides Technology for Ecuador's Mass-Surveillance ECU 911 Emergency System," *CuencaHighLife,* December 28, 2019, https://cuencahighlife.com/china-provides-technology-for-ecuadors-mass-surveillance-ecu-911-emergency-system/.

[121] Charles Rollet, "Chinese Government Builds Far-Reaching, Allegedly Corrupt, Surveillance System in Ecuador," IPVM, 27:47 400AD, https://ipvm.com/reports/china-ecuador.

[122] Frank Fang, "China Provides Technology for Ecuador's Mass-Surveillance ECU 911 Emergency System," *CuencaHighLife,* December 28, 2019, https://cuencahighlife.com/china-provides-technology-for-ecuadors-mass-surveillance-ecu-911-emergency-system/.

[123] Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

[124] Charles Rollet, "Chinese Government Builds Far-Reaching, Allegedly Corrupt, Surveillance System in Ecuador," IPVM, 27:47 400AD, https://ipvm.com/reports/china-ecuador.

[125] Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China," *Foreign Policy*, August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

Ecuador's legal environment and surveillance practices are generally on par with those of Central Asia, but they have improved under President Moreno. Ecuador passed in 2008 a resolution that established data privacy as a right but failed to develop regulations for that right until recently.[126] In 2019, because of the large-scale data breach, the Ecuadorian government began to fast-track personal data privacy legislation similar to GDPR, but it has not yet completed the legislation itself. The previous President Correa created the National Secretariat of Intelligence (SENAIAN) in 2009 to monitor the digital activity of Ecuadorian citizens for "the integral security of the state, society, and democracy."[127] Recently revealed evidence suggests that SENAIAN actively spied on journalists, politicians, activists, and citizens while it was operating. In 2018, however, the new President Moreno abolished SENAIAN because of "citizens' ethical demands" and replaced it with a Coordinating Unit of Public Security under his own direct control.[128] It is unclear if this new government organ will cease the surveillance measures practiced by its predecessor. Overall, Moreno presents himself as a liberal reformer to the more authoritarian Correa, but only a month after abolishing SENAIAN, Moreno's administration ordered all ISPs to keep an updated registry of subscriptions without providing any transparency for its use of personal data.[129] With Ecuador completing personal data privacy legislation soon, the new Ecuadorian government's surveillance measures may become more transparent. Even if this legislation is adopted, however, its existence does not prevent surveillance practices as can be seen from Central Asia.

Unlike the digital surveillance systems in Central Asia, digital surveillance systems in Ecuador, specifically the operation and management of ECU-911, are better understood. Data storage and management happens at each regional management center, and the system is fully scalable.[130] The hardware and expertise utilized to create and manage the system have come from Huawei and CEIEC, respectively, which in combination with our knowledge of ECU-911's overall infrastructure, demonstrates the high degree of access that Chinese ICT companies enjoy. Given the security risks and political relationships these two companies have to the Chinese government, it can be assumed that China has access to domestic Ecuadorian data. Unlike in Central Asia, where Chinese ICT involvement can only be inferred, in Ecuador it is openly known that CEIEC engineers work in ECU-911's headquarters and that the hardware, data storage systems, and management software have been provided by Huawei. The creation of a research laboratory to develop facial recognition capabilities signaled Ecuador's interest in expanding ECU-911 and switching from manual monitoring to automatic, AI monitoring. Having successfully done both, the Ecuadorian government has made its support of ECU-911 and the use of FRT clear.

Ecuador has continually expanded ECU-911 under both the previous autocratic-leaning president and the current president. Both have publicly supported the project and have actively courted greater Chinese investment. ECU-911 has also been credited with cutting down crime by 11.8 percent according to Ecuador's National Statistics and Census Institute.[131] Finally, according to the *New York Times*'s report on ECU-911, the surveillance program generally enjoys high support among Ecuadorians, despite the degree of Chinese ICT cooperation's

---

[126] Scott Ikeda, "Leak of the Personal Information of 20 Million in Ecuador Data Breach Leads to Fast-Tracking of an Improved Data Privacy Law," *CPO Magazine,* September 27, 2019, https://www.cpomagazine.com/cyber-security/leak-of-the-personal-information-of-20-million-in-ecuador-data-breach-leads-to-fast-tracking-of-an-improved-data-privacy-law/.

[127] "Refworld | Freedom on the Net 2018 - Ecuador," Refworld, accessed November 1, 2018, https://www.refworld.org/docid/5be16b1d6.html.

[128] "Refworld | Freedom on the Net 2018 - Ecuador," Refworld, accessed November 1, 2018, https://www.refworld.org/docid/5be16b1d6.html.

[129] Ibid

[130] Danilo Corral-De-Witt et al., "From E-911 to NG-911: Overview and Challenges in Ecuador," *IEEE Access* 6 (2018): 42578–91, https://doi.org/10.1109/ACCESS.2018.2858751.

[131] "Feature: Chinese Technology Brings Falling Crime Rate to Ecuador," *XinhuaNet,* January 19, 2018, http://www.xinhuanet.com/english/2018-01/19/c_136908255.htm.

being common knowledge.[132] Considering the signaled support of ECU-911 from two Ecuadorian presidents despite the differences in their political tendencies, the supposed effectiveness of ECU-911, and the general support of the Ecuadorian people, it is clear that Ecuador will continue to expand this system. It is also likely that the government in cooperation with Huawei and CEIEIC will outfit the entire system with FRT capabilities, which should further improve its effectiveness. Ecuador was China's case study for measuring the demand for digital surveillance, and it has successfully demonstrated the highest efficiency a Chinese-designed and -operated surveillance apparatus can function. Ecuador will continue to be the litmus test for predicting the trajectories of similar states that seek the benefits of improving suppressive capacity through technology. In this sense, Ecuador demonstrates the likely trajectory that Central Asian countries will follow if they continue expanding their surveillance networks through partnerships with Chinese ICT companies.

Conclusions

Digital surveillance that relies on artificial intelligence and facial recognition systems has the capacity to dramatically alter state–societal relations and allow states to develop fully panoptic societies. States have been prevented from adopting such models of governance because the technology to do so did not exist and often countries, especially in the developing world, lacked the digital infrastructure and expertise to create the required sophisticated surveillance apparatuses. China, however, through numerous ICT companies has both developed Safe City technology that can be implemented on a countrywide level but has also begun exporting this technology as a commodity.

It is logical that the most likely clients of this technology would be authoritarian or semi-democratic countries because they have the greatest incentives to improve suppressive capacity and the fewest constraints to implementing surveillance. These types of regimes are also the most common partners of BRI projects. Can this trend, therefore, be seen in Central Asia, which is a developing region that tends toward authoritarianism and has been a major target of BRI projects? In looking at four Central Asian republics, we see that the answer is clearly yes. Central Asian governments are eager to develop their digital surveillance systems largely through partnerships with Chinese ICT companies. Throughout the four Central Asian republics analyzed, all four have similar timelines for developing their individual Safe City projects. Kazakhstan has attempted to balance Chinese ICT involvement by integrating domestic IT companies into their surveillance systems. The other countries, however, have simply outsourced the creation and potentially management of their systems to Chinese companies. In each Central Asian case the details of operation and management are not known, but what is known suggests that large-scale digital projects are being implemented, data centers are being built, and expertise that would not necessarily have been available without foreign aid is being utilized.

Considering the porous personal data privacy legislation adopted by each country, alongside their histories of surveillance, it is clear that Central Asian states are interested in developing their surveillance systems to improve their degree of control over their societies. The ICT companies they have decided to cooperate with, however, are all either owned directly by the Chinese government or have suspiciously close ties to the CCP. This suggests, broadly, that China might have access to much of the data being produced by the surveillance systems it is building and operating within Central Asia. This then means that Central Asian countries are choosing to prioritize the development of their surveillance capacity and domestic control at the cost of greater Chinese

[132] Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

financial dependency and sacrificing autonomy over their citizens' data. As a result of these systems' being relatively new to the region, however, it is unclear how large these surveillance systems might become and what the region's surveillance environment might look like in the coming years.

A glimpse into Central Asia's future can be found by examining Ecuador, which was the original flagship country for Chinese ICT companies nearly a decade ago. ECU-911 is a countrywide surveillance system that involves thousands of cameras, management centers, drones, and newly installed facial recognition systems. It was designed by CEIEC and operated with Huawei hardware, two companies also active in Central Asia. ECU-911 proved the effectiveness of Chinese surveillance systems and inspired most of South America to purchase similar networks. In many ways, Ecuador and ECU-911 cemented the model that China would follow throughout the world, including Central Asia. It shares many similarities with Central Asian states, and its eagerness for further developing ECU-911 mirrors the rhetoric and policy of most Central Asian governments. It is probable, therefore, that surveillance systems on the same scale as ECU-911 will be adopted throughout Central Asia, and that they will be even more effective due to utilizing artificial intelligence. Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan have already signaled their intention to move toward this direction by expanding their surveillance systems to other cities and announcing plans to create nationwide systems. ECU-911 will not be a unique case in the world; instead, it, along with contemporary networks in Central Asia, will simply be the first of many throughout the world.

On a geopolitical level this has implications for both BRI recipient countries and China. As seen in Ecuador and Central Asia, these surveillance systems come at the cost of autonomy and dependency. It is difficult to change the operation and hardware of digital infrastructure if its foundation is provided by one country. Considering China is the most likely state to begin outsourcing 5G globally, BRI recipient countries will be entirely dependent on Chinese ICT companies for their own digital spheres and surveillance networks. The Chinese government has made it an open goal to become the technological center of the world, and between 5G and global ICT reliance, this future might become a reality where the Chinese government will have direct and indirect access to global data networks.

At a societal level, the further development of digital surveillance might fundamentally alter state–societal relations. This technology has the capacity to remove certain fundamental constraints on a government's power over its citizenry. The rise of authoritarianism is already a notable aspect of the current world order, and sophisticated digital surveillance might expedite this process and ultimately make it far more difficult to fight against tyrannical regimes. Central Asia, therefore, demonstrates the beginning of a global trend that may shift geopolitical power away from the West toward China and define new state–societal relations where people live within perfectly panoptic environments.

Bibliography

Akhmediarov, Lukpan. "Kitaiskaia kompaniia stroit v ZKO tsentr khraneniia informatsii" ["A Chinese Company is Building an Information Storage Center in WKO]. Uralskaia Nedelia, 2019, https://www.uralskweek.kz/2020/02/12/kitajskaya-kompaniya-stroit-v-zko-centr-xraneniya-informacii/.

Ashurov, Abdullo. "Smartfony Huawei v Tadzhikistane populiarny. A bezopasny li?" [Huawei Smartphones are Popular in Tajikistan. Are they Safe?]. Radio Ozodi, 2019. https://rus.ozodi.org/a/29692588.html.

Bloomberg.com. “Costar Group Co Ltd - Company Profile and News.” Accessed April 2, 2020. https://www.bloomberg.com/profile/company/002189:CH.

Bluescreen. “Chto Slozhnee “Sozdat «umnyi Gorod» Ili Nauchitsia v Nem Zhit?” [What is More Difficult “to Create a “Smart City” or to Learn to Live with it?]. Accessed May 27, 2019. https://bluescreen.kz/digital-kazakhstan/chto-slozhnee-sozdat-umnyj-gorod-ili-nauchitsja-v-nem-zhit/.

Casey, Nicholas, and Clifford Krauss. “It Doesn’t Matter If Ecuador Can Afford This Dam. China Still Gets Paid. - The New York Times.” *New York Times*, December 24, 2018. https://www.nytimes.com/2018/12/24/world/americas/ecuador-china-dam.html.

Cimpanu, Catalin. “Kazakhstan Government Is Now Intercepting All HTTPS Traffic.” ZDNet, Accessed March 28, 2020. https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/.

CITIC.com. “CITIC Limited.” Accessed April 2, 2020. https://www.citic.com/en/.

Commsupdate.com. “Telefonica, ZTE Deploy VIMS in LatAm Ahead of VoLTE Rollout,” December 20, 2016. https://www.commsupdate.com/articles/2016/12/20/telefonica-zte-deploy-vims-in-latam-ahead-of-volte-rollout/.

Corral-De-Witt, Danilo, Enrique V. Carrera, José A. Matamoros-Vargas, Sergio Muñoz-Romero, José Luis Rojo-Álvarez, and Kemal Tepe. “From E-911 to NG-911: Overview and Challenges in Ecuador.” *IEEE Access* 6 (2018): 42578–91. https://doi.org/10.1109/ACCESS.2018.2858751.

Dentons.com. “Uzbekistan to Develop Smart Cities,” January 28, 2019. https://www.dentons.com/en/insights/alerts/2019/january/28/uzbekistan-to-develop-smart-cities.

Digital Report. “80% naseleniia Uzbekistana obespecheno biometricheskimi pasportami” [80% of the Population of Uzbekistan has been Provided Biometric Passports]. April 12, 2017. https://digital.report/80-naseleniya-uzbekistana-obespecheno-biometricheskimi-pasportami/.

———. “Kyrgyzstan: State of Affairs report.” April 18, 2018. https://digital.report/kyrgyzstan-state-of-affairs-report/.

———. “V Uzbekistane Vvedut Biometricheskie Zagranpasporta s 1 Ianvaria 2019 Goda” [Biometric Passports to Be Introduced in Uzbekistan from January 1, 2019]. August 18, 2017. https://digital.report/v-uzbekistane-vvedut-biometricheskie-zagranpasporta-s-1-yanvarya-2019-goda/.

———. “Obzor Telekom Rynka Tadzhikistana: Fiksirovannaia, Mobilnaia i Mezhdunarodnaia Sviaz” [Tajikistan Telecom Market Review: Fixed, Mobile and International Communications].

June 5, 2017. https://digital.report/tadzhikistan-svyaz/.

Doffman, Zak. “Warning as Millions Of Chinese-Made Cameras Can Be Hacked To Spy On Users: Report.” *Forbes*, Accessed March 28, 2020. https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/.

Enelane, Nikolai. “Kak Rabotaet Proekt ‘Sergek’” [How the ‘Sergek’ Project Works]. *Informbiuro*, 2019. https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html.

Faskhumdinov, Galim. “Tadzhikistan podgotovil biometricheskie pasporta v Germanii” [Tajikistan Prepared Biometric Passports in Germany] *DW*, February 2010. https://www.dw.com/ru/%D1%82%D0%B0%D0%B4%D0%B6%D0%B8%D0%BA%D0%B8%D1%81%D1%82%D0%B0%D0%BD-%D0%BF%D0%BE%D0%B4%D0%B3%D0%BE%D1%82%D0%BE%D0%B2%D0%B8%D0%BB-%D0%B1%D0%B8%D-0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5-%D0%BF%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%B0-%D0%B2-%D0%B3%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D0%B8/a-5198915.

Freedom House. “Ecuador.” Accessed April 12, 2020. https://freedomhouse.org/country/ecuador/freedom-world/2020.

Fang, Frank. “China Provides Technology for Ecuador’s Mass-Surveillance ECU 911 Emergency System.” *CuencaHighLife*, December 28, 2019. https://cuencahighlife.com/china-provides-technology-for-ecuadors-mass-surveillance-ecu-911-emergency-system/.

Fidler, Mailyn. “African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts.” *Council on Foreign Relations*, March 7, 2018. https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

Freedom House. “Freedom in the World.” Accessed May 15, 2020. https://freedomhouse.org/report/freedom-world.

Giiasov, Negmat. “Grazhdane Kyrgyzstana Poluchat Biometricheskie Zagranpasporta Lish k 2021 Godu” [Citizens of Kyrgyzstan Will Receive Biometric Passports Only by 2021]. *Aziia TV*. May 8, 2019. http://asiatv.kg/2019/08/05/%D0%B3%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%D0%B5-%D0%BA%D1%8B%D1%80%D0%B3%D1%8B%D0%B7%D1%81%D1%82%D0%B0%D0%BD%D0%B0-%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B0%D1%82-%D0%B1%D0%B8%D0%BE%D0%BC%D0%B5%D1%82/.

Gosudarstvennaia Registratsionnaia Sluzhba. “Zakon KR” [Law of the Kyrgyz Republic]. Accessed April 1, 2020. https://grs.gov.kg/ru/documents/laws/29-Zakon-KR-O-biomietrichieskoi-rieghistratsii-ghrazh/.

Hashimova, Umida. “China Dominates Digital Infrastructure in Uzbekistan.” *The Diplomat*, June 28, 2019. https://thediplomat.com/2019/06/china-dominates-digital-infrastructure-in-uzbekistan/.

Huawei. “Huawei Zhuli Eguaduoer Kaiqi 5G” [Huawei Helps Ecuador Turn on 5G]. July 18, 2019. https://www.huawei.com/cn/press-events/news/2019/7/huawei-ecuador-5g.

Human Rights Watch. “World Report 2020: Rights Trends in Kyrgyzstan.” December 10, 2019. https://www.hrw.org/world-report/2020/country-chapters/kyrgyzstan.

———. “World Report 2020: Rights Trends in Tajikistan.” December 10, 2019. https://www.hrw.org/world-report/2020/country-chapters/tajikistan.

———. "World Report 2020: Rights Trends in Uzbekistan." December 10, 2019. https://www.hrw.org/world-report/2020/country-chapters/uzbekistan.

Ikeda, Scott. "Leak of the Personal Information of 20 Million in Ecuador Data Breach Leads to Fast-Tracking of an Improved Data Privacy Law." *CPO Magazine*, September 27, 2019. https://www.cpomagazine.com/cyber-security/leak-of-the-personal-information-of-20-million-in-ecuador-data-breach-leads-to-fast-tracking-of-an-improved-data-privacy-law/.

Iuldashev, Avaz. "Skolko Grazhdan Tadzhikistana Imeiut Biometricheskie Pasporta?" [How Many Tajik Citizens Have Biometric Passports?]. *Novosti Tadzhikistana ASIA-Plus*, 2019. https://www.asiaplustj.info/ru/news/tajikistan/society/20190802/v-mid-soobtshili-skolko-grazhdan-tadzhikistana-imeyut-biometricheskie-pasporta.

Informatsionnaia sistema PARAGRAF. "Zakon Respubliki Kazakhstan Ot 21 Dekabria 1995 Goda № 2710 «Ob Organakh Natsionalnoi Bezopasnosti Respubliki Kazakhstan» (s Izmeneniiami i Dopolneniiami Po Sostoianiiu Na 10.01.2020 g.)" [Law of the Republic of Kazakhstan dated December 21, 1995 No. 2710 "On the National Security Bodies of the Republic of Kazakhstan" (with Amendments and Additions as of 10.01.2020)]. Accessed March 28, 2020, //online.zakon.kz/Document/?doc_id=1005971.

———. "Zakon Respubliki Kazakhstan Ot 21 Maia 2013 Goda № 94-V «O Personalnykh Dannykh i Ikh Zashchite» (s Izmeneniiami i Dopolneniiami Po Sostoiâniiu Na 28.12.2017 g.)" [The Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V" On Personal Data and Their Protection "(with Changes and Additions as of December 28, 2017]. Accessed March 28, 2020, //online.zakon.kz/Document/?doc_id=31396226.

Jardine, Bradley. "China's Surveillance State Has Eyes on Central Asia." *Foreign Policy*, November 15, 2019. https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/.

Karavansarai. "V Bishkeke budet ustanovlena sistema raspoznavaniia lits v ramkakh proekta Smart City" [A Face Recognition System Will be Installed in Bishkek as Part of the Smart City project].

February 9, 2018. https://central.asianews.com/ru/articles/cnmi_ca/newsbriefs/2018/02/09/newsbrief-02.

Kelleher, Kevin. "Trump, China and ZTE: An Explainer." *Fortune*, June 13, 2018. https://fortune.com/2018/06/13/zte-trump-china-heres-fuss-all-about/.

Kondrateva, Dasha. âKyrgyzstanis Skeptical about Government Biometric Data Drive · Global Voices.â *Global Voices*, November 24, 2014. https://globalvoices.org/2014/11/24/kyrgyzstanis-skeptical-about-government-biometric-data-drive/.

Kudryavtseva, Tatyana. "Passport Data of Kyrgyzstanis to Be Sold to Banks, Cellular Companies." *24.Kg*, November 6, 2019, sec. English. https://24.kg/english/134288__Passport_data_of_Kyrgyzstanis_to_be_sold_to_banks_cellular_companies/.

Kunavut, Kunagorn, Atsuko Okuda, and Dongjung Lee. "Belt and Road Initiative (BRI): Enhancing ICT Connectivity in China-Central Asia Corridor." *Journal of Infrastructure, Policy and Development* 2, no. 1 (February 27, 2018): 116. https://doi.org/10.24294/jipd.v2i1.164.

Kursiv - Delovye Novosti Kazakhstana. "Zloumyshlenniki vylozhili v set dannye millionov kazakhstantsev" [Attackers Have Posted the Data of Millions of Kazakhstanis on the Network]. April 7, 2019. https://kursiv.kz/news/obschestvo/2019-07/zloumyshlenniki-vylozhili-v-set-dannye-millionov-kazakhstancev.

Lex.uz. "ZRU-547-Son 02.07.2019. O Personalnykh Dannykh" [ZRU-547-Son 02.07.2019. About Personal Data]. Accessed April 2, 2020. https://lex.uz/docs/4396428.

Ministerio de Relaciones Exteriores y Movilidad Humana. "Ecuador Incorporates 32 Historical Figures to the Electronic Passport." May 27, 2018. https://www.cancilleria.gob.ec/en/ecuador-incorporates-32-historical-figures-to-the-electronic-passport/.

Ministerstvo Iustitsii Kyrgyzskoi Respubliki [Ministry of Justice of the Kyrgyz Republic]. "Zakon KR ot 14 Aprelia 2008 Goda № 58 'Ob Informatsii Personalnogo Xaraktera'" [Law of the Kyrgyz Republic of April 14, 2008 No. 58' On Personal Information]. April 1, 2020. http://cbd.minjust.gov.kg/act/view/ru-ru/202269.

Mogilevskii, Roman. "Kyrgyzstan and the Belt and Road Initiative." Bishkek, Kyrgyzstan: University of Central Asia: Graduate School of Development, 2019.

Molbulak.ru. "V Tadzhikistane Prokhodit Massovaia Daktiloskopiia" [Mass Fingerprinting is Underway in Tajikistan]. November 29, 2016. https://www.molbulak.ru/news/tadzhikistan/v-tadzhikistane-prokhodit-massovaya-daktiloskopiya/.

Moldabekov, Daniiar. „Evraziiskii kibersoiuz: Istoriia o nesamostoiatelьnosti Kazakhstana v oblasti kiber-bezopasnosti" [Eurasian Cyber Union: A Story of Kazakhstan's Dependence in Cyber Security]. *Vlast.kz*, February 19, 2019, https://vlast.kz/obsshestvo/31791-evrazijskij-kibersouz.html.

Mozur, Paul, Jonah M. Kessel, and Melissa Chan. "Made in China, Exported to the World: The Surveillance State - The New York Times." *New York Times*, April 24, 2019. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

Mukhitkyzy, Asemgul. ăRaspoznaet Dazhe v Maskakh». Nuzhny Li Kazakhstanu Kamery Hikvision?ă [Recognizes Even in Masks ă Does Kazakhstan Need Hikvision Cameras?]. *Radio Azattyk*, 2019, https://rus.azattyq.org/a/kazakhstan-china-survelliance-camera/30210035.html.

Narodnaia Gazeta. "Zakony Respubliki Tadzhikistan" [Laws of the Republic of Tajikistan]. Accessed April 1, 2020. http://www.narodnaya.tj/index.php?option=com_content&view=article&id=7232:2018-08-08-07-09-50&catid=69:zakoni&Itemid=171.

Oster, Shai. "China Tries Its Hand at Pre-Crime." *Bloomberg*, March 3, 2016. https://www.bloomberg.com/news/articles/2016-03-03/china-tries-its-hand-at-pre-crime.

Radio Free Europe/Radio Liberty. "Tashkent Forcing Internet Firms to Locate Uzbek User Data Within Uzbekistan." February 21, 2020. https://www.rferl.org/a/internet-firms-user-data-within-uzbekistan/30447111.html.

Reuters. "300044.SZ - Shenzhen Sunwin Intelligent Co.,Ltd. Profile." Accessed April 2, 2020. https://www.reuters.com/companies/300044.SZ.

Review.uz. "S 2021 Goda v Uzbekistane Vmesto Biometricheskogo Pasporta Budut Vydavatsia ID-Karty" [From 2021 in Uzbekistan ID-Cards will be Issued instead of a Biometric Passport]. March 9, 2020, https://review.uz/ru/post/s-2021-goda-v-uzbekistane-vmesto-biometricheskogo-pasporta-budut-vdavatsya-id-kart.

Reynolds, Sam. "For Tajikistan, the Belt and Road Is Paved with Good Intentions." *The National Interest*, August 23, 2018. https://nationalinterest.org/feature/tajikistan-belt-and-road-paved-good-intentions-29607.

Rickleton, Chris. "Kazakhstan Embraces Facial Recognition, Civil Society Recoils." *Eurasianet*, October 17, 2019. https://eurasianet.org/kazakhstan-embraces-facial-recognition-civil-society-recoils.

Rollet, Charles. "Chinese Government Builds Far-Reaching, Allegedly Corrupt, Surveillance System in Ecuador." *IPVM*, 27:47 400AD. https://ipvm.com/reports/china-ecuador.

———. "Ecuador's All-Seeing Eye Is Made in China." *Foreign Policy*, August 9, 2018. https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

Rysaliev, Aktan. "Kazakhstan Introducing Compulsory Fingerprinting Program." *Eurasianet*, November 15, 2016. https://eurasianet.org/kazakhstan-introducing-compulsory-fingerprinting-program.

Selezneva, Inga. "Kazakhstan Launches Pilot Programme Using Biometric Data to Deliver Public Services." *The Astana Times*, January 24, 2019, sec. Nation. https://astanatimes.com/2019/01/kazakhstan-launches-pilot-programme-using-biometric-data-to-deliver-public-services/.

Stickland, James. "Ecuador Data Breach: An Entire Nation's Data Exposed." *Veridium*, October 2, 2019. https://veridiumid.com/ecuador-data-breach-an-entire-nations-data-exposed/.

Syundyukova, Nazerke. "Data Center to Be Built in Nur Sultan." *The Qazaq Times*, September 12, 2019. https://qazaqtimes.com/en/article/69113.

Timofeeva, Daria. "Na ulitsakh Bishkeka poiavilis kamery raspoznavaniia lits. Kitai ustanovil ikh besplatno" [Face Recognition Cameras Appeared on the Streets of Bishkek. China Installed Them for Free]. *Nastoiashchee Vremia*, 2019. https://www.currenttime.tv/a/30246828.html.

Trubacheva, Tatiana. "Bolshoi Brat: Kak Budet Rabotat Natsionalnaia Sistema Videomonitoringa v Kazakhstane" [Big Brother: How the National Video Monitoring System Will Work in Kazakhstan]. *Forbes*, 2020, https://forbes.kz//process/technologies/bolshoy_brat_po-kazahski_1582187734/.

Tukhvatshin, Rinat. "Samarageti, epizod 1. Kak server pravitelstva Kyrgyzstana ispolzovali dlia popytki vliianiia na prezidentskie vybory" [Samaragate, Episode 1. The Government of Kyrgyzstan was used as a Server to try to Influence the Presidential Elections]. *KLOOP.KG - Novosti Kyrgyzstana,* October 26, 2017. https://kloop.kg/blog/2017/10/26/samara_elections_kg/.

Turdimov, Zhadmoliddin. “Uzbekistan privlechet svyshe $1 milliarda kitaǎkikh investitsii v razvitie tsifrovoi infrastruktury” [Uzbekistan will Attract over $1 Billion of Chinese investments in the Development of Digital Infrastructure]. *Kursiv - Delovye Novosti Kazakhstana,* April 2019. https://kursiv.kz/news/ekonomika/2019-04/uzbekistan-privlechet-svyshe-1-milliarda-kitayskikh-investiciy-v-razvitie.

Umarov, Temur. “China Looms Large in Central Asia.” *Carnegie Moscow Center*. Accessed April 2, 2020. https://carnegie.ru/commentary/81402.

Umarova, Aziza. “Why Kyrgyzstan Uses Biometrics in Its Voting System.” *GovInsider*, June 29, 2018, sec. Connected Gov. https://govinsider.asia/connected-gov/kyrgyzstan-uses-biometrics-voting-system/.

Vega.su. “About.” Accessed April 1, 2020. http://vega.su/en/about/.

World Bank. “GDP, PPP (Current International $) - Tajikistan, Kyrgyz Republic, Ecuador, Turkmenistan, Uzbekistan, Kazakhstan | Data.” Accessed April 12, 2020. https://data.worldbank.org/indicator/NY.GDP.MKTP.PP.CD?locations=TJ-KG-EC-TM-UZ-KZ.

———. “Population, Total - Tajikistan, Kyrgyz Republic, Ecuador, Turkmenistan, Uzbekistan, Kazakhstan | Data.” Accessed April 12, 2020. https://data.worldbank.org/indicator/SP.POP.TOTL?locations=TJ-KG-EC-TM-UZ-KZ.

———. “WGI 2019 Interactive > Documentation.” Accessed May 15, 2020. https://info.worldbank.org/governance/wgi/Home/Documents.

———. “World Bank Open Data | Data.” Accessed May 15, 2020. https://data.worldbank.org/.

Wood, Murakami David. “The Global Turn to Authoritariansim and After.” *Surveillance & Society* 15, no. 3/4 (2017): 357–70.

XinhuaNet. “Feature: Chinese Technology Brings Falling Crime Rate to Ecuador.” January 19, 2018. http://www.xinhuanet.com/english/2018-01/19/c_136908255.htm.

Yan, Tsz Yau. “China Taking Big Brother to Central Asia.” *Eurasia.net*, Accessed April 1, 2020. https://eurasianet.org/china-taking-big-brother-to-central-asia.

Yeniseyev, Maksim. “Tashkent ‘Safe City’ Project to Unify Security Information Systems.” *Caravanserai*, September 20, 2017. https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2017/09/20/feature-01.

Yujian, Wu, Zhang Yuzhe, Yu Ning, Qu Yunxu, Lin Jinbing, and Han Wei. “How Did an Ambitious Cross-Border Settlement Firm’s Dream Turn Sour?” *Caixin Global,* Accessed April 1, 2020. https://www.caixinglobal.com/2017-09-18/how-did-an-ambitious-cross-border-settlement-firms-dream-turn-sour-101146346.html.

Zhumakadyr kyzy, Bermet. “Right to Privacy in Kyrgyzstan.” *EUCAM*, January 21, 2020, sec. Commentaries. https://eucentralasia.eu/2020/01/right-to-privacy-in-kyrgyzstan/.

The Sino-Russian Digital Cooperation and Its Implications for Central Asia

Miranda Lupion[1]

Sino-Russian digital relations feature a complex ecosystem with emulation and cooperation, as well as competition and suspicion. China functions predominantly as a supplier, exporting (1) technology products and services and (2) Internet control and surveillance models to Commonwealth of Independent States (CIS) countries. Russia, in contrast, both produces and consumes products and policy. In certain domains, Moscow competes with Beijing to sell digital wares in Central Asian markets, and some Central Asia states have selectively adopted parts of Russian systems and laws. At the same time, the Russian government itself has signed lucrative contracts for Chinese information communications technology (ICT) and surveillance hardware and is increasingly implementing aspects of China's digital control methods.

The Chinese and Russian Models of Digital Control: A Brief Overview

Chinese and Russian leaders use "digital information technology . . . to surveil, repress and manipulate" citizens, each pursuing its own breed of what experts call "digital authoritarianism."[2] While both Beijing and Moscow place a premium on surveillance and filtering, their approaches vary. These differences are partially a relic of (1) the particular ideological trajectories that guided the regimes and (2) the historical circumstances facing the two states during the commercial Internet's birth. Under one-party rule, China brought the Internet under state control in 1996 with State Council Order No. 195. The Order requires Internet-connected devices to access the World Wide Web through a state-run "exit information channel" or exit node, laying the groundwork for government filtering.[3] In the mid-1990s, China had only 150,000 Internet users—a small fraction of its total population.[4] Asserting authority over the digital sphere from the get-go, the Chinese government sought to normalize filtering and surveillance. In this way, many Chinese Internet netizens never used an uncensored Internet in China.

---

[1] Research carried out as part of a Title VI–funded Innovation Fellowship at, and on behalf of, the Davis Center for Russian and Eurasian Studies.

[2] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (The Brookings Institution: Foreign Policy Program, August 2019), 1, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

[3] "Interim Provisions Governing the Management of the Computer Information Networks in The People's Republic of China Connecting to the International Network," Laws of the People's Republic of China, accessed November 15, 2020, http://www.asianlii.org/cn/legis/cen/laws/ipgtmotcinitprocttin1488/.

[4] Ibid., 3.

In contrast, during the same period, in Russia the RuNet or Russian-language portion of the Internet remained relatively free of state interference. The newly created Russian Federation was fighting hyperinflation, an uptick in crime and poverty, and a war in Chechnya; the net was not a major priority. At the time, President Boris Yeltsin's administration was also pursuing democratization and integration with the West, goals with which strict Internet censorship was not readily compatible.

That changed in the late 2000s and early 2010s, as an increasingly authoritarian regime watched seasoned autocrats fall in the Arab Spring protests and faced the anti-government rallies in the capital.[5] Social media facilitated opposition organization, amplified grievances, and allowed for the spread of information that undermined the dominant narrative. The Kremlin recognized the Web's potential to threaten regimes. In 2012, Russia's federal telecommunications regulator Roskomnadzor launched a blacklist or register of prohibited sites.[6] With a comparatively late start to Internet filtering, Moscow lacked the infrastructure, resources, and capacity to censor content consistently and effectively—as Beijing does.[7]

These legacies inform both states' current methods for filtering, censorship, and even surveillance. Russia relies on a lower-tech approach that promotes self-censorship, selective filtering, and more traditional telecommunications surveillance, all of which is backed by law. China's techniques are tech-heavy, employing artificial intelligence and impressive manpower to remove content and track citizens systematically.[8] Understanding the two approaches is crucial to analyzing what drives ICT policy diffusion (or the lack thereof) in Central Asia.

Russian and Chinese Approaches to Filtering and Censorship

Moscow uses a three-pronged technical, legal, and informational approach to control Internet content that rests on filtering and block lists, laws that encourage self-censorship, and pro-government information campaigns that both overwhelm and undermine alternative narratives. Most centrally, Internet service providers (ISPs) must filter content listed on Roskomnadzor's register.[9] Failure to block designated sites may result in hefty fines.

---

[5] Justin Sherman, "The Russian Doll of Putin's Internet Clampdown," *Wired*, May 1, 2020, https://www.wired.com/story/opinion-the-russian-doll-of-putins-internet-clampdown/.

[6] Jaclyn Kerr, "The Russian Model of Digital Control and Its Significance," in AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives, ed. Nicholas Wright, Strategic Multilayer Assessment (SMA) Periodic Publication (Department of Defense, 2018), 57.

[7] Max Seddon and Henry Foy, "Russian Technology: Can the Kremlin Control the Internet?," *Financial Times*, June 5, 2019.

[8] Robert Morgus, "The Spread of Russia's Digital Authoritarianism," in AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives, ed. Nicholas Wright, Strategic Multilayer Assessment (SMA) Periodic Publication (Department of Defense, 2018), 85.

[9] Ibid., 85.

Numerous laws give Roskomnadzor and the courts broad authority to order the blacklisting of sites and applications and the removal of categories of content. Most notable are:

- The Anti-Piracy Law (2013) addressing copyrighted material[10]
- The Anti-LGBT Propaganda Law (2014) targeting LGBT-youth support groups[11]
- The Law on Pre-Trial Blocking of Websites (2014) authorizing the blacklisting of sites that incite "extremism or riots"; used heavily during the Crimean annexation to target opposition[12]

Other laws encourage self-censorship, aiming to prevent the initial publication of anti-government material.[13] Examples include:

- The Bloggers Law (2014) requiring all bloggers with an "audience of more than 3,000" to register and take responsibility for the accuracy of material they post[14]
- The Anti-Encryption Law (2016) compelling encrypted messengers to furnish decryption keys to the Federal Security Service (FSB) (the law is part of the Yarovaya Amendments package, discussed in detail later)[15]

These laws, however, are selectively enforced and often used to target regime critics.[16] Legally enabled filtering complements the final major pillar of Russian policy: concerted, pro-regime information campaigns. The systematic promotion of Kremlin-backed narratives through digital news and social media strives to compete with and, ideally, overtake anti-regime content.[17]

The Russian government's capacity to filter trails its ambitions for digital control. In developing policy, Russia's security and regulator apparatuses neglect to take their limited technical capabilities into account.[18] As a result, Roskomnadzor sometimes struggles to make blacklisted sites and applications fully inaccessible. The regulator's deficiencies were most apparent in its 2018 campaign to block encrypted-messaging application Telegram in Russia. By targeting Telegram's IP address, ISPs accidentally took down millions of Web pages hosted at the same address. Telegram migrated its IP address to avoid targeting. The application remained consistently accessible through virtual private networks (VPNs) and often without VPNs. As discussed in a later section, the Russian government has recently sought to enhance its filtering capabilities with new Chinese-style approaches.

---

[10] "Russia Beefs up Anti-Piracy Laws," *BBC*, May 1, 2015, https://www.bbc.com/news/technology-32531275.

[11] "Propaganda Netraditsionnykh Seksualăıykh Otnoshenii Sredi Nesovershennoletnikh [Propaganda on Non-Traditional Sexual Orientation Aimed at Minors]," Pub. L. No. N 195-F3, Article 6.21 The Russian Federation's Code of Administrative Offenses (2013), http://www.consultant.ru/document/cons_doc_LAW_34661/f385ab5d34de901b2e5f3d08ac0b454481377d6a/.

[12] Olga Razumovskaya, "Putin Signs Bill Blocking Websites That Incite Rioting, Promote Extremism," *Wall Street Journal*, December 30, 2013, sec. World, http://www.wsj.com/articles/putin-signs-bill-blocking-websites-that-incite-rioting-promote-extremism-1388416128.

[13] Valentin Weber, "Why China's Internet Censorship Model Will Prevail Over Russia's," *Net Politics* (blog), December 12, 2017, https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.

[14] "'Draconian' Russian Net Law Enacted," *BBC*, August 1, 2014, sec. Technology, https://www.bbc.com/news/technology-28583669.

[15] "Russia: 'Big Brother' Law Harms Security, Rights," Human Rights Watch, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

[16] Kerr, "The Russian Model of Digital Control and Its Significance," 58.

[17] Morgus, "The Spread of Russia's Digital Authoritarianism," 86.

[18] Seddon and Foy, "Russian Technology: Can the Kremlin Control the Internet?"

In contrast, China effectively leverages real-time automated and extensive manual filtering to remove anti-regime content and block websites.[19] Colloquially known as the "Great Firewall," these digital censorship controls are a part of China's larger Golden Shield Project. Government developers integrated artificial intelligence (AI) to upgrade automatic keyword-based filtering.[20] Human capital is crucial as well. Chinese messaging application WeChat boasts 2 million employees tasked with policing public opinion—and this is for a single web service. For comparison, Roskomnadzor—the regulatory agency in Russia—counts only 3,000 employees total.[21] This integrated filtering system allows applications like Weibo (China's Twitter) to remove about a third of "contentious posts" within half an hour of their publication and 90 percent of such posts within a day.[22] With its efficient controls and domestic Web services (Weibo, Baidu, Alibaba, WeChat, etc.), China can also block entire Western platforms before they take off.[23] The government complements these efforts by banning nongovernment-approved VPNs and paying more than 2 million members of the so-called "50 Cent Party" to leave pro-regime comments on the Web.[24]

Digital Surveillance Methods in Russia and China

Both Moscow and Beijing track their citizens' digital and actual footsteps. While there is increasing overlap in the technologies they employ, the two countries have historically emphasized different aspects of surveillance.

In Russia, more traditional telecommunications and Internet surveillance techniques are most prevalent.[25] The 1995 Law on Operational Investigations granted the FSB the authority to monitor "all private communications of citizens, including electronic communications."[26] To this right operational, the government required telecommunications operators to install and pay for lawful interception equipment that sends a copy of all traffic to FSB servers.[27] Developed by KGB researchers in the 1980s, the System for Operative Investigative Activities (SORM) dictates the technical details of interception. First-generation SORM covered mobile and landline telephone traffic. Later updates to the system enabled collection of voice over Internet protocol (VoIP) and basic Internet traffic (SORM-2), while the most recent iteration of the specification (SORM-3) covers virtually all communications media (e-mail, GPS coordinates, IP addresses, social media messages, etc.).[28]

---

[19] Valentin Weber, "Understanding the Global Ramifications of China's Information Controls Model," in AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives, ed. Nicholas Wright, Strategic Multilayer Assessment (SMA) Periodic Publication (Department of Defense, 2018), 72.

[20] Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls" (The Open Technology Fund, September 2019), 10.

[21] Seddon and Foy, "Russian Technology: Can the Kremlin Control the Internet?"

[22] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 72.

[23] Weber, "Why China's Internet Censorship Model Will Prevail Over Russia's."

[24] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 72.

[25] Morgus, "The Spread of Russia's Digital Authoritarianism," 86–87.

[26] "Federalăyi Zakon 'Ob Operativno-Rozysknoi Deiatelăosti' [Federal Law on Operational and Investigative Activities]," Pub. L. No. N 144-ф3 (1995), http://www.libertarium.ru/l_sormlaw_101.

[27] Morgus, "The Spread of Russia's Digital Authoritarianism," 86–87.

[28] Andrei Soldatov and Irina Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You," *Wired*, 2012, https://www.wired.com/2012/12/russias-hand/; Sherman, "The Russian Doll of Putin's Internet Clampdown."

Two recent laws govern how SORM and other data is stored. Also known as the Data Localization Law, the User Data Storage Law (2014) stipulates that data on Russian citizens be held on servers located in Russia.[29] Among other provisions, the Yarovaya Amendments (2016) to Russia's laws governing terrorism compel telecommunications operators and ISPs to store communication content and metadata for six months and three years respectively.[30] Other surveillance-related laws require the provision of personally identifying information to use public WiFi, purchase a SIM card, and register for certain messaging applications.[31]

While Beijing monitors users' online activities as well, its video-enabled physical surveillance systems are second to none. Through its Safe Cities projects, China began to blanket the country with CCTV infrastructure. What initially functioned as a traffic monitoring system morphed into a pervasive tool for political surveillance.[32] The "Sharp Eyes" Initiative similarly entails erecting a national video surveillance network that will monitor the entire country.[33] As part of this program, the Chinese government now aims to cover all of China's public spaces with cameras by the end of 2020.[34] Beijing has been 100 percent covered since 2015.[35]

Over the past decade, the Chinese government has not only expanded but also upgraded these systems. The integration of facial recognition technology (FRT) into cameras is a major priority. Since 2018, the regime has funneled upward of US$2 billion into Chinese startups for AI-based FRT development.[36] The government has also sought to link physical cameras to Internet-of-Things (IoT) devices, like smart TVs.[37] Footage from cameras in conjunction with data from citizens' mobile phones informs citizens' social credit scores.[38] The Communist Party's "Strike Hard Campaign," which purportedly aims to root out violent extremism in Xinjiang, has taken this

---

[29] " O Vnesenii Izmenenii v Otdelʹnye Zakonodatelʹnye Akty Rossiiskoĭ Federatsii v Chasti Utochneniia Poriadka Obrabotki Personalʹnykh Dannykh v Informatsionno-Telekommunikatsionnykh Setiakh [Amendments to Specific Russian Federation Laws to Clarify the Processing of Personal Data on Information-Telecommunications Networks]," Pub. L. No. N 152-F3 (2014), http://pravo.gov.ru/proxy/ips/?docbody=&nd=102355893.

[30] "O Vnesenii Izmeneniĭ v Federalʹnyĭ Zakon «O Protivodeĭstvii Terrorizmu» i Otdelʹnye Zakonodatelʹnye Akty Rossiĭskoĭ Federatsii v Chasti Ustanovleniia Dopolnitelʹnykh Mer Protivodeĭstviia Terrorizmu i Obespecheniia Obshchestvennoĭ Bezopasnosti [On Amendments to the Federal Law 'On Combating Terrorism' and Separate Legislative Acts of the Russian Federation to Establish Additional Measures to Counter Terrorism and Ensure Public Safety]," Pub. L. No. 374- FZ (2016), http://www.kremlin.ru/acts/bank/41108/page/1.

[31] "Obzor Dokumenta: O Vnesenii Izmenenii v Federalʹnyĭ Zakon Ob Informatsii, Informatsionnykh Tekhnologiiakh i o Zashchite Informatsii i Otdelʹnye Zakonodatelʹnye Akty Rossiiskoi Federatsii Po Voprosam Uporiadocheniia Obmena Informatsiei s Ispolʹzovaniem Informatsionno-Telekommunikatsionnykh Setei [Summary of the Document: Amendments to the Federal Law 'On Information, Information Technologies and about Information Protection' and Certain Legislative Acts of the Russian Federation on Streamlining the Exchange of Information Using Information and Telecommunication Networks"]," August 8, 2014, http://www.garant.ru/hotlaw/federal/558201/; "Novye pravila identifikatsii v messendzherakh vstupili v silu," RIA News, 20190505T1314, https://ria.ru/20190505/1553268769.html; "O Vnesenii Izmeneniĭ v Federalʹnyĭ Zakon 'O Sviazi' [Changes to the Federal Law 'on Communications']," Pub. L. No. N 245-F3 (2017), http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284289&fld=134&dst=1000000001,0&rnd=0.10568643889263796%20%20#044800986310585156.

[32] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," The Diplomat, August 7, 2019, https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/.

[33] Louise Lucas and Emily Feng, "Inside China's Surveillance State," The Financial Times, July 20, 2018, https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543.

[34] Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 4.

[35] Ibid., 3.

[36] Ibid., 4.

[37] Ibid.

[38] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 72–73.

technology to the extreme, creating "the world's largest open air digital prison" for ethnic Uyghurs.[39] The system integrates CCTV cameras, biometric sensors and data collection, spyware on mobile devices, surveillance drones, and GPS tracking to monitor and often detain the region's Muslims.[40]

While maintaining its distinct approach to digital control, the Russian government has started to import aspects of Chinese surveillance and filtering policies, particularly smart physical surveillance mechanisms and infrastructure for isolating its national Internet. The next section discusses the extent and nature of this diffusion.

Dragon Diffusion? Russia's Selective Adoption of Chinese Digital Control Mechanisms and ICT

Over the past decade, Moscow has begun to integrate aspects of Beijing's policy into its existing digital control regimes. Among other measures, Russia has (1) enhanced its national filtering infrastructure, mimicking elements of China's Golden Shield, (2) sought to ban VPNs, and (3) adopted Safe Cities–style surveillance programs. To implement borrowed measures, the country relies on an unequal mix of Chinese- and domestically produced technology. In 2018 alone, the Kremlin procured 82 billion rubles' (about $1.24 billion at the 2018 exchange rate) worth of foreign hardware, spending only 18 billion (about $2.72 million) rubles on Russian-made equipment.[41] Russia's dependence on foreign surveillance and filtering technology leaves the country vulnerable to Chinese spying. To mitigate this threat without forgoing digital control aspirations, Russia has prioritized developing custom software to deploy on Chinese hardware.[42] Despite lingering espionage risks, Russia is looking to Chinese companies, like ZTE and Huawei, for future ICT projects.

Shields and Splinternets: Upgrading Russia's Filtering Architecture and Centralizing Its Internet Controls

From the get-go, Roskomnadzor's filtering system shared an underlying similarity with China's program: the blacklisting and blocking of key sites.[43] During the past five years, however, the Kremlin has sought to boost Roskomnadzor's precision with tools that would enable Chinese-style filtering of specific content (not just of entire websites).[44] These tactics would likely require widespread and automated use of Deep Packet Inspection

---

[39] Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 5.

[40] "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance; Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 5.

[41] Seddon and Foy, "Russian Technology: Can the Kremlin Control the Internet?"

[42] Valentin Weber, "The Sinicization of Russia's Cyber Sovereignty Model," Council on Foreign Relations, *Net Politics* (blog), April 1, 2020, https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model.

[43] Alexander Gabuev, "Digital Bromance: The Sino-Russian Partnership Racing Ahead," Carnegie Moscow Center, December 7, 2015, https://carnegie.ru/2015/12/07/digital-bromance-sino-russian-partnership-racing-ahead-pub-62253.

[44] Weber, "The Worldwide Web of Chinese and Russian Information Controls," 23.

(DPI) to complement and eventually replace ISP-based censorship.[45] Based on a 2015 bilateral cooperative agreement, Russia's Assistant on Internet Issues Igor Shchegolev has consulted with Lu Wei, the head of China's Internet information office, and Fang Binxing, the architect of China's firewall, on filtering infrastructure.[46] [47]

A series of November 2019 amendments to existing federal laws on ICT provide additional technical and legal support for this project. The amendments

- require ISPs to install DPI systems for targeted filtering[48]
- give Roskomnadzor the authority to take control of the Russian network during a crisis and to oblige all ISPs to route traffic through networks in Russia[49]
- develop infrastructure for a national Domain Name System (DNS)[50]

The media often refer to these amendments as the "Sovereign Internet Law," as they theoretically give the government the power to isolate the RuNet from the World Wide Web (creating a "splinternet" or sovereign Internet) and potentially shut off the Internet temporarily within Russia's borders. The Kremlin framed the legislative package as boosting the nation's defense against U.S. cyberattacks, but experts believe it serves to further Russian censorship.[51]

The amendments further Sino-Russian digital ties in two ways. The law's technical stipulations (1) pave the way for Chinese-style digital controls and (2) likely necessitate Chinese assistance to execute effectively.

If Moscow successfully implements the technical policies outlined above, Russia's digital censorship will more closely resemble China's program. The amendment requiring ISPs to install certain equipment suggests that Russia will continue to pursue a **Chinese-like hybrid filtering method**, using DPI and changes to protocols to determine which Internet traffic can pass.[52] Like China's system, the Kremlin's ideal filtering setup does not block all foreign sites; rather, it lets some information flow freely and censors certain topics.[53] As of January 2020, the Russian government claims to have tested this national Internet setup. The trials concentrated on firewalls that prevent protocol layers from relaying certain types of data.[54]

---

[45] Seddon and Foy, "Russian Technology: Can the Kremlin Control the Internet?"

[46] Andrei Soldatov and Irina Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact," the *Guardian*, November 29, 2016, http://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.

[47] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 73.

[48] "FederalăuyăZakon "O Vnesenii Izmenenii v FederalăuyăZakon 'O Sviazi' i FederalăuyăZakon 'Ob Informatsii, Informatsionnykh Tekhnologiiakh i o Zashchite Informatsii' [Federal Law "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies, and Information Protection'"]," Pub. L. No. 90- FZ (2019), http://publication.pravo.gov.ru/Document/View/0001201905010025.

[49] Ibid.

[50] Ibid.

[51] Zak Doffman, "Huawei Soars in Russia as Putin Engages in New 'Technological War,'" *Forbes*, November 3, 2019, https://www.forbes.com/sites/zakdoffman/2019/11/03/huawei-soars-in-russia-as-putin-engages-in-new-technological-war/#39c8782765ca.

[52] Sally Adee, "The Global Internet Is Disintegrating. What Comes Next?," *BBC*, May 14, 2019, https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

[53] Ibid.

[54] Lily Hay Newman, "Russia Takes a Big Step Toward Internet Isolation," *Wired*, accessed May 10, 2020, https://www.wired.com/story/russia-internet-control-disconnect-censorship/.

The amendments allow Roskomnadzor to assert greater central control over the Russian Internet using **traffic routing** and a **mirror DNS**. These are techniques Beijing already employs. Roskomnadzor now has the authority (although perhaps not the ability) to route all Internet traffic through domestic exchanges during a crisis.[55] Beijing already boasts centralized control over its traffic, relaying all packets through national "choke points."[56] China also uses DNS manipulation to direct traffic away from banned sites, a strategy Russia could adopt with its copy of the DNS.[57] A parallel web built on Russian servers with traffic guided through state-controlled connection points theoretically would allow Roskomnadzor to shut down the Internet across Russia.[58] [59] Internet blackouts are standard in China's playbook. Russia is even investing 2 billion rubles (about $25 million) in a Wikipedia alternative.[60] This effort to create domestic Web service substitutes to shore up its national narrative mimics China's use of homegrown platforms for activities like research, social networking, and chatting.[61]

Russia will continue to rely on China for the expertise and equipment necessary to carry out these policies. Retrofitting the Russian Internet with Chinese-style filtering and isolation mechanisms is challenging.[62] China has fewer ingress and egress points, while Russia lacks large choke points, making a major Internet shutdown complicated.[63] Experts have concluded that, given Russia's current regulatory and technical capacity, the country could not construct a DPI-based filtering platform on its own (although a Rostelecom-owned company is slated to supply some necessary equipment).[64] Instead, the Russian government must source hardware and help from China (although there is little publicly available information on filtering equipment exports). Finally, Russia's current strategy for killing the Web was developed in "close cooperation with China after a string of high-level meetings" in 2016.[65]

Twin VPN Bans: Diffusion(?) Without Capacity

Virtual Private Networks, or VPNs, challenge Chinese and Russian digital censorship and surveillance efforts. VPNs re-route user traffic through a remote server, disguising the device's IP address and allowing access to banned sites. As an added layer of security, VPNs often encrypt traffic, hindering surveillance efforts. Both Beijing and Moscow purport to block nongovernment-sanctioned VPNs. On paper, the policies are similar. State regulators (1) target VPN applications through filtering and/or removal from marketplaces and (2) threaten users with fines. The level of enforcement, however, varies between countries and with time.

---

[55] Federal'nyĭzakon "O vnesenii izmenenii v Federal'nyĭzakon "O sviazi i Federal'nyi zakon "Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii" [Federal law "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies, and Information Protection'"].

[56] Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law'" (DGAP Analysis: German Council on Foreign Relations, January 2020), 3, https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf.

[57] Adee, "The Global Internet Is Disintegrating. What Comes Next?"

[58] Seddon and Foy, "Russian Technology: Can the Kremlin Control the Internet?"

[59] The Russian government has previously carried out at least one Internet blackout. It occurred in Ingushetia during the 2018 protests over a border dispute. See Seddon and Foy.

[60] Newman, "Russia Takes a Big Step Toward Internet Isolation."

[61] Weber, "The Sinicization of Russia's Cyber Sovereignty Model."

[62] Newman, "Russia Takes a Big Step Toward Internet Isolation."

[63] Epifanova, "Deciphering Russia's 'Sovereign Internet Law,'" 7.

[64] Seddon and Foy, "Russian Technology: Can the Kremlin Control the Internet?"

[65] Soldatov and Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact."

Similar to filtering efforts, China's ban pre-dated Russia's and has generally been more successful. In the early 2010s, China began leveraging its "Great Firewall" to restrict access to non-approved VPNs.[66] Over time, the filtering system has improved its process for recognizing VPN protocols.[67] Beijing doubles-down on these efforts during sensitive periods, such as the anniversary of the Tiananmen Square protests. In July 2017, the Chinese government publicly ordered ISPs to block personal VPNs, and Apple removed VPN applications from its Chinese store.[68]

China's VPN ban may have paved the way for Russia's measures. Russia's law "On Anonymizers" went into effect on November 1, 2017—only a few months after China's crackdown.[69] For a period, authorities neglected to enforce the ban. This changed in 2019, when Roskomnadzor ordered ten popular VPN services, such as NordVPN and TorGuard, to filter according to the agency's blacklist or risk being blocked themselves.[70] With its less-than-stellar filtering capabilities, Roskomnadzor, however, lacks the capacity to enforce the ban, and many of the VPN providers have vowed to resist. In a tacit acknowledgment of its capacity shortcomings, Roskomnadzor has lobbied for an amendment to the law that would allow the agency to fine (rather than block) noncompliant VPN services.[71] In this way, the VPN ban may serve as another example of Chinese policy diffusion, in which Roskomnadzor's inferior technical capabilities thwart Chinese-level enforcement.

Safe Cities, Facial Recognition Technology, and Artificial Intelligence

Beyond mimicking China's censorship measures, Russia also copies aspects of its neighbor's surveillance systems, most notably its Safe Cities program. Moscow's Safe City project began in the mid-2000s. Updates to enhance existing capabilities followed. In 2018, China's Hikvision (in conjunction with Safe Logic) upgraded security cameras in more than 100,000 Moscow building entryways. The new equipment supports SIP protocol (for real-time video transfer) and software updates and connects to the unified system for emergency calls.[72] In the same year, the city announced a facial recognition technology (FRT) pilot in the Moscow metro.[73] In May 2019, the city government announced its biggest expansion yet with a tender to install FRT in up to 200,000 surveillance

---

[66] Charles Arthur, "China Cracks down on VPN Use," the *Guardian*, May 13, 2011, http://www.theguardian.com/technology/2011/may/13/china-cracks-down-on-vpn-use.

[67] Zach Toombs, "China's Censors Take on Virtual Private Networks," *The Diplomat*, November 6, 2014, https://thediplomat.com/2014/11/chinas-censors-take-on-virtual-private-networks/.

[68] Ryan Browne, "Russia Follows China in Tightening Internet Restrictions, Raising Fresh Censorship Concerns," *CNBC*, July 31, 2017, https://www.cnbc.com/2017/07/31/russia-follows-china-in-vpn-clampdown-raising-censorship-concerns.html.

[69] Ibid.

[70] Vyacheslav Polovinko and Lilit Sarkisyan, "Teperʹoni prishli za VPN [Now they're come for our VPNs]," Novaya Gazeta, March 28, 2019, https://www.novayagazeta.ru/articles/2019/03/28/80032-teper-oni-prishli-za-vpn.

[71] Yekaterina Brizgalova, "Роскомнадзор решил пока не блокировать VPN-сервисы [Roskomnadzor decided not to block VPN-services for now]," *Vedomosti*, June 26, 2019, https://www.vedomosti.ru/technology/articles/2019/06/26/805110-roskomnadzor.

[72] "Bezopasnyi Gorod Moskva Sozdaetsia Vmeste s Hikvision i Safe Logic [Together Hikvision and Safe Logic Create Safe City Moscow]," Hikvision, accessed May 17, 2020, https://hikvision.ru/success/city.

[73] Felix Light, "Russia Is Building One of the World's Largest Facial Recognition Surveillance Networks," *The Moscow Times*, November 12, 2019, https://www.themoscowtimes.com/2019/11/12/russia-building-one-of-worlds-largest-facial-recognition-networks-a68139.

cameras, with 105,000 connected by the end of 2019.[74] Outside of Moscow, the 2018 FIFA World Cup provided the impetus for the roll-out of FRT in the eleven host cities.[75] Saint Petersburg installed 30,000 cameras (5.53 per 1,000 residents) in 2019 alone. In Moscow, that figure stood at 146,000 or 11.7 per 1,000 residents. [76]

In implementing these programs, the authorities rely on a mix of foreign and domestic technology. To limit Beijing's access to collected data, Russia imports Chinese hardware, such as cameras, but prefers to deploy native software and algorithms for facial recognition.[77] (1) Ample training data and (2) a growing homegrown AI sector make this possible. Like China, Russia lacks rigorous data protection laws, allowing developers to legally access large pools of data for training facial recognition algorithms.[78] Still in its infancy, Russia's AI industry is comparatively small but exceptionally promising. The Russian government directs US$12.5 million annually toward AI research, aiming to grow the domestic market to US$400 million by 2021. Even at this pace, Chinese spending will outpace Russian investment, with Beijing splanning to spend US$150 billion in this sector by 2030.[79] The nature of activity also varies. Historically, the Russian government has invested heavily in AI applications for the military, developing smart fighter jets, drones, and missiles.[80] In comparison, China appears to have robust AI development in both the public and private sectors.

Although the Ministry of Defense still leads in AI R&D, Russia's private sector has enjoyed significant success. A relic of the Soviet education system, the national curriculum's emphasis on mathematics has produced top computer science talent. Software from Russia's NTech Labs and Vision Labs makes the National Institute for Standards and Technology's (NIST) top ten list for facial recognition algorithms.[81] NTech Lab's FanceN algorithm took first place in the 2015 World Championship for Facial Recognition Technology, and, in 2019, Samsung Electronics founded an AI center in Moscow.[82] The Russian government increasingly turns to these companies to furnish software for projects, like Safe Cities. However, issues with capital access may drag down private-sector development efforts and, as discussed in a later section, make competing with China in the AI sphere challenging.[83]

---

74 Ibid.

75 Ibid.

76 "Russia: Surveillance Cameras by Major City 2019," Statista, accessed May 29, 2020, https://www.statista.com/statistics/1040717/surveillance-cameras-moscow-st-petersburg/.

77 Light, "Russia Is Building One of the World's Largest Facial Recognition Surveillance Networks."

78 Ibid.

79 Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 9.

80 Samuel Bendett, "The Development of Artificial Intelligence in Russia," in AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives, ed. Nicholas Wright, Strategic Multilayer Assessment (SMA) Periodic Publication (Department of Defense, 2018), 161–64.

81 Light, "Russia Is Building One of the World's Largest Facial Recognition Surveillance Networks."

82 Bendett, "The Development of Artificial Intelligence in Russia," 163.

83 Ibid., 163.

Other Sino-Russian Digital Connections: ICT, Mobile Devices, and 5G

Despite Russia's burgeoning success in AI and software development, China remains one of the country's largest ICT and networked device suppliers. In the mid-2010s, Russian customers began replacing American company Cisco Systems products with equipment from China's ZTE and Huawei.[84] Today Western sanctions prevent Russia from importing U.S. and EU technology—a boon for Huawei.[85] To comply with the 2016 Yarovaya Amendments, Russian telecommunications companies, such as Bulat, have looked to Huawei for data storage solutions. Most recently, Rostelecom is in talks with Huawei to supply 360,000 tablets running Russia's native Aurora operating system for use in the country's 2020 census.[86]

Beyond government, Huawei has aggressively marketed its smartphones—particularly its "Honor" brand value devices—to Russian consumers. This strategy is paying dividends. As of 2019, the Chinese company controlled 37 percent of Russia's smartphone market. This represents a marked increase from 13 percent market share two years earlier.[87] As part of a Russian government pilot program, Aurora may eventually be pre-installed on Huawei smartphones sold in the country.[88] The use of a native operating system would complement a December 2019 law, requiring all smart devices sold in Russia come preinstalled with Russian applications.[89]

Russia dpends substantially, although not solely, on Chinese infrastructure for its fifth-generation (5G) wireless networks. National security concerns may partially drive Russian efforts to diversify 5G suppliers. During the 2018 FIFA World Cup, Moscow piloted 5G for the first time, with Russia's second-largest mobile phone operator MegaFon using equipment from Finland's Nokia.[90] Aiming for full commercial 5G use by 2022, Moscow's city government lets operators select their own 5G suppliers. While MTS signed with Huawei, Tele2 chose Sweden's Ericsson.[91] MegaFon also eventually selected Ericsson for 5G "mobile transport solutions" nationwide.[92] In the future, state-owned Rostec may supply domestically produced 5G equipment to MegaFon and Rostelecom.[93] Experts suggest, however, that Huawei and ZTE will remain top picks for additional 5G infrastructure upgrades.[94] To gain a greater foothold in Russia, Huawei has already provided free 5G-related training to Russian technicians and plans to reach more than 10,000 trainees over the next half-decade.[95] Beyond profit, the partnership pays off

---

[84] Gabuev, "Digital Bromance."

[85] Michael Reilly, "Russia Turns to China for Help Building Its Own 'Great Firewall' of Censorship," MIT Technology Review, November 29, 2016, https://www.technologyreview.com/2016/11/29/155746/russia-turns-to-china-for-help-building-its-own-great-firewall-of-censorship/; Soldatov and Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact."

[86] Nadezhda Tsydenova and Anna Rzhevkina, "Huawei in Talks to Install Russian Operating System on Tablets for Country's Population Census—Sources," *Reuters*, August 26, 2019, https://uk.reuters.com/article/uk-huawei-russia-partnership-idUKKCN1VG1VJ.

[87] Doffman, "Huawei Soars in Russia as Putin Engages in New 'Technological War.'"

[88] Zak Doffman, "Huawei Just Launched 5G in Russia with Putin's Support: 'Hello Splinternet,'" *Forbes*, September 1, 2019, https://www.forbes.com/sites/zakdoffman/2019/09/01/hello-splinternet-huawei-deploys-5g-in-russia-with-putins-support/#71cb4fc5199d.

[89] Newman, "Russia Takes a Big Step Toward Internet Isolation."

[90] Doffman, "Huawei Just Launched 5G in Russia with Putin's Support: 'Hello Splinternet.'"

[91] Ibid.

[92] Juan Pedro Tomás, "Ericsson to Deploy Transport Network for Russian Carrier MegaFon," *RCR Wireless News* (blog), September 5, 2019, https://www.rcrwireless.com/20190905/5g/ericsson-deploy-transport-network-russian-carrier-megafon.

[93] Juan Pedro Tomás, "Russian State Firm Rostec to Develop 5G Equipment," RCR Wireless News (blog), July 25, 2019, https://www.rcrwireless.com/20190725/5g/russian-state-firm-rostec-develop-5g-equipment.

[94] Alexander Gabuev, "The Pandemic Could Tighten China's Grip on Eurasia," Carnegie Moscow Center, April 24, 2020, https://carnegie.ru/2020/04/24/pandemic-could-tighten-china-s-grip-on-eurasia-pub-81635.

[95] Doffman, "Huawei Just Launched 5G in Russia with Putin's Support: 'Hello Splinternet.'"

for Huawei as well. Placed on the U.S. Department of Commerce's blacklist, the company is leveraging Russia's manufacturing base and Russian demand to compensate for losses in U.S. business. For many ICT products, Russia lacks a domestic substitute to compete with Huawei. [96]

Looking Ahead: Double Diffusion? Or Policy as a Product of Circumstance?

While far from exhaustive, this section has shown how Russia increasingly imports elements of China's digital control policy and Chinese surveillance and ICT products. Lacking China's technical acumen and early start in Internet filtering, Roskomnadzor often struggles to implement borrowed measures. As Russia's regulatory and technical capacity improves, however, greater policy convergence will occur. As a result, in the future diffusion may change in two ways. It could become (1) less one-sided, with China learning from Russian efforts, and (2) more difficult to discern. Are governments copying one another or are their policies similar because the regimes face analogous threats and have comparable levels of technical know-how? Some evidence suggests this "double diffusion" is already occurring. A Chinese draft law on cybersecurity featured provisions that closely mirrored the Federation Council's 2014 legislation.[97] Beijing has become increasingly concerned with keeping its traffic and data about its citizens within Chinese borders. These priorities resonate with Russia's data localization and domestic internet policies.[98]

Competing and Complementary Markets: Russian and Chinese Digital Control Exports in Central Asia

While Russia primarily imports Chinese digital policy and devices, the Kremlin seeks to compete with Beijing in exporting measures and technologies in its traditional sphere of influence: Central Asia.[99] These countries make ideal customers. Like Russia and China, they feature authoritarian (in the case of Kyrgyzstan, hybrid) governments that face Internet-enabled threats to regime survival.[100] Lacking a fully developed domestic tech industry, however, they must import technologies to mitigate these risks.[101] These states' financial, technical, and organizational capacities, their specific technology needs, and their relations with exporting countries determine what products and policies they import and which supplier makes the proverbial sale.[102]

---

[96] Doffman, "Huawei Soars in Russia as Putin Engages in New 'Technological War.'"

[97] Gabuev, "The Pandemic Could Tighten China's Grip on Eurasia."

[98] Dennis Broeders, Liisi Adamson, and Rogier Creemers, "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace" (The Hague Program for Cyber Norms Policy Brief, November 2019), 10; Kieron O'Hara and Wendy Hall, "Four Internets: The Geopolitics of Digital Governance" (Centre for International Governance Innovation, December 2018), 9.

[99] Morgus, "The Spread of Russia's Digital Authoritarianism," 90.

[100] Jaclyn Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," International Journal of Communication 12 (2018): 3818.

[101] Weber, "The Worldwide Web of Chinese and Russian Information Controls," 14.

[102] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region."

In Central Asia, the diffusion of digital controls occurs in two primary ways. States (1) collaborate (freely or under pressure) with the supplier to develop policy and procure equipment and (2) simply copy other states (what the literature calls "uncoordinated diffusion").[103] As this section will show, Chinese diffusion typically spreads through the former "coordinated" approach; Beijing uses state agency trips, state-owned companies, and private companies (in which the Party still plays a role) to actively promote policy and tech.[104] The Chinese government has conducted "training" in all five Central Asian states.[105] Russia historically has relied more on the latter "uncoordinated" method, with Central Asian states copying digital control laws from former Soviet security service colleagues.

For Russia and China, the stakes are high and the competition is fierce. The exporter of choice nets not only financial gains but also political and norm-setting clout as well as potentially valuable intelligence assets.[106] While CIS members account for a quarter of Russia's surveillance control exports, 82 percent of China's foreign sales go to Belt and Road Initiative (BRI) countries through the Digital Silk Road project.[107] [108] Through the BRI, China has made significant inroads into Russia's customary "sphere of influence." Although Moscow's tools are typically lower cost and require less in the way of existing technical infrastructure, China's high-tech offerings (perfected at home prior to export) meet these regimes' desire for greater control.[109] Although the two countries compete in certain areas, both have clear niches. Russia, for instance, is best suited to provide information influence platforms and techniques and more traditional and low-cost telecommunications surveillance.[110] The following sections discuss in detail Central Asian imports of specific Russian and Chinese digital control policies and technologies.

Surveillance, Filtering, and Digital Censorship Laws: A Russian Export

In the 2000s and early 2010s, Central Asian states adopted aspects of Russia's digital doctrine and legal mechanisms for handling Internet control.[111] To ground this framework, CIS countries began by emulating Russia's 2000 Doctrine of Information Security, including its concept of a "national information space" and Russian terms like "information security."[112] A shared Soviet history and regime structure likely accounts for this diffusion. The overlap in conceptualizing information stems from a common "cultural and historical perspective on the risks . . . from free flows of information."[113] Regional KGB branches morphed into the security and intelligence services of newly independent Central Asian states. With similar infrastructure and policies in place

---

[103] Ibid., 3817.

[104] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 73.

[105] Weber, "The Worldwide Web of Chinese and Russian Information Controls," 41.

[106] Ibid., 26.

[107] Broeders, Adamson, and Creemers, "A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace," 6.

[108] Weber, "The Worldwide Web of Chinese and Russian Information Controls," 20.

[109] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 74; Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 1.

[110] Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 2.

[111] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3821.

[112] Ibid.

[113] Ibid., 3823.

from the Soviet era, their leaders modeled their new countries' surveillance frameworks on Russia's policies.[114] For regimes in Russia, Kazakhstan, and Kyrgyzstan, justifying digital control policies with law served to legitimize unpopular and illiberal measures—especially in the 2000s. The emphasis on rule of law is perhaps a vestige of efforts to appear democratic and also contributes to the diffusion of legal frameworks.[115]

Nine former Soviet states have emulated Russia's telecommunications surveillance approach. In Central Asia, **Kazakhstan**, **Uzbekistan**, **Kyrgyzstan**, **Tajikistan**, and **Turkmenistan** all either have SORM-based systems or similar programs.[116] While there are technical differences, the states use nearly identical protocols and policies. Kazakhstan and Uzbekistan have similar laws.[117] In 2012, Kyrgyzstan's national security committee passed almost an exact copy of Russia's intersection laws.[118] Less developed, Tajikistan's system can intercept landlines, while Turkmenistan's collects mobile phone data.[119] Similar to Russia's data localization law, Kazakhstan and Uzbekistan also have policies requiring the domestic storage of their citizens' personal data.[120]

Legal overlap is also clear in measures that enable filtering and encourage self-censorship. Russia, Uzbekistan, Kazakhstan, and Tajikistan all have laws, decrees, and orders that permit targeted censorship in the name of protecting "moral values, public order, national security, state secrets, and other privileged data."[121] Kyrgyzstan's Program for Information Security is purposefully vague, potentially allowing regulators to apply its stipulations to Internet content.[122] Kazakhstan and Uzbekistan have copied Russia's mass media registration law, which allows the government to hold certain sites, usually social media platforms and blogs, to a higher regulatory standard.[123] Like Russia (and China), Tajikistan and Kazakhstan expand blocking and content removal efforts during national events, such as elections.[124] These examples are by no means exhaustive, but they illustrate the extent to which Russian-style filtering, censorship, and lawful interception frameworks have diffused in the region.

Niche Markets in Surveillance and Filtering Technologies and Programs

Moscow and Beijing have carved out distinct markets in surveillance and filtering technology. While Chinese companies supply most of the technology for photo and video surveillance, Russia has dominated regional exports of traditional telecommunications surveillance technology.

---

[114] Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

[115] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3828.

[116] Ibid., 3822.

[117] Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

[118] Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 10; Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

[119] Kerr, "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region," 3823.

[120] In 2016, Kazakhstan amended a 2013 law to require data localization, permitting the external storage of copies of data with "adequate" protection measures. As of 2020, Uzbekistan has tried to force companies, including Facebook, Google, and Yandex, to store personal data within Uzbek territory. For more, see Cian Skyker's working paper in this volume.

[121] Kerr, 3820.

[122] Ibid., 3824.

[123] Ibid., 3821.

[124] Ibid., 3924; "Freedom on the Net 2019: Kazakhstan," Freedom House, 2019, https://freedomhouse.org/country/kazakhstan/freedom-net/2019.

As Central Asia's regimes copied Russia's lawful interception laws, ISPs in these countries purchased Russian-produced SORM-compliant systems.[125] Founded by Russian citizens, Protei and Peter-Service are two of the best-known SORM suppliers.[126] This Russian equipment is cost-effective; Russian systems sold for a third of the price of comparable devices produced by an Israeli competitor.[127] The difference in price and shared cultural connections may account for Russian firms' edge in SORM tech.

Kazakhstan, Kyrgyzstan, and Uzbekistan have all imported SORM equipment from Russian companies. **Kazakhstan's** replica of SORM enables DPI for surveillance and filtering.[128] The government purchased DPI technology from VAS Experts and SORM technology from MFI-SOFT and Protei. It procured additional monitoring tools from iTecho and mobile forensics software from Speech Technology Center and Oxygen Software respectively—all Russian companies.[129] **Uzbekistan** originally imported DPI equipment from VAS Experts and Protei- and SORM-compliant systems from MFI-Soft. Like Kazakhstan, it sourced additional tools from Speech Technology Center and Oxygen Software.[130] **Kyrgyzstan** bought SORM equipment from Protei, Moscow's Oniks-Line, and Novosibirsk's Signatek.[131] The latter two companies have faced accusations of maintaining a backdoor in their equipment. While Russian firms have historically dominated exports in this area, a 2018 report finds that Chinese companies updated aging Russian-produced SORM systems in Kazakhstan and Uzbekistan.[132] Beijing may see an opportunity to capture a traditionally Russian market.

Chinese companies already monopolize technology exports for a newer form of surveillance: CCTV systems equipped with FRT. Uzbekistan, Tajikistan, Kazakhstan, and Kyrgyzstan join Russia in emulating aspects of China's Safe Cities Projects. China's CITIC Group and COSTAR Group are partnering with **Uzbekistan's** Information Technology Development Ministry to implement a Safe Cities program with Huawei technology. As part of these efforts, the government closed a US$1 billion contract with Huawei that includes updates to more than 880 cameras in Tashkent.[133] In 2013, **Tajikistan's** government paid Huawei US$22 million to establish a Safe City program in Dushanbe. Announced upgrades will integrate FRT into cameras at airports, shopping centers, and other public spaces.[134]

In their Safe Cities programs, Kazakhstan and Kyrgyzstan depend less on China than their neighbors do. With 2000 cameras in Nur-Sultan alone, Sergek**, Kazakhstan's** version of Safe City, relies on domestic IT companies to run the program, which uses equipment from China's Dahua Technology.[135] Kazakhstan's President Kassym-Jomart Tokayev has praised China's surveillance system and reportedly visited Hikvision, a company on the U.S. blacklist for abuses in Xinjiang.[136] After a deal with Huawei fell through, **Kyrgyzstan** contracted Russia's Vega to

---

[125] Morgus, "The Spread of Russia's Digital Authoritarianism," 89.

[126] Ibid., 89.

[127] Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

[128] Polyakova and Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," 10.

[129] Weber, "The Worldwide Web of Chinese and Russian Information Controls," 20.

[130] Ibid., 21.

[131] Morgus, "The Spread of Russia's Digital Authoritarianism," 89; Weber, "The Worldwide Web of Chinese and Russian Information Controls," 20.

[132] Weber, "Understanding the Global Ramifications of China's Information Controls Model," 73.

[133] Yan, "Smart Cities or Surveillance?"

[134] Ibid.

[135] Ibid.; Chris Rickleton, "Kazakhstan Embraces Facial Recognition, Civil Society Recoils," Euraisanet, October 2019, https://eurasianet.org/kazakhstan-embraces-facial-recognition-civil-society-recoils.

[136] Rickleton, "Kazakhstan Embraces Facial Recognition, Civil Society Recoils."

implement its Safe Cities project for US$34 million. Vega hardware, however, operates on software developed by China's National Electronics and Export Corporation (CEIEC). Additionally, since the Vega deal, Kyrgyzstan has hired CEIEC to install additional separate cameras and build a command center.[137] CEIEC, which also produces technology used in Xinjiang, has apparently provided surveillance products to Kyrgyzstan free of charge.[138]

Chinese Domination in 5G and ICT[139]

Chinese companies dominate telecommunications contracts with governments and mobile providers in Uzbekistan, Kazakhstan, Tajikistan, and Kyrgyzstan. Huawei has a longstanding relationship with Tashkent. In 2008, the company updated the country's telecommunications network. It later incorporated 5G service into state-affiliated Uzmobile and Ucell. In Kazakhstan, Huawei supports Kazakhtelecom, Kcell, Beeline, and Tele2, while in Kyrgyzstan, it produces roughly 90 percent of technology for Sky Mobile and 70 percent for Alfa Telecom.[140] Before it withdrew from the market, Tajik telecom operator TK Mobile had majority ZTE ownership.[141]

Conclusion: Challenging Conventional Wisdom

With niche exports markets, selective policy and technology diffusion, and significant differences in regulatory capacity, it is an understatement to say that Sino-Russian digital relations are more nuanced than commonly assumed. The analysis in this white paper helps dispel two common myths about Internet controls in the region.

Myth 1: Russia's digital control regime will soon mirror China's in character and scope.

News reports about Huawei 5G in Moscow or Russia's splinternet often oversimplify the matter, frequently suggesting that Russia copies Chinese policy and imports Chinese technology wholesale. Alarmist in tone, these pieces imply that Russia will soon possess surveillance and filtering systems that rival China's own programs.

The reality is more complicated. The Kremlin has undoubtedly sought to strengthen its control over the RuNet and looked to China for guidance. The nature and extent of these efforts, however, require qualification. As this working paper shows, Russia has *selectively adopted Chinese-style controls* and is *partially dependent on Chinese technology exports*. Furthermore, Roskomnadzor's trailing technical capacity hampers their full implementation. There is no indication that the agency will overcome these deficiencies, at least in the medium-term.

[137] Bermet Zhumakadyr Kyzy, "Right to Privacy in Kyrgyzstan," *EUCAM* (blog), January 21, 2020, https://eucentralasia.eu/2020/01/right-to-privacy-in-kyrgyzstan/.

[138] Yan, "Smart Cities or Surveillance?"; Yau Tsz Yan, "China Taking Big Brother to Central Asia," *Eurasianet*, September 6, 2019, https://eurasianet.org/china-taking-big-brother-to-central-asia.

[139] For more on this topic, see Cian Stryker'chapter in this volume.

[140] Yan, "Smart Cities or Surveillance?"

[141] "TK Mobile Withdraw from Country's Telecommunications Market," April 11, 2018, https://asiaplustj.info/en/news/tajikistan/economic/20180411/tk-mobile-withdraw-from-countrys-telecommunications-market.

Russia's COVID-19 pandemic prompted a wave of proposals for expanded digital surveillance measures, such as geotracking.[142] As critics have pointed out, tracking the spread of the virus provides convenient cover for implementing new monitoring systems, while existing programs will likely get additional Chinese-style upgrades.[143] Without improved human and technological know-how, however, these updates are unlikely to be fully effective, both at stopping COVID and keeping tabs on citizens.

Myth 2: China enjoys a monopoly on Central Asia's digital controls market.

Popular belief holds that, through its Belt and Road Initiative, Chinese policy tools and devices dominate digital control regimes in Central Asia. The wide-scale adoption of Chinese surveillance camera technology and programs does diminish Russia's influence in this realm. The Kremlin, however, has managed to maintain its niches. A common history and desire to claim democratic legitimacy continue to encourage legal diffusion; Central Asian states have drawn on Russia's lawful interception and information security frameworks. For Central Asia's authoritarian regimes, facial recognition video surveillance and SORM-style telecommunications interception meet different control needs. As long as Russia maintains its market in updating SORM-like systems, the Kremlin will retain a degree of clout in the region.

Bibliography

Adee, Sally. "The Global Internet Is Disintegrating. What Comes Next?" BBC, May 14, 2019. https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

Arthur, Charles. "China Cracks down on VPN Use." the Guardian, May 13, 2011. http://www.theguardian.com/technology/2011/may/13/china-cracks-down-on-vpn-use.

Bendett, Samuel. "The Development of Artificial Intelligence in Russia." In *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas Wright, 161–69. Strategic Multilayer Assessment (SMA) Periodic Publication. Department of Defense, 2018.

Hikvision. "Bezopasnyi Gorod Moskva Sozdaetsia Vmeste s Hikvision i Safe Logic [Together Hikvision and Safe Logic Create Safe City Moscow]." Accessed May 17, 2020. https://hikvision.ru/success/city.

Brizgalova, Yekaterina. "Roskomnadzor reshil poka ne blokirovatăVPN-servisy [Roskomnadzor decided not to block VPN-services for now]." Vedomosti, June 26, 2019. https://www.vedomosti.ru/technology/articles/2019/06/26/805110-roskomnadzor.

Broeders, Dennis, Liisi Adamson, and Rogier Creemers. "A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace." The Hague Program for Cyber Norms Policy Brief, November 2019.

---

[142] Peter Mironenko, "Kak vlasti otsledyat zabolevshih po smartfonam…" [How the authorities will track the infected using smartphones . . .], *The Bell* (blog), March 23, 2020, https://thebell.io/kak-vlasti-otsledyat-zabolevshih-po-smartfonam-bespoleznaya-atomnaya-bomba-frs-i-sovety-po-udalenke/.

[143] Gabuev, "The Pandemic Could Tighten China's Grip on Eurasia."

Browne, Ryan. “Russia Follows China in Tightening Internet Restrictions, Raising Fresh Censorship Concerns.” CNBC, July 31, 2017. https://www.cnbc.com/2017/07/31/russia-follows-china-in-vpn-clampdown-raising-censorship-concerns.html.

Human Rights Watch. “China’s Algorithms of Repression | Reverse Engineering a Xinjiang Police Mass Surveillance App,” May 1, 2019. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.

Creemers, Rogier. “The International and Foreign Policy Impact of China’s AI and Big Data Strategies.” In *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas Wright, 112–27. Strategic Multilayer Assessment (SMA) Periodic Publication. Department of Defense, 2018.

Doffman, Zak. “Huawei Just Launched 5G In Russia With Putin’s Support: ‘Hello Splinternet.’” Forbes, September 1, 2019. https://www.forbes.com/sites/zakdoffman/2019/09/01/hello-splinternet-huawei-deploys-5g-in-russia-with-putins-support/#71cb4fc5199d.

———. “Huawei Soars In Russia As Putin Engages In New ‘Technological War.’” Forbes, November 3, 2019. https://www.forbes.com/sites/zakdoffman/2019/11/03/huawei-soars-in-russia-as-putin-engages-in-new-technological-war/#39c8782765ca.

“‘Draconian’ Russian Net Law Enacted.” *BBC*, August 1, 2014, sec. Technology. https://www.bbc.com/news/technology-28583669.

Epifanova, Alena. “Deciphering Russia’s ‘Sovereign Internet Law.’” DGAP Analysis: German Council on Foreign Relations, January 2020. https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf.

Federalʹnyi zakon “O vnesenii izmenenii v Federalʹnyi zakon “O sviazi” i Federalʹnyĭzakon “Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii” [Federal law “On Amendments to the Federal Law ‘On Communications’ and the Federal Law ‘On Information, Information Technologies, and Information Protection’”], Pub. L. No. 90- FZ (2019). http://publication.pravo.gov.ru/Document/View/0001201905010025.

FederalʹnyĭZakon “Ob operativno-rozysknoĭdeiatelʹnosti” [Federal law on operational and investigative activities], Pub. L. No. N 144-ф3 (1995). http://www.libertarium.ru/l_sormlaw_101.

Gabuev, Alexander. “Digital Bromance: The Sino-Russian Partnership Racing Ahead.” Carnegie Moscow Center, December 7, 2015. https://carnegie.ru/2015/12/07/digital-bromance-sino-russian-partnership-racing-ahead-pub-62253.

———. “The Pandemic Could Tighten China’s Grip on Eurasia.” Carnegie Moscow Center, April 24, 2020. https://carnegie.ru/2020/04/24/pandemic-could-tighten-china-s-grip-on-eurasia-pub-81635.

“Interim Provisions Governing The Management Of The Computer Information Networks In The People’s Republic Of China Connecting To The International Network.” Accessed November 15, 2020. http://www.asianlii.org/cn/legis/cen/laws/ipgtmotcinitproccttin1488/.

Kerr, Jaclyn. "Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region." *International Journal of Communication* 12 (2018): 3814–34.

Korzak, Elaine. "The Next Level For Russia-China Cyberspace Cooperation?" Council on Foreign Relations. *Net Politics* (blog), August 20, 2015. https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation.

Kyzy, Bermet Zhumakadyr. "Right to Privacy in Kyrgyzstan." *EUCAM* (blog), January 21, 2020. https://eucentralasia.eu/2020/01/right-to-privacy-in-kyrgyzstan/.

Light, Felix. "Russia Is Building One of the World's Largest Facial Recognition Surveillance Networks." The Moscow Times, November 12, 2019. https://www.themoscowtimes.com/2019/11/12/russia-building-one-of-worlds-largest-facial-recognition-networks-a68139.

Lucas, Louise, and Emily Feng. "Inside China's Surveillance State," July 20, 2018. https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543.

Morgus, Robert. "The Spread of Russia's Digital Authoritarianism." In *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas Wright, 85–93. Strategic Multilayer Assessment (SMA) Periodic Publication. Department of Defense, 2018.

Newman, Lily Hay. "Russia Takes a Big Step Toward Internet Isolation." *Wired*. Accessed May 10, 2020. https://www.wired.com/story/russia-internet-control-disconnect-censorship/.

RIA News. "Novye pravila identifikatsii v messendzherakh vstupili v silu," 20190505T1314. https://ria.ru/20190505/1553268769.html.

O vnesenii izmenenii v Federalnyi zakon «O protivodeistvii terrorizmu» i otdelnye zakonodatelnye akty Rossiiskoi Federatsii v chasti ustanovleniia dopolnitelnykh mer protivodeistviia terrorizmu i obespecheniia obshchestvennoi bezopasnosti [On Amendments to the Federal Law 'On Combating Terrorism' and Separate Legislative Acts of the Russian Federation to establish additional measures to counter terrorism and ensure public safety], Pub. L. No. 374- FZ (2016). http://www.kremlin.ru/acts/bank/41108/page/1.

O vnesenii izmenenii v Federalnyi zakon "O sviazi" [Changes to the federal law "on communications"], Pub. L. No. N 245-ФЗ (2017). http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284289&fld=134&dst=1000000001,0&rnd=0.10568643889263796%20%20#044800986310585156.

O vnesenii izmenenii v otdelnye zakonodatelnye akty Rossiiskoi Federatsiii v chasti utochneniia poriadka obrabotki personalnykh dannykh v informatsionno-telekommunikatsionnykh setiakh [Amendments to specific Russian Federation laws to clarify the processing of personal data on information-telecommunications networks], Pub. L. No. N 152-ФЗ (2014). http://pravo.gov.ru/proxy/ips/?docbody=&nd=102355893.

"Obzor Dokumenta: O Vnesenii Izmenenii v Federalnyi Zakon Ob Informatsii, Informatsionnykh Tekhnologiiakh i o Zashchite Informatsii i Otdelnye Zakonodatelnye Akty Rossiiskoi Federatsii Po Voprosam Uporiadocheniia Obmena Informatsiei s Ispolzovaniem Informatsionno-Telekommunikatsionnykh Setei [Summary of the Document: Amendments to the Federal Law 'On

Information, Information Technologies and about Information Protection' and Certain Legislative Acts of the Russian Federation on Streamlining the Exchange of Information Using Information and Telecommunication Networks"]," August 8, 2014. http://www.garant.ru/hotlaw/federal/558201/.

O'Hara, Kieron, and Wendy Hall. "Four Internets: The Geopolitics of Digital Governance." Centre for International Governance Innovation, December 2018.

Polovinko, Vyacheslav, and Lilit Sarkisyan. "Teperăoni prishli za VPN [Now they're come for our VPNs]." Novaya Gazeta, March 28, 2019. https://www.novayagazeta.ru/articles/2019/03/28/80032-teper-oni-prishli-za-vpn.

Polyakova, Alina, and Chris Meserole. "Exporting Digital Authoritarianism: The Russian and Chinese Models." The Brookings Institution: Foreign Policy Program, August 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Propaganda netraditsionnykh seksualăynykh otnoshenii sredi nesovershennoletnikh [Propaganda on non-traditional sexual orienation aimed at minors], Pub. L. No. N 195-Ф3, Article 6.21 The Russian Federation's Code of Administrative Offenses (2013). http://www.consultant.ru/document/cons_doc_LAW_34661/f385ab5d34de901b2e5f3d08ac0b454481377d6a/.

Razumovskaya, Olga. "Putin Signs Bill Blocking Websites That Incite Rioting, Promote Extremism." *Wall Street Journal*, December 30, 2013, sec. World. http://www.wsj.com/articles/putin-signs-bill-blocking-websites-that-incite-rioting-promote-extremism-1388416128.

Reilly, Michael. "Russia Turns to China for Help Building Its Own 'Great Firewall' of Censorship." MIT Technology Review, November 29, 2016. https://www.technologyreview.com/2016/11/29/155746/russia-turns-to-china-for-help-building-its-own-great-firewall-of-censorship/.

Rickleton, Chris. "Kazakhstan Embraces Facial Recognition, Civil Society Recoils." Euraisanet, October 2019. https://eurasianet.org/kazakhstan-embraces-facial-recognition-civil-society-recoils.

BBC. "Russia Beefs up Anti-Piracy Laws," May 1, 2015. https://www.bbc.com/news/technology-32531275.

Human Rights Watch. "Russia: 'Big Brother' Law Harms Security, Rights," July 12, 2016. https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

Statista. "Russia: Surveillance Cameras by Major City 2019." Accessed May 29, 2020. https://www.statista.com/statistics/1040717/surveillance-cameras-moscow-st-petersburg/.

Sherman, Justin. "The Russian Doll of Putin's Internet Clampdown." *Wired*, May 1, 2020. https://www.wired.com/story/opinion-the-russian-doll-of-putins-internet-clampdown/.

"Soderzhanie zakona o SMI i blogerakh [Summary of the law on mass media and bloggers]," May 14, 2018. https://lawlinks.ru/zakon-o-blogerax/.

Soldatov, Andrei, and Irina Borogan. "In Ex-Soviet States, Russian Spy Tech Still Watches You." WIRED, 2012. https://www.wired.com/2012/12/russias-hand/.

———. “Putin Brings China’s Great Firewall to Russia in Cybersecurity Pact.” the Guardian, November 29, 2016. http://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.

“TK Mobile Withdraw from Country’s Telecommunications Market,” April 11, 2018. https://asiaplustj.info/en/news/tajikistan/economic/20180411/tk-mobile-withdraw-from-countrys-telecommunications-market.

Tomás, Juan Pedro. “Ericsson to Deploy Transport Network for Russian Carrier MegaFon.” *RCR Wireless News* (blog), September 5, 2019. https://www.rcrwireless.com/20190905/5g/ericsson-deploy-transport-network-russian-carrier-megafon.

———. “Russian State Firm Rostec to Develop 5G Equipment.” *RCR Wireless News* (blog), July 25, 2019. https://www.rcrwireless.com/20190725/5g/russian-state-firm-rostec-develop-5g-equipment.

Toombs, Zach. “China’s Censors Take on Virtual Private Networks.” The Diplomat, November 6, 2014. https://thediplomat.com/2014/11/chinas-censors-take-on-virtual-private-networks/.

Tsydenova, Nadezhda, and Anna Rzhevkina. “Huawei in Talks to Install Russian Operating System on Tablets for Country’s Population Census - Sources.” *Reuters*, August 26, 2019. https://uk.reuters.com/article/uk-huawei-russia-partnership-idUKKCN1VG1VJ.

Weber, Valentin. “The Sinicization of Russia’s Cyber Sovereignty Model.” Council on Foreign Relations. *Net Politics* (blog), April 1, 2020. https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model.

———. “The Worldwide Web of Chinese and Russian Information Controls.” The Open Technology Fund, September 2019.

———. “Understanding the Global Ramifications of China’s Information Controls Model.” In *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Nicholas Wright, 72–75. Strategic Multilayer Assessment (SMA) Periodic Publication. Department of Defense, 2018.

———. “Why China’s Internet Censorship Model Will Prevail Over Russia’s.” *Net Politics* (blog), December 12, 2017. https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.

Yan, Yau Tsz. “China Taking Big Brother to Central Asia.” Eurasianet, September 6, 2019. https://eurasianet.org/china-taking-big-brother-to-central-asia.

———. “Smart Cities or Surveillance? Huawei in Central Asia.” The Diplomat, August 7, 2019. https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/.

Beyond the GovTech: The Pitfalls of Kazakhstan's Digitalization Agenda

Anna Gussarova

The emergence of the Kazakhstan e-government has changed the relationship between the state and society. On the one hand, it contributed to fostering good governance and democratization, and, on the other hand, significantly contributed to massive data acquisition and digital surveillance by the state. In the case of Kazakhstan, transformation to digital society has encountered a few limitations and constraints.

"Digital Kazakhstan" in a nutshell

The first Public Service Centers and the e-gov portal (eGov.kz) were established in 2005–2007,[1] aiming at improving the quality of public services and reducing pervasive corruption. The Kazakh government envisions digitalization exclusively as automation of as many public services as possible (335[2] as of July 2020). Larger GovTech initiatives, such as e-gov, have become quite widespread, as governments tend to increase the efficiency of their operations by digitizing work processes and bringing new tools. Indeed, the Kazakh e-gov project has helped the state to reduce waiting time, introduce easier procedures, and bring benefits to citizens.

Still, to maximize efforts to achieve this goal, having a technological solution is just one side of the coin. The other—which is missing—is about shaping digitalization culture, promoting cyber hygiene and digital literacy among its citizens to promote democratization and a digitalization agenda. As a result, without a strategic vision and a secure-by-design and secure-by-default approach, the Kazakh digitalization efforts have become exposed to frequent vulnerabilities emanating from state and nonstate actors (from data breaches to sophisticated cyber-attacks).[3]

---

[1] "Digital Kazakhstan" State Program", accessed March 18, 2021, https://zerde.gov.kz/en/activity/program-control/digital-kazakhstan.

[2] "Elektronnoe pravitelʹstvo Kazakhstana v tsifrovuiu epokhu" [Electronic government of Kazakhstan in the digital age], *Profit.kz,* July 10, 2020, accessed March 18, 2021, https://profit.kz/articles/14612/Elektronnoe-pravitelstvo-Kazahstana-v-cifrovuu-epohu.

[3] Catalin Cimpanu, "Extensive Hacking Operation Discovered in Kazakhstan," *ZDNet*, November 23, 2019, https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan; Victoria Kelly-Clark, "Central Asia: The Land of CyberCrime?" *Global Risk Insights.* April 29, 2019, https://globalriskinsights.com/2019/04/central-asia-cybercrime-land; Almaz Kumenov, "Hackers Eyeing Kazakhstan as a Safe Haven," Eurasianet.org, November 27, 2018, https://eurasianet.org/hackers-eyeing-kazakhstan-as-a-safe-haven.

In 2017 the government introduced "Digital Kazakhstan,"[4] a national digitalization plan until 2020 and a blueprint of the Singaporean Smart Nation initiative.[5] The Kazakh version outlines four key areas of the long-term objectives to transform:

Economy. The transformation of traditional sectors of economy using breakthrough technologies and opportunities should increase labor productivity and lead to an increase in capitalization.

State. Digital state should provide services to the population and businesses, anticipating their needs, including electronic services.

Infrastructure. Digital Silk Road should provide high-speed and secure infrastructure for transmission, storage, and processing of data.

Human capital. The development of human capital should lead to the so-called creative society to ensure the transition to the knowledge economy.

Yet digitalization comes with certain pitfalls, which include the prevailing role of the state, over-emphasis on information and communication technologies, and the need for quick quantitative results (e.g., the UN global e-government development index and Smart City ranking) and benefits (e.g., jobs). Additionally, the capacity of Kazakhstan in achieving its strategic goals of digitalization is constrained and contingent on foreign assistance and support in technology, investment, and skills. On the one hand, the over-emphasis on information and communication can lead to a quicker digital transformation, desired and formulated in the state development agenda. On the other hand, the focus on a more aggressive, non-transparent and rapid approach to digitalization of civil services leaves behind knowledge and culture in understanding the long-term benefits and side effects for the people, their freedoms and trust in government.

The far-reaching implications of finding rapid solutions in seeking technologies to deliver modernization agenda have resulted in choosing the Russian and Chinese soft- and hardware as well as having a robust regulatory experience to deal with data protection and surveillance, discounting the EU and U.S. investments and knowledge and privacy versus security practices. Furthermore, in a country with a super-strong state position in economic and political systems there is no capacity in bringing public–private partnerships (PPPs) to share the burden and invest in cyber security and welfare.

When it comes to soft connectivity, significantly less attention is paid to e-education and e-healthcare. Despite some positive changes, the level of computer and digital literacy remains critically low. According to the OECD's Programme for the International Assessment of Adult Competencies survey results,[6] "adults in Kazakhstan perform below the OECD average in literacy and numeracy," while the 2018 International Computer and

---

[4] "Gosudarstvennaia programma «Tsifrovoi Kazakhstan» na 2017-2020 goda" [State Program "Digital Kazakhstan" for 2017-2020], accessed March 18, 2021, https://zerde.gov.kz/images/%D0%93%D0%9F%20%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9%20%D0%9A%D0%B0%D0%B7%D0%B0%D1%85%D1%81%D1%82%D0%B0%D0%BD%20%D0%BD%D0%B0%202017-2020%20%D0%B3%D0%BE%D0%B4%D1%8B.pdf; "Poslanie Prezidenta Kazakhstana «Tretia modernizatsiia Kazakhstana: globalnaia konkurentosposobnost'" [Address of the President of Kazakhstan "Third modernization of Kazakhstan: global competitiveness], accessed March 18, 2021, https://online.zakon.kz/document/?doc_id=35676318

[5] Smart Nation Singapore,"Pillars of Smart Nation," February 1, 2021, accessed March 18, 2021. https://www.smartnation.gov.sg/why-SmartNation/pillars-of-smart-nation.

[6] OECD PIAAC. Kazakhstan. Country Note, accessed March 18, 2021, https://www.oecd.org/skills/piaac/publications/countryspecificmaterial/PIAAC_Country_Note_Kazakhstan.pdf.

Information Literacy Study[7] concluded that "33 percent of Kazakhstani eighth grade students have not reached the minimum level of computer and information literacy." This report also reveals the problem of inequality of education, depending on the type of school, language of instruction, and location (urban versus rural). Location is even more important in terms of Internet penetration, its speed, and access to laptops to proceed with online education in the times of COVID-19.[8] As a result, the digital divide remains one of numerous barriers to a widespread e-government, because many citizens and low-income families have no access to e-services.[9]

Digitalization-surveillance nexus

The topics of digital surveillance, data protection, and privacy concerns in Kazakh society have been on agenda since before the coronavirus outbreak. They have been driven and fuelled by human rights activists in response to increased cooperation with China since 2018, when the Kazakh government launched its national strategy "Digital Kazakhstan" and Smart City projects to reshape urban areas with the help of the ICT.[10] Moreover, in October 2019, after the state visit to China, President Kassym-Jomart Tokayev instructed his cabinet to adopt the Chinese experience of mass digitalization[11] in Kazakhstan.

Since that time, face recognition, biometrics, artificial intelligence, and video surveillance technologies have been rapidly emerging domestically in close cooperation with the companies from the EAEU area, including Russian and Belorussian, and several Chinese companies such as Hikvision and Dahua Technology (sanctioned by the United States for facilitating human rights violations against Muslim minorities in China). The latter is the key partner of local Korkem Telecom in building the Kazakh video surveillance capacity to decrease traffic accidents and criminal activities in five Kazakh major cities (widely known as Sergek).

Extrapolating these solutions to the size of the country will result in hundreds of thousands of cameras that should be installed by 2022 according to the Ministry of Interior's plan on crime prevention[12] on the one hand and introducing nationwide biometric identification[13] and collecting fingerprints in 2021 on the other. This will result in the biggest digitalization of the country's personal data that should be collected, processed, and safely stored on local servers with adequate anti-intrusion and leakage protection.

---

[7] "Kazakhstani Results in the ICILS-2018 International Computer and Information Literacy Study," accessed March 18, 2021, http://iac.kz/en/events/kazakhstani-results-icils-2018-international-computer-and-information-literacy-study.

[8] " Bolee 300 tys. detei ne imeiut kompǎuterov dlia distantsionnogo obucheniia v RK" [More than 300 thousand children do not have computers for remote learning in the RK], *Zona.kz*, March 31, 2020, https://zonakz.net/2020/03/31/bolee-300-tys-detej-ne-imeyut-kompyuterov-dlya-distancionnogo-obucheniya-v-rk/.

[9] Saltanat Janenova, "E-Government in Kazakhstan: Challenges For a Transitional Country," NISPAcee Conference, 2018, accessed September 1, 2020. https://www.nispa.org/files/conferences/2010/papers/201004220915450.janenovasaltanat.pdf.

[10] Anna Gussarova, "Kazakhstan Experiments With Surveillance Technology to Battle Coronavirus Pandemic." *Jamestown.org*, April 08, 2020, https://jamestown.org/program/kazakhstan-experiments-with-surveillance-technology-to-battle-coronavirus-pandemic/.

[11] Zhanbolat Mamyshev, " Tokaev poruchil pereniatǎu Kitaia opyt tsifrovizatsii grazhdan" [Tokayev instructed to borrow China's experience of digitalization of citizens], *Kursiv*, October 9, 2019. Accessed March 18, 2021. https://kursiv.kz/news/obschestvo/2019-10/tokaev-poruchil-perenyat-u-kitaya-opyt-cifrovizacii-grazhdan.

[12] LLP, Profit Online. " Vo dvorakh mnogoetazhek khotiat ustanovitǎkamery videonabliudeniiaa k 2022 godu" [There is an intention to set up CCTV cameras in the courtyards of multi-story buildings], *Profit.kz*, September 25, 2019, https://profit.kz/news/56690/Vo-dvorah-mnogoetazhek-hotyat-ustanovit-kameri-videonabludeniya-k-2022-godu/.

[13] Irina Sevostianova, "Kogda vsekh kazakhstantsev obiazhut sdavatǎotpechatki palǎsev" [When will all Kazakhstanis be obliged to get fingerprints], *Forbes.kz*, February 20, 2019, https://forbes.kz/process/vvedenie_daktiloskopicheskoy_registratsii_v_kazahstane_mogut_otlojit/.

When it comes to data protection, it remains unclear who has access to and controls the security of collection, processing, and storage of personal information. The situation backslides as it is not clear how and if state agencies, particularly security services, will respect the rights of citizens to protect personal data. In the context of the implementation of the National Video Monitoring System, the question is how the government will balance between the right to privacy and interference in it for the sake of maintaining public order and ensuring national security.[14]

Currently, the study on data protection in Kazakhstan by Gussarova and Dzhaksylykov argues that citizens are not motivated to protect their personal data because of the belief that "the state conducts digital surveillance and knows everything, thus there is nothing to hide."[15] Research findings also suggest that people who hide their personal data, including via VPN services, are afraid not of Internet companies, but rather state surveillance. For instance, the "security certificate" has received both criticism and support in the society. Some are outraged by the violation of the right to privacy; others are ready to sacrifice this right for the sake of national security.

Finally, it is essential to understand that application of national data protection legislation should consider basic human rights and adequately balance between confidentiality and freedom of information.[16] Access to the digital environment and its use are important pillars of the fundamental human rights and freedoms that Kazakhstan has agreed to follow.[17]

Repercussions of digitalization

One of the consequences of the chosen top-down digitalization strategy is inconsistency and lack of coordination among state agencies. While the goal of introducing advanced technologies in all aspects of public life remains genuine, different ministries and departments have different levels of digitalization and technological advance (security services have utilized their opportunities to increase surveillance capacity). President Tokayev has recently highlighted this problem, suggesting the establishment of a unified monitoring system that should combine all state bodies under "Smart Data Ukimet."[18]

Another important aspect associated with digital transformation in the Kazakh efforts is speed and time of introducing emerging technologies, particularly Big Data, Cloud, and AI. On the one hand, they remain of utmost importance for the public, industry and business, and government. On the other hand, most new technological solutions have been quickly implemented in the technology-friendly environment of big cities

[14] Trubacheva, Tatiana. "Bolăhoi Brat: Kak budet rabotatănatsionalăaia sistema videomonitoringa v Kazakhstane" [Big Brother: How will the national system of video surveillance work in Kazakhstan], *Forbes.kz*, February 20, 2020, https://forbes.kz/process/technologies/bolshoy_brat_po-kazahski_1582187734.

[15] Anna Gussarova and Serik Dzhaksylykov, "Zashchita personalăykh dannykh v Kazakhstane: status, riski i vozmozhnosti." Public Policy Initiative. Soros Foundation Kazakhstan. April 2020, https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf.

[16] Anna Gussarova, "Culture of Protecting Personal Data: From Online Freedom to Digital Surveillance?" *CABAR.asia*, April 15, 2020, https://cabar.asia/en/culture-of-protecting-personal-data-from-online-freedom-to-digital-surveillance/.

[17] "Guidelines to respect, protect and fulfil the rights of the child in the digital environment," Recommendation CM/Rec(2018)7 of the Committee of Ministers Council of Europe, September 2018: 13, accessed March 18, 2021, https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.

[18] "Glava Gosudarstva Provel Soveshchanie Po Realizatsii Gosudarstvennoi Programmy «Tsifrovoi Kazakhstan» 4 Marta 2020" [Head of the State conducted a meeting on the realization of the state program "Digital Kazakhstan" on 4 March 2020], *Akorda.kz*, https://www.akorda.kz/ru/events/akorda_news/meetings_and_sittings/glava-gosudarstva-provel-soveshchanie-po-realizacii-gosudarstvennoi-programmy-cifrovoi-kazahstan.

with infrastructure. As a result, this policy has significantly increased the digital and socioeconomic gap between the country's urban and rural areas and remote communities. Besides, massive digitalization has not resulted in a major economic breakthrough. The welfare of the Kazakhstanis remains relatively low, and the state is overburdened with consequences of its irresponsible economic policy, while digitalization cannot bring quick benefits and profit.

Kazakhstan certainly needs to make the Internet safer, considering the growing use of e-commerce and increasing digitization of citizens' personal information through the e-gov platform. Nonetheless, the large number of citizens who were penalized for their political activities indicates the priority of ensuring security over individual freedoms. Since recent restriction on the Internet and control of information flows have become common practice in Kazakhstan, the country remains one of the least free in the World Press Freedom Index with the 158th ranking.[19]

Furthermore, Internet blockings and censorship also target ex-president Nazarbayev's primary opponent, Mukhtar Ablyazov, whose political party, Democratic Choice of Kazakhstan (later changed to Street Party), is proscribed as extremist and banned.[20] Moreover, since 2018 the National Security Committee and the Interior and Defense ministries have been sanctioned to block the Internet during "emergencies of a social, natural or man-made nature".[21]

Regular disruption of communications and blocking efforts (of the Internet) associated with protests in the main cities of the country, full-scale implementation of the national cybersecurity program "Cyber Shield" and, as a result, strengthening of governance and control over the Internet (implementation of "electronic sovereignty" and a "security certificate"), and the development of local software for Internet security reinforces the importance of promoting the culture of personal data protection as a human rights concept.[22]

Eventually, the post-communist legacy continues to shape the way individuals think and state authorities perceive digitalization. On the one hand, trust in conspiracy theories (5G; Bill Gates and alleged chipping) among the public in Kazakhstan remains high. On the other hand, the country still preserves the Soviet legacy in distrust, hierarchy, and dissent. As a result, it has failed to build an effective communication strategy with the public, which in case of Internet shutdown, control of information flows and suppression of dissent have affected the way citizens perceive new technological solutions with respect to surveillance and human rights.

---

[19] Dina Baidildayeva, "Internet Censorship in Kazakhstan: More Pervasive than You May Think." OpenDemocracy, March 26, 2018, Accessed August 3, 2020. https://www.opendemocracy.net/en/odr/internet-censorship-in-kazakhstan/; "Reporters Without Borders: Heavy Internet Censorship in Kazakhstan." *Targeted News Service* (Washington, D.C.), 2019.

[20] Almaz Kumenov, "Hackers Eyeing Kazakhstan as a Safe Haven," *Eurasianet.org*, November 27, 2018, https://eurasianet.org/hackers-eyeing-kazakhstan-as-a-safe-haven.

[21] Chris Rickleton, "Kazakhstan: Internet Block Spotlights Unease among Elite," *Eurasianet.org*, February 17, 2020, https://eurasianet.org/kazakhstan-internet-block-spotlights-unease-among-elite.

[22] Luca Anceschi, "The Persistence of Media Control under Consolidated Authoritarianism: Containing Kazakhstan's Digital Media," Demokratizatsiya, 23, no. 3 (2015): 277-295; Madeline Earp, "Kazakhstan's Move to Control Internet Prompts Censorship, Surveillance Concerns," Committee to Protect Journalists, July 25, 2019, accessed September 1, 2020, https://cpj.org/2019/07/kazakhstans-move-to-control-internet-prompts-censo/.

Moreover, critically low levels of computer and digital literacy among the Kazakhstanis and reliance on foreign technologies have exposed the country to cybercriminals who exploit these weaknesses and capitalize on them.[23] One recent example is the activity of the Golden Falcon (earlier known as DustSquad, a sophisticated espionage hacking group) with mobile malware and radio interception hardware that targeted the thirteen biggest cities of Kazakhstan and stole personal data.[24]

When more countries turn to surveillance tools as a result of the coronavirus, it is also important to think strategically beyond collecting information. All digital plans and programs should build a healthy cyber ecosystem with credible legal norms and safety regulations, aimed at boosting economic welfare and developing new social rights. And if the Kazakh government could succeed in introducing strategic culture into its digitalization efforts without surveillance stigmatisation, it would receive higher support and better results in the long run.

Bibliography

Anceschi, Luca. "The Persistence of Media Control under Consolidated Authoritarianism: Containing Kazakhstan's Digital Media." Demokratizatsiya, 23, no. 3 (2015): 277-295.

Baidildayeva, Dina. "Internet Censorship in Kazakhstan: More Pervasive than You May Think." *OpenDemocracy*, March 26, 2018. Accessed August 3, 2020. https://www.opendemocracy.net/en/odr/internet-censorship-in-kazakhstan.

Cimpanu, Catalin. "Extensive Hacking Operation Discovered in Kazakhstan." ZDNet. November 23, 2019. Accessed March 18, 2021. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan;

Earp, Madeline. "Kazakhstan's Move to Control Internet Prompts Censorship, Surveillance Concerns." Committee to Protect Journalists. July 25, 2019. Accessed September 1, 2020. https://cpj.org/2019/07/kazakhstans-move-to-control-internet-prompts-censo/.

Gussarova, Anna. "Kazakhstan Experiments With Surveillance Technology to Battle Coronavirus Pandemic." Jamestown. April 08, 2020. Accessed September 1, 2020. https://jamestown.org/program/kazakhstan-experiments-with-surveillance-technology-to-battle-coronavirus-pandemic/.

Gussarova, Anna. "Culture of Protecting Personal Data: From Online Freedom to Digital Surveillance?" CABAR.asia. April 15, 2020. Accessed September 1, 2020. https://cabar.asia/en/culture-of-protecting-personal-data-from-online-freedom-to-digital-surveillance/.

Gussarova, Anna, and Dzhaksylykov, Serik. "Zashchita personalĭnykh dannykh v Kazakhstane: status, riski i vozmozhnosti." Public Policy Initiative. Soros Foundation Kazakhstan. April 2020. Accessed August 3, 2020. https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf.

---

[23] Anna Gussarova, "Culture of Protecting Personal Data: From Online Freedom to Digital Surveillance?" *CABAR.asia*, April 15, 2020, https://cabar.asia/en/culture-of-protecting-personal-data-from-online-freedom-to-digital-surveillance/.

[24] Cimpanu, "Extensive Hacking Operation Discovered in Kazakhstan."

Janenova, Saltanat. "E-Government in Kazakhstan: Challenges For a Transitional Country." Accessed September 1, 2020. https://www.nispa.org/files/conferences/2010/papers/201004220915450.janenovasaltanat.pdf.

Kelly-Clark, Victoria. "Central Asia: The Land of CyberCrime?" Global Risk Insights. April 29, 2019. Accessed March 18, 2021. https://globalriskinsights.com/2019/04/central-asia-cybercrime-land

Kumenov, Almaz. "Hackers Eyeing Kazakhstan as a Safe Haven." Eurasianet. November 27, 2018. Accessed March 18, 2021. https://eurasianet.org/hackers-eyeing-kazakhstan-as-a-safe-haven.

"Reporters Without Borders: Heavy Internet Censorship in Kazakhstan." *Targeted News Service* (Washington, D.C.), 2019.

Rickleton, Chris. "Kazakhstan: Internet Block Spotlights Unease among Elite." Eurasianet.org, February 17, 2020. Accessed September 1, 2020. https://eurasianet.org/kazakhstan-internet-block-spotlights-unease-among-elite.

Turkmenistan's Digitalization Strategy: Old Practices, New Façade?

Rustam Muhamedov

Turkmenistan embarked upon an ambitious digitalization strategy in late 2018. Since then, the government has taken a number of steps to improve its digital capacity. It devised the concept of the development of digital economy in Turkmenistan for the 2019–2025 period.[1] The concept is the government's first comprehensive strategy in the policy field that was fragmented by underdeveloped sector-focused (i.e., healthcare, tourism, etc.) digitalization initiatives.[2] The concept binds them together, setting a unifying and ambitious target—the radical transformation of all economic sectors, social sphere, and public governance through the introduction of digital technologies.[3]

At the organizational level, the government assigned Turkmen Communications Agency the task of policy coordination and established an ad hoc interministerial committee to steer the process of digitalization across sectors.[4] In addition, it adopted several legislative acts related to cyberspace development, such as e-signature and data protection; e-documents, e-document management systems, and digital services; Internet regulation; and cybersecurity.

These efforts together are yielding some visible, albeit still modest, progress in the country's digital development. The Turkmen segment of the Internet is steadily expanding; Turkmen banks and financial institutions, state enterprises (e.g., Turkmen Post, Turkmen Railways), and private companies are developing their own websites and expanding their e-services to citizens and businesses. The mass media are also being digitized: State TV channels and radio stations offer online broadcasting via the "Turkmen TV" website and mobile application, and Turkmen State Publishing Service's website hosts digitized issues of print media.

---

[1] "Prezident Berdymukhamedov utverdil Kontseptsiyu razvitiya tsifrovoy ekonomiki [President Berdymukhamedov adopted the concept of the development of digital economy]," *Khronika Turkmenistana*, December 1, 2018, https://www.hronikatm.com/2018/12/prezident-berdyimuhamedov-utverdil-kontseptsiyu-razvitiya-tsifrovoy-ekonomiki/.

[2] Ibid.

[3] "Digital Economy Development Strategy: Roadmap for Technological Transformation," *The State News Agency of Turkmenistan – Turkmenistan today*, January 28, 2019, https://tdh.gov.tm/en/post/16498/digital-economy-development-strategy-roadmap-for-technological-transformation.

[4] Batyr Berdyev, "Itogi pervogo kvartala tsifrovizatsii v Turkmenistane [The results of the first quarter of digitalization in Turkmenistan]," *Arzuw News*, April 8, 2020, https://arzuw.news/itogi-pervogo-kvartala-cifrovizacii-v-turkmenistane.

In a similar vein, authorities are expanding the e-services provision in the public governance sector. Most of state and state-affiliated institutions launched their own websites. In January 2019, the government introduced the e-document management system in public administration to streamline intra- and interagency workflow.[5] In November 2019, the government presented an "automated information system 'one-window' for the provision of public services in electronic form."[6]

The state's policy approach, however, has noticeable shortcomings, particularly in regard to facilitating good governance and catalyzing social growth.

First, though the government vows to transform all spheres, its efforts in digitalization are excessively skewed toward the economy, leading to uneven uptake of new technologies in other sectors. The government views digitalization primarily as a policy means of enhancing the competitiveness of the national economy.[7] The government struggles to reanimate the declining economy and hopes digitalization will contribute to mitigating the country's overdependence on the export of hydrocarbons for revenue.

Second, the policy implementation leaves much to be desired. It is characterized by a general lag in quality, hastiness and disorganization, and lack of clearly identified priorities and interim objectives in e-governance. The governmental web portals, including the e-gov platform, appear underdeveloped and visually outdated and have limited functional capacity, providing only a handful of e-services. They function as online information desks, letting citizens learn about the services online but still forcing them to visit the office to get the service they want. Moreover, these portals are filled with ideologically charged content that is mainly devoted to President Berdymukhamedov and his countless activities. At the time of writing, main political institutions—the Parliament, the Supreme Court, the Cabinet of Ministers, and even the office of the President—did not have their own websites. As a result, current efforts do little to simplify and streamline interactions among the government, citizens, and businesses and to boost the public's confidence in the utility of e-governance.

Third, the government is disinclined to implement far-reaching reforms in fundamentally important areas that can strengthen digitalization efforts and contribute to inclusive and innovative growth.

The digital divide is one such area. The national information and communications technology (ICT) infrastructure is largely underdeveloped, especially in rural areas. Turkmenistan's Internet connection is slow, discriminatively expensive, and unreliable. As a result, the country's Internet penetration rate stands at 26 percent, roughly half of the global average of 59 percent.[8] This digital divide limits citizens' access to essential governmental services and constrains their societal and political engagement, particularly that of vulnerable social groups, such as citizens with low income levels or residents of rural or remote areas. Consequently, the digital divide deepens further the existing social inequality and exclusion.

---

[5] "V Turkmenistane zapushchena sistema elektronnogo dokumentooborota [Turkmenistan launches electronic document workflow]," *EurAsia Daily,* January 23, 2019, https://eadaily.com/ru/news/2019/01/23/v-turkmenii-zapushchena-sistema-elektronnogo-dokumentooborota.

[6] "The trends of development of the sphere of telecommunications and information technologies presented in Ashgabat," *The State News Agency of Turkmenistan – Turkmenistan today*, November 27, 2019, https://tdh.gov.tm/en/post/20642/the-trends-of-development-of-the-sphere-of-telecommunications-and-information-technologies-presented-in-ashgabat.

[7] "Digital Economy Development Strategy," *The State News Agency of Turkmenistan*.

[8] Simon Kemp, "Digital 2020: Turkmenistan," DATAREPORTAL, last modified February 18, 2020, https://datareportal.com/reports/digital-2020-turkmenistan#:~:text=Internet%20penetration%20in%20Turkmenistan%20stood%20at%2026%25%20in%20January%202020.

The skills gap is another important concern. Turkmenistan's public has a low level of digital literacy and cyber-hygiene. The problem is exacerbated by the widespread use of unlicensed software,[9] which makes users even more vulnerable to nefarious cyber activities. It is difficult to assess the real magnitude of both problems, as authorities do not publish data on these issues.

Turkmenistan has initiated steps to address both problems. The government pledges to modernize the country's ICT infrastructure,[10] including in rural areas.[11] It also established the Institute of Telecommunications and Informatics and IT-platforms to train specialists in software support[12] and launched a number of computer literacy courses for public servants.[13] These efforts are insufficient, however. The government needs to reform the rigidly regulated and highly ineffective telecommunications and education sectors and address endemic corruption, nepotism, and opaque management practices. Turkmenistan also needs to foster public–private partnership to ensure continuous learning and skills improvement and share of best practices.

It is arguable that the government deliberately delays genuine reforms and is keen to retain its stranglehold on the Internet as current conditions ease its task of mass surveillance and control of the local population. In fact, the government has strengthened its repressive cyber capabilities in recent years.

In the financial sector, the government imposes informal restrictions on cash withdrawals and outbound money transfers and arbitrarily denies access to other financial services.[14] As all banks are state-controlled and citizens' salaries and social benefits are paid onto cards, the government exercises unfettered nationwide control over the cash flow to mask the domestic liquidity crises.

Ashgabat is equally eager to improve its capacity in advancing self-serving narratives online. President Berdymukhamedov has stressed the need to develop a Turkmen telegram-fashioned messenger and urged state mass media to register in major social networks to spread "credible" (government-favored) information about domestic developments and popularize the country's (regime's) achievements in the international arena.[15] In addition, Turkmenistan is becoming increasingly assertive in attacking foreign-based dissidents and independent media outlets that publish critical information about the regime's misconduct, accusing them of spreading "fake news" and "slandering" the country.[16]

---

[9] "The US calls on Turkmenistan's authorities to use licensed software," *Chronicles of Turkmenistan*, May 8, 2019, https://en.hronikatm.com/2019/05/the-us-calls-on-turkmenistans-authorities-to-use-licensed-software/.

[10] Vitali Volkov, "Tsifrovizatsiya Turkmenii: Zachem Ashgabadu bystryi internet? [Digitalization of Turkmenistan: What for does Ashgabat need the fast Internet?]," *Deutsche Welle*, October 31, 2018, https://p.dw.com/p/37Nau.

[11] "Prezident prikazal obespechit' sela shirokopolosnym internetom do kontsa goda [President ordered to provide rural areas with broadband Internet]," *Khronika Turkmenistana*, May 9, 2020, https://www.hronikatm.com/2020/05/internet/.

[12] "V Turkmenistane otkroyut samookupaemyie IT-ploshadki [Turkmenistan will establish self-financing IT-platforms]," *Khronika Turkmenistana*, October 27, 2019, https://www.hronikatm.com/2019/10/it-centers/.

[13] "Tsifrovizatsiya po-turkmenski. Byudzhetnikov posylaiut uchit'sia kompyuternym azam [Digitalization Turkmen way. State employed are ordered to learn computer basics]," *Turkmen.news*, March 26, 2020, https://turkmen.news/news/sifrovizasiya-turkmenistan/.

[14] Bruce Pannier, "Food lines in a land of marble," in Spotlight on Turkmenistan, ed. Adam Hug (The Foreign Policy Centre, 2019), 25-26.

[15] "Berdymukhamedov predlozhil sozdat' turkmenski messendzher dlia rasprostraneniia 'dostovernoi informatsii [Berdymukhamedov suggested creating Turkmen messenger to spread "credible information"]," *Current Time*, June 25, 2020, https://www.currenttime.tv/a/turkmenistan-berdimuhamedov-messenger/30690432.html.

[16] "Turkmenistan: Government responds to COVID-19 and hurricane with denial, cover-ups and intimidation tactics," *International Partnership for Human Rights (IPHR)*, June 11, 2020, https://www.iphronline.org/turkmenistan-government-responds-to-covid-19-and-hurricane-with-denial-cover-ups-and-intimidation-tactics.html.

Domestically, the government is strengthening its capacity in restricting access to information that criticizes it or exposes its misconduct. The state authorities block access to foreign media outlets, almost all social media platforms (e.g., Twitter, Facebook), and video-hosting sites (e.g., YouTube).[17] They also use a wide range of tactics, such as DNS spoofing, HTTP Host Header Inspection and IP blocking, disruption of Internet service, and monitoring and eavesdropping[18] to detect and intimidate activists who post critical commentary about the government online.[19]

Ashgabat is eager to strengthen its cooperation with like-minded technology-exporting states, namely Russia, to improve its surveillance capacity. In April 2019, Turkmenistan and Russia signed a bilateral agreement on strengthening cooperation in information security.[20] In October 2019, the leaders of both states issued a joint statement that reiterated the pledge to intensify efforts in deterring the use of digital technologies by outside agents for interference in domestic affairs.[21] The message is clear if one considers that both states endorse the "sovereign Internet" vision, which places excessive cyber oversight powers in the hands of the government under the pretext of securing civil stability and public order. Turkmenistan has already expressed an interest in Russian IT companies' developing Ashgabat's "smart city" project.[22]

Cooperation with China is currently less pronounced; however, both parties identify the telecommunications and AI technologies as promising areas for cooperation.[23] Some Turkmen IT companies are using the Chinese technology already. Agzybirlik Tilsimaty, the manufacturer of electronic devices, uses Chinese parts. Moreover, the company itself was established in partnership with Hengsheng Lianhua Investment Management Co. Ltd. and Tongfang Hongkong Limited.[24] Another company, Dogrulyk HJ, uses Chinese technology for its "safe city" digital solutions. The cooperation with both states is currently small-scale but is likely to intensify.

The government's intensifying repressiveness to quell the public's growing discontent with deteriorating living conditions galvanizes domestic online activism. The Turkmen public has regarded the Internet mainly as a recreational tool and medium for social interaction.[25] In recent years, the online space is increasingly being viewed as an outlet for expressing frustration and dissatisfaction with governmental policies. Currently, Turkmen online activism is mainly oriented toward foreign audiences. Its main goal is to shed light on negative domestic developments, which the regime tries to conceal. In April 2020, for instance, residents of the Lebap province shared visuals of the damage that was inflicted by a deadly hurricane, while the authorities kept a deafening

---

[17] "Turkmenistan: Report of Inquiry to German Cybersecurity Firm," *Human Rights Watch,* June 25, 2018, https://www.hrw.org/news/2018/06/25/turkmenistan-report-inquiry-german-cybersecurity-firm.

[18] "Freedom in the World 2020: Turkmenistan," Freedom House, last modified June 20, 2020, https://freedomhouse.org/country/turkmenistan/freedom-world/2020.

[19] "Turkmenistan: Report of Inquiry," *Human Rights Watch*.

[20] "O podpisanii Soglasheniya mezhdu Pravitel'stvom Rossiyskoi Federatsii i Pravitel'stvom Turkmenistana o sotrudnichestve v oblasti obespecheniia mezhdunarodnoo informatsionnoi bezopasnosti [On signing the Agreement between Russian Federation and Turkmenistan on cooperation in the area of international information security]," The Ministry of Foreign Affairs of the Russian Federation, last modified April 5, 2019, https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3602835.

[21] "Rossiya i Turkmenistan budut sotrudnichat' v sfere 'informatsionnoi bezopasnosti' [Russia and Turkmenistan to co-operate in the sphere of "information security"]," *Khronika Turkmenistana*, October 12, 2019, https://www.hronikatm.com/2019/10/olgino-tm-edition/.

[22] Evgeniya Tsinkler, "Ot raskopok do sudostroeniya [From digging to shipbuilding]," Rossiyskaya Gazeta, February 16, 2020, https://rg.ru/2020/02/16/reg-szfo/sankt-peterburg-i-turkmenistan-podpisali-dorozhnuiu-kartu-po-sotrudnichestvu.html.

[23] "Development of Turkmen-Chinese trade and economic cooperation is a priority," The Embassy of Turkmenistan in People's Republic of China, last modified October 15, 2020, https://china.tmembassy.gov.tm/en/news/67184.

[24] "'Agzybirlik tilsimaty" podgotovit okolo 160 tysiach kompiuterov dlia pervoklassnikov [Agzybirlik tilsimaty is to prepare around 160 thousand personal computers for first graders]," *Biznes Turkmenistan,* May 4, 2020, https://business.com.tm/ru/post/5455/agzybirlik-tilsimaty-podgotovit-okolo-160-tysyach-kompyuterov-dlya-pervoklassnikov.

[25] Annette Bohr, Turkmenistan: Power, Politics and Petro-Authoritarianism (London: The Royal Institute of International Affairs, 2016), 56.

silence.[26] Similarly, citizens shared visuals and information about the government's poor management of the COVID-19 pandemic.[27] Turkmen online activism is still in an embryonic state, but it is evolving and can potentially lay the foundation for full-fledged dissent against the incumbent regime in the long-term perspective.

Turkmenistan is most likely to keep its contradictory approach toward digitalization. The government is likely to keep its focus on improving the overall performance of the economy and state institutions, downplaying the good-governance aspect and ignoring genuine reforms. Consequently, it is highly unlikely that the government's efforts will lead to greater transparency and accountability or broaden citizens' engagement in the decision-making process.

The regime's wariness of digital tools' potential for challenging its repressive political model will remain a determining factor in setting the course, the intensity, the depth, and the breadth of digitalization. As of now, maintaining a firm grip on the Internet and developing a domestic digital ecosystem within strict limits will remain key priorities.

It is evident that Turkmenistan seeks to emulate the Chinese Internet governance model. Turkmenistan, however, is far less technologically advanced and far more resource restrained to pursue this goal unaided. The government, hence, will seek to strengthen cooperation with like-minded technology-exporting states, namely China and Russia.

The government's course of action risks putting the state in a disadvantaged position, making it dependent on outside actors and their interests. Further, it can stifle human and social capital growth and the development of innovative capacity. It can also cause greater distress for the public, exacerbating social inequality and insecurity.

This scenario is not predetermined, however. The government can make sustainable and inclusive social development happen if it supplements digitalization with genuine institutional reforms. Political will is the major pre-requisite for the success of this project. Otherwise, Turkmenistan's digitalization strategy will remain what it is now—just a new, fancy façade for the old rigid practices.

Bibliography

Berdyev, Batyr. "Itogi pervogo kvartala tsifrovizatsii v Turkmenistane." *Arzuw News*, April 8, 2020. https://arzuw.news/itogi-pervogo-kvartala-cifrovizacii-v-turkmenistane.

Biznes Turkmenistan. "'Agzybirlik tilsimaty" podgotovit okolo 160 tysiach kompiuterov dlia pervoklassnikov." *Biznes Turkmenistan*, May 4, 2020. https://business.com.tm/ru/post/5455/agzybirlik-tilsimaty-podgotovit-okolo-160-tysyach-kompyuterov-dlya-pervoklassnikov.

Bohr, Annette. *Turkmenistan: Power, Politics and Petro-Authoritarianism.* London: The Royal Institute of International Affairs, 2016.

[26] Rachel Denber, "Turkmenistan Government's Deafening Silence after Hurricane," *Human Rights Watch*, May 4, 2020, https://www.hrw.org/news/2020/05/04/turkmenistan-governments-deafening-silence-after-hurricane.

[27] "Turkmenistan: Government responds to COVID-19," *IPHR*.

Chronicles of Turkmenistan. "The US calls on Turkmenistan's authorities to use licensed software." *Chronicles of Turkmenistan*, May 8, 2019. https://en.hronikatm.com/2019/05/the-us-calls-on-turkmenistans-authorities-to-use-licensed-software/.

Current Time. "Berdymukhamedov predlozhil sozdat' turkmenski messendzher dlia rasprostraneniia 'dostovernoi informatsii'." *Current Time*, June 25, 2020. https://www.currenttime.tv/a/turkmenistan-berdimuhamedov-messenger/30690432.html.

Denber, Rachel. "Turkmenistan Government's Deafening Silence after Hurricane." *Human Rights Watch*, May 4, 2020. https://www.hrw.org/news/2020/05/04/turkmenistan-governments-deafening-silence-after-hurricane.

EurAsia Daily. "V Turkmenistane zapushchena sistema elektronnogo dokumentooborota." *EurAsia Daily*, January 23, 2019. https://eadaily.com/ru/news/2019/01/23/v-turkmenii-zapushchena-sistema-elektronnogo-dokumentooborota.

Freedom House. "Freedom in the World 2020: Turkmenistan." Last modified June 20, 2020. https://freedomhouse.org/country/turkmenistan/freedom-world/2020.

Human Rights Watch. "Turkmenistan: Report of Inquiry to German Cybersecurity Firm." June 25, 2018. https://www.hrw.org/news/2018/06/25/turkmenistan-report-inquiry-german-cybersecurity-firm.

International Partnership for Human Rights. "Turkmenistan: Government responds to COVID-19 and hurricane with denial, cover-ups and intimidation tactics." *International Partnership for Human Rights (IPHR),* June 11, 2020. https://www.iphronline.org/turkmenistan-government-responds-to-covid-19-and-hurricane-with-denial-cover-ups-and-intimidation-tactics.html.

Kemp, Simon. "Digital 2020: Turkmenistan." DATAREPORTAL. Last modified February 18, 2020. https://datareportal.com/reports/digital-2020-turkmenistan#:~:text=Internet%20penetration%20in%20Turkmenistan%20stood%20at%2026%25%20in%20January%202020.

Khronika Turkmenistana. "Prezident Berdymukhamedov utverdil Kontseptsiyu razvitiya tsifrovoy ekonomiki." *Khronika Turkmenistana*, December 1, 2018. https://www.hronikatm.com/2018/12/prezident-berdyimuhamedov-utverdil-kontseptsiyu-razvitiya-tsifrovoy-ekonomiki/.

Khronika Turkmenistana. "Prezident prikazal obespechit' sela shirokopolosnym internetom do kontsa goda." *Khronika Turkmenistana*, May 9, 2020. https://www.hronikatm.com/2020/05/internet/.

Khronika Turkmenistana. "Rossiya i Turkmenistan budut sotrudnichat' v sfere 'informatsionnoi bezopasnosti'." *Khronika Turkmenistana*, October 12, 2019. https://www.hronikatm.com/2019/10/olgino-tm-edition/.

Khronika Turkmenistana. "V Turkmenistane otkroyut samookupaemyie IT-ploshadki." *Khronika Turkmenistana,* October 27, 2019. https://www.hronikatm.com/2019/10/it-centers/.

Pannier, Bruce. "Food lines in a land of marble." In *Spotlight on Turkmenistan,* edited by Adam Hug, 24-28. The Foreign Policy Centre, 2019.

The Embassy of Turkmenistan in People's Republic of China. "Development of Turkmen-Chinese trade and economic cooperation is a priority." Last modified October 15, 2020. https://china.tmembassy.gov.tm/en/news/67184.

The Ministry of Foreign Affairs of the Russian Federation. "O podpisanii Soglasheniya mezhdu Pravitel'stvom Rossiyskoi Federatsii i Pravitel'stvom Turkmenistana o sotrudnichestve v oblasti obespecheniia mezhdunarodnoo informatsionnoi bezopasnosti." Last modified April 5, 2019. https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3602835.

The State News Agency of Turkmenistan. "Digital Economy Development Strategy: Roadmap for Technological Transformation." *The State News Agency of Turkmenistan – Turkmenistan today,* January 28, 2019. https://tdh.gov.tm/en/post/16498/digital-economy-development-strategy-roadmap-for-technological-transformation.

The State News Agency of Turkmenistan. "The trends of development of the sphere of telecommunications and information technologies presented in Ashgabat." *The State News Agency of Turkmenistan – Turkmenistan today,* November 27, 2019. https://tdh.gov.tm/en/post/20642/the-trends-of-development-of-the-sphere-of-telecommunications-and-information-technologies-presented-in-ashgabat.

Tsinkler, Evgeniya. "Ot raskopok do sudostroeniya." *Rossiyskaya Gazeta*, February 16, 2020. https://rg.ru/2020/02/16/reg-szfo/sankt-peterburg-i-turkmenistan-podpisali-dorozhnuiu-kartu-po-sotrudnichestvu.html.

Turkmen.news. "Tsifrovizatsiya po-turkmenski. Byudzhetnikov posylaiut uchit'sia kompyuternym azam." *Turkmen.news*, March 26, 2020. https://turkmen.news/news/sifrovizasiya-turkmenistan/.

Volkov, Vitali. "Tsifrovizatsiya Turkmenii: Zachem Ashgabadu bystryi internet?" *Deutsche Welle*, October 31, 2018. https://p.dw.com/p/37Na

The Role of Big Earth Data for the Implementation of the Sustainable Development Goals in Central Asia

Brendan Duprey and Akmal Akramkhanov

There is an ever-increasing understanding among policymakers and academics that the solutions to the challenges the world faces require a system's thinking approach. This means understanding how different parts of a system relate and interact with the whole. Using the system's thinking approach, in 2015, governments around the world passed the Sustainable Development Goals (SDGs) as the overarching road map for human development focusing on its three core aspects: social, environmental, and economic. The digital revolution has provided policymakers and academics with a greater ability than at any other time in human history to understand the complex interactions between these areas on a regional and global scale. Big earth data deriving from earth observation systems and ground-based observations can be analyzed to obtain an improved understanding of regional and global issues like climate change, human migration, and land use patterns, among others. In this context, the Big Earth Data Science Plan was established under the BRI to obtain Big Earth Data in an organized way and accelerate the use of that data for its practical application in support of the implementation of the SDGs in countries participating in the BRI.

This article explores ongoing environmental, social, and economic challenges facing Central Asia in the context of the implementation of the SDGs. Moreover, it identifies some of the initiatives related to ongoing Big Earth Data projects in Central Asia and potential interlinkages with the Big Earth Data Platform of the BRI. The consequences of not fully understanding regional environmental changes in Central Asia based on robust data sources are severe. Regional security, economic growth, and overall well-being of citizens residing in Central Asia are directly linked with the sustainable use of cultural and natural resources. Therefore, the benefits of participating in the Science Plan are substantial. In order for the Belt and Road Science Plan to be effective, however, it not only needs to help build technical infrastructure and professional capacities within Central Asian countries, but it must also deal with the issue of trust between the Chinese government and Central Asian states. Knowledge platforms such as the Big Earth Data Platform of the BRI require trustful relationships with dependencies and shared responsibilities between partners in Central Asian countries. Ethics and security concerns regarding how this data will be used and interpreted must also be openly presented to potential contributors. Moreover, outreach should be made by its creators to ensure that points of collaboration are identified and synergies created between ongoing initiatives in the region. Central Asia's participation in the Science Plan would be beneficial not only to stakeholders in Central Asian countries but also to the Chinese government as the region holds a rich array of natural resources ranging from oil and gas to rare earth metals. This article describes all of these issues in detail. It is the hope of the authors that readers will obtain a richer understand of the value of big earth data in the implementation of the SDGs in Central Asia and how the DBAR Science Plan and subsequent Big Earth Data Platform could prove to be a useful tool for integrated system's thinking for the implementation of the Sustainable Development Goals if concerns of stakeholders are addressed in an open and transparent way.

Global Environmental Challenges: A System's Thinking Approach

The world has seen remarkable social, environmental, and economic changes since the start of the Industrial Revolution. The human population has exploded from a little over a billion people in 1800 to almost eight billion in 2020 (Chamie, 2020). We have also seen rapid urbanization. Ten years ago, the planet hit the milestone of more than half the world's population's living in urban areas. Urbanization is predicted to continue at a rapid rate with more than 70 percent of the world's population living in urban settlements by 2050 (Chamie, 2020). These changes have led to a dramatic reconfiguration of the biosphere and have fundamentally altered the natural world. Once altered, natural habitats stand very little chance of being restored. Moreover, with further digitalization of the world, new technologies can help either conserve the value of "natural environment" or completely deplete it for new generations that are increasingly immersed and nurtured in urban and virtual environments, detaching them from human impacts on the natural world. Our impact as a species is so great that geologists have formally proposed to the International Commission on Stratigraphy to designate a new epoch "Anthropocene" where human activity has significantly altered the planet's climate and ecosystems. All ecological indicators ranging from biodiversity loss to freshwater ecosystems health have deteriorated significantly over the past fifty years. For example, from 1974 to 2014, the world has seen a 60 percent decline in population of vertebrate species (Grooten & Almond, 2018). The United Nations estimates that by 2050 5 billion people could suffer from shortages of fresh water (Crellin, 2018). The above-mentioned problems are exacerbated by climate change. driven by more than 410 parts per million of CO_2 in the atmosphere. The last time the climate had accumulated such a large concentration of CO_2 was more than 800,000 years ago (Grooten & Almond, 2018). Rockstrom notes in his work "A Safe Operating Space for Humanity" that we must live within certain ecological limits as a species to in order make the Earth suitable for our existence. Within the nine planetary boundaries, he defines we are beyond our boundaries in three: climate change, nitrogen cycle, and biodiversity loss (Figure 1) (Rockstrom et al., 2009).

The causes for this decline are complex and consist of a variety of social, ecological, and environmental factors. What the world leaders have come to realize is that traditional ways of thinking in regard to environmental problems and subsequent policy solutions are no longer relevant to the interconnected and interrelated problems we face as a global community. One cannot look at water scarcity without looking at social patterns of migration, water consumption by citizens, and precipitation variabilities due to climate change. Therefore, system's thinking identifies how different parts of a system—climate, migration, and water scarcity—interact with one another. In system's thinking, information is used to ensure that actions taken on a systems level are greater than acting on their individual parts. For the first time in human history, world leaders have set the roadmap for future development of the planet using the system's thinking approach as its framework. Under this approach, social, environmental, and economic development are linked under the umbrella of the Sustainable Development Goals (SDGs) (2015–2030). These goals are an unprecedented commitment by world leaders from around the globe to put sustainability as the overarching theme for human development.

Environmental Challenges in Central Asia

Similar to the challenges globally, Central Asia is experiencing a host of environmental problems. These problems pose serious long-term threats to ecosystems, the economy, and social stability. One of the most pressing environmental issues facing Central Asia is the scarcity of water resources due to agricultural use, high consumption rates, and an inexpensive pricing system for these resources. Some of the largest bodies of water

in the region are Lake Balkhash and the Aral Sea, both part of the endorheic basin that also includes the Caspian Sea. Irrigation and water use for industrial purposes have contributed to the significant reduction of these water bodies, among others. Rivers that connect to these water bodies have been diverted for agricultural and industrial purposes as well, further exacerbating the problem. Global climate change has also contributed to a substantial reduction of the available water resources in the region (Qi & Kulmatov, Jan 2008). Snow and glacier melt are essential in many Central Asian cities like Almaty, Kazakhstan, for fresh drinking water and irrigation. Farinotti et al. (2015) illustrate that Central Asian glaciers have shrunk 20 to 30 percent over the past fifty years (Farinotti et al., 2015). This current trend is expected to continue and will eventually deplete the glacial ice and significantly reduce or virtually eliminate glacial runoff (Fu et al., 2017). Most of the population growth in Central Asia is concentrated in large urban cities. This is primarily due to lack of employment opportunities in rural communities, as well as the scarcity of water resources in the vast steppes of the region (Eshonov & Kamilov, 2013). According to an ESCAP report on urbanization, the urban population will grow in Central Asia about 1.5 percent per year until 2050, which exceeds the annual growth rate of the overall population (Eshonov & Kamilov, 2013).

Soil erosion and salinization have also been recognized as serious problems in Central Asia. These are primarily due to increasing agricultural production and irrigation efforts that began in the 1960s while Central Asia was still part of the Soviet Union. The result was a steady decrease in the available fertile land for agriculture. Water evaporation due to irrigation intensifies the salinization of agricultural lands, a process that is hard to reverse once it has begun (Qi & Kulmatov, 2008).

Water scarcity and salinization are inextricably interconnected, and the solution to one challenge must be visualized in the form of a system. For example, the ever-increasing use of land for agricultural purposes has led to a decrease in water feeding the Aral Sea. As the Aral Sea continued to dry up, the climate in the region also changed. This has caused additional dust and salt to transport to its surroundings, as well as reduced air humidity. If we take into consideration the ever-increasing population dynamics leading to increased consumption, the ramifications are predictable (Qi & Kulmatov, 2008).

What we see from these examples is the ever-growing need for accurate and integrated data that can help drive policy decisions that lead to the sustainable use of natural resources. Regional data, while useful, must also be analyzed in the context of broader global environmental trends—in particular, climate change.

What Is Big Earth Data?

The digital revolution has led to a greater understanding of our planet today than at any other point in the history of human civilization. Al Gore was one of the first political figures to recognize the value of digital information in understanding our planet. In 1998, he submitted to the California Science Center a statement which stressed the need for a "Digital Earth, i.e. a multi-resolution, three-dimensional representation of the planet, into which we can embed vast quantities of geo-referenced data" (Gore, 1998, p. 1). Subsequently, the International Society on Digital Earth was founded in 2006 with the aim of providing a platform for academic exchange, innovation, and education on Digital Earth (ISDE, 2020). The Society expanded its role to "accelerate information transfer from science to applications in support to the implementation of UN Sustainable Development Goals and in support of a sustainable management of global environmental commons" (Guo et al., 2020). In this context, Digital Earth utilizes "Big Earth Data to study big data analytics ecosystems and platforms to comprehend the complex Earth

system coupled with social systems—utilizing data from Earth observation and social sensing" (Guo et al., 2020) Therefore, digital earth is supported by information deriving from Big Earth Data. This concept of Big Earth Data refers to "all data related to the Earth including its interior, surface, atmosphere, and near space environment" (ISDE, 2020). This data is utilized for scientific exploration and discovery in regards to the earth's systems. According to the ISDE, Big Earth Data is defined by being "massive, multi-source, heterogeneous, multi-temporal, multi-scalar, highly dimensional, highly complex, nonstationary, and unstructured" (ISDE, 2020). For example, satellite observations and sensors can provide useful information on soil, ecosystems, atmosphere, among other topics, as well as their changes over time. The Internet of Things, model simulations, oceanic-based observations, and ground-based observations, among others, are all data streams that can be defined as Big Earth Data.

This type of data has become so important that a field of science has been created around it called Big Earth Data Science. Its objective is to study from a holistic perspective and in a multidisciplinary way the complexity of earth systems, understand how to manage and store data on various platforms, forecast and identify future earth trends based on digital data, and determine how earth data can be used as a tool for managing complex earth systems (Guo et al., 2020). Big Earth Data and the science surrounding its use will, therefore, play a critical role in the implementation of the Sustainable Development Goals in Central Asia and worldwide.

Belt and Road Initiative and the Need for Big Earth Data

The Belt and Road Initiative (BRI) is a massive endeavor by the Chinese government to build up human connectivity and trade among Asia, Europe, and Africa. The initiative, officially launched in Kazakhstan in 2013, is expected to involve $1 trillion in investments, more than 70 countries accounting for 65 percent of the world's population, and approximately one-third of the world's gross domestic product. These investments will be made primarily in telecommunication networks, roads, ports, airports, railways, and power plants (EBRD, 2020). Major infrastructure projects can and will have a significant impact on the natural systems in the countries where they are launched.

There is little precedent, however, for analyzing, let alone managing, the ecological impacts of investment projects the size and complexity of the ones forecasted as part of the Belt and Road Initiative. Moreover, most of the existing research has specialized within a particular field of study or a specific site (Teo, et al., 2019). There is an increasing understanding that a system's approach must be taken to incorporate the specific characteristics of interconnected and complex systems (Hamilton et al., 2015). Belt and Road investments in Central Asia, such as the Western Europe–Western China Highway and projects along the China-Kyrgyzstan-Uzbekistan transportation corridor, have multiple impacts on the natural ecosystems where these corridors are located. Moreover, these impacts are also cumulative, as investments attract new infrastructure and affect population flows by increasing economic opportunities and accessibility of previously inaccessible locations. Teo et al. (2019) use an ecosystems approach to characterize how various infrastructure projects along the Belt and Road can affect various aspects of the earth systems, including the biosphere, hydrosphere, atmosphere, and geosphere. Roads like the Western Europe–Western China Highway can affect the atmosphere by increasing air pollution, dust, and microclimatic effects from warming (Figure 2). Highways can also affect the biosphere through habitat loss, roadkills, habitat fragmentation, and other effects. The geosphere is affected adversely by roads through soil erosion and landslides in mountainous areas. Finally, the hydrosphere can be adversely affected through pollution and sediments in runoff, littering, and impeding drainage (Teo et al., 2019). This example illustrates the need for diverse sets of data

to better understand complexity and think on a system's level in regard to the impact of projects along the Belt and Road corridors. Climate change, land degradation, and ecosystem destruction, among other sustainability challenges, are widespread through the BRI countries, including those in Central Asia, and had existed before the BRI was formulated (DBRI, 2017). Unfortunately, research has shown the lack or, in some cases, absence of data to understand the complex causations for these changes for most Belt and Road Initiative routes (Zhang et al., 2019). Lack of data and results from the region stems partly from the shortsightedness in support of research and consequent lack of capacity in these countries to make use of already available and accessible open data. The potential positive implications of the widespread use of Big Earth Data for countries participating in the BRI are vast as infrastructure investments continue in the region.

What Is the DBAR Science Plan and the Big Earth Data Platform?

Addressing the need for Big Earth Data along the BRI countries, in 2016, the Chinese government passed the "Beijing Declaration on Earth Observation for Belt and Road." The Declaration emphasized the need for the implementation of the "Digital Belt and Road" Program, a science and technology partnership for efficient use of earth-observation (EO) science and technologies and Big Earth Data platforms and frameworks for sustainable development. Moreover, it seeks to integrate low-carbon and green approaches to social and economic growth to help achieve commitments within the framework of the 2015 Paris Climate Agreement (DBRI, 2017).

One of the core aspects of the Science Plan is the creation of a Big Earth Data Platform. Its overarching goal is to develop itself as a platform that will "facilitate the sharing of Earth observation technologies and information services across B&R countries for effective application of EO technology for sustainable economic and societal development" (DBAR, 2017, p. 2). What sets the DBAR Science Plan and its Big Earth Data Platform apart from other initiatives and platforms is the number of countries covered under the Platform and the intention of its creators to use data deriving from the Platform to implement concrete projects. These projects are based on data related to a diverse set of social, economic, and environmental issues ranging from preservation of natural heritage to management of urban development. Moreover, this work is being delivered simultaneously with large-scale infrastructure and investment projects in BRI countries, providing the opportunity to apply this data to real-time investments. Through scientific analysis leading to improved understanding of the spatial distribution of natural resources and ecosystems, the DBAR Science Platform seeks to create a decision-making system that can change trends in the region (DBRI, 2017, p. 5). These projects are intended to contribute significantly to the implementation of the Sustainable Development Goals on a global scale (DBRI, 2017).

Topical Areas of the DBAR Science Plan

As mentioned, the DBAR Science Plan aims to link data streams such as ground-based observations, remote sensing satellites, communication satellites, ocean-based observations, and navigation satellites into a Big Earth Data Platform used to translate complex data into useable information. The system is meant to allow any user in the BRI countries to access the information and to use it regardless of his or her technological or computational abilities. The information is divided into Foci that are clustered into three categories: natural impact, societal development, and regional Foci. These are further categorized into two parts. One is the eight Foci relevant to address sustainable development (Natural Impact—Disaster Risk, Climate Change and Ecosystems, Water

Resources and Security; Societal Development—Infrastructure and Urban, Natural and Cultural Heritage, Agriculture and Food Security; Regional Foci—Coast and Marine, High Mountains and Artic); the other is the centralized Big Earth Data System (DBAR, 2017). These Foci were determined as areas where there is a research gap. Moreover, they were selected as a result of outstanding research questions deemed relevant to solve in order to attain SDG goals and targets in Belt and Road Countries (Figure 3). These Foci are highly relevant to the sustainability challenges facing Central Asia, namely High Mountains, Natural and Cultural Heritage, Agriculture and Food Security, Infrastructure and Urban, Water Resources and Security, among others. Data on critical habitats for climate and biodiversity like the Kazakh Steppe or Tien Shan mountain glaciers is vital for managing the sustainability of these ecosystems.

Research Design and Timeline

Figure 4, DBAR Workflow (DBAR, 2017), illustrates the five levels of research actions that will be taken within the framework of the Science Plan. Actions of the first level aim to obtain access to diverse data streams. The second level envisages providing an easy-to-use platform to take those data streams and turn them into useable information for interested parties within the BRI countries. The third level includes experimentation to model the earth's processes, concentrating on the eight Foci relevant for countries of the BRI, along with activities to support the Foci. These results will then be disseminated at level four, where achievements will be highlighted and best practices shared. Finally, the fifth level entails promoting project outcomes that are most pertinent for the implementation of the SDGs in the region and globally (DBRI, 2017). The Science Platform is expected to be implemented in three phases over a ten-year period:

- Phase I: Design and Launch (2016–2018)
- Phase II: Implementation Stage 1 (2019–2022)
- Phase III: Implementation Stage 2 (2023–2026)

DBAR Science Plan Governance

The Plan also has a comprehensive governance strategy consisting of several governance bodies. The Scientific Committee oversees the operations and projects implemented within the context of the science plan. The Secretariat oversees the day-to-day operations of the Plan, reports to the Scientific Committee, provides information to stakeholders on the outcomes and progress of the Plan, coordinates the day-to-day communications with the scientific community and stakeholder groups in the DBAR countries, and promotes funding opportunities available for its implementation. The working groups (seven in total) for each Foci area have a task to ensure implementation of activities linked with their respective Foci. Finally, the task forces are set up to deal with emerging issues such as High Mountains and Cold Regions. One notable governance aspect is the creation of International Centers of Excellence (ICoEs) established to contribute to the DBAR in their respective countries and areas of work. They can be based on existing institutions specializing in Big Earth Data and projects

linked with implementation of sustainability initiatives based on this data. They are tasked with generally aligning with the objectives of the Plan, actively engaging in fostering partnerships and promoting awareness-raising campaigns for the Plan, and cooperating with other academic institutions participating in the Plan (DBRI, 2017).

Status of the Plan

The Chinese government has been moving forward with this initiative since its inception. All governing structures mentioned above have been created and are actively engaged in work. In 2018, the SC approved the locations of the International Centers of Excellence in Peshawar, Bangkok, Helsinki, Potenza, Moscow, El Jadida, Lusaka and Columbia; four ICoEs have been officially inaugurated and are now operational. The Big Earth Data Platform hosted seven data products and contained more than 90TB of data. It also hosts more than 60 web map services and provides web-processing services (Guo et al., 2018b). In 2020, the Chinese Academy of Sciences published a report with 26 case studies at an international, regional, national and local scale to showcase best practices on and monitoring the results of SDG targets. This included "24 data products 13 methodologies and 19 results that are of value to policy makers" (Huadong, 2020, p. 6)

Opportunities to Link the DBAR Big Earth Data Platform to Ongoing Efforts in Central Asia

The DBAR has the ambitious target of developing a platform that handles diverse types of information in countries in which it operates. This is especially true for Central Asia, as it plays a key role in the initiative because of its vast natural reserves and strategic location for trade with Europe. Central Asia's participation in the initiative and subsequent Big Earth Data Platform, however, is lacking. There is experience in Central Asia looking at different aspects of agriculture and environment. Such experience is important, in order to better understand how protecting environment can oftentimes run counter to economic development (Guo, 2018). Teo (2019) assessed BRI impacts on natural system of infrastructure projects. Figure 2 demonstrates mostly affected areas. Air and soil pollution, habitat fragmentation and loss, and contaminants are among frequently mentioned areas that seem to be most vulnerable. This means that projects conducted within the context of the BRI must be analyzed before, during, and after such projects are initiated, as also indicated by Tracy et al. (2017). The analysis should be used to prevent, monitor, and mitigate their impacts on the sustainable use of natural and cultural resources in Central Asia and more broadly BRI countries. Several initiatives involving Big Earth Data collection and analysis have been conducted in Kazakhstan and Central Asia. Integrating these projects and initiatives into the Big Earth Data Platform would be not only useful, but a necessary measure. Such integration can be used to ensure that comprehensive sets of data for Central Asia are utilized when determining investment schemes by the Chinese government based on data gaps, impacts of proposed projects, and capacities needed. The below projects are diverse and presented to illustrate the breadth of Big Earth Data initiatives undertaken or currently underway in Central Asia. This is by no means meant to be an exhaustive list but merely a representation of a broader set of data available for use by the BRI Big Earth Data Platform.

Central Asia Climate Information Platform

Climate change studies in Central Asia are not abundant; however, global modeling efforts and reports generally project higher than average warming trends. Reports indicate that even if the global mean temperature increase is limited to 2°C above pre-industrial levels, Central Asia will be severely affected by climate change. This is primarily caused by the potential for impacts to occur simultaneously and compound one another (Reyer et al., 2015). Data on the detailed effects of projected higher temperatures is lacking, particularly in mountainous areas (Xenarios et al., 2019). This emphasizes the need for better and regionalized data and for tools to help analyze climate change trends by regional stakeholders.

Central Asia Climate Information Platform[1] (CACIP) commissioned by Regional Environmental Centre (CAREC) is one of the attempts to provide climate-related information for the region. CACIP has also similarities with the Big Earth Data Platform, as it aims to make available comprehensive and up-to-date relevant data and information from global, regional, and local sources. It also seeks to provide analytical tools and interfaces for the visualization and interpretation of data and information (Figure 5).

The process of conceptualizing an operational platform took into account outcomes of several rounds of national and regional consultations to fine-tune the design. CACIP platform is designed to consist of three blocks of information: website, knowledge hub, and geoportal (Figure 6). System architecture of geoportal is functions through GeoServer, which is able to publish local and remote data using open international interoperability standards (Figure 7).

The platform allows many different users, like policymakers, researchers, and farmers, to access and analyze a wide range of climate-relevant information, supporting improved awareness, assessment, and decision making. CACIP covers the five Central Asian countries, providing both a regional outlook and country-specific information. CACIP is available in Russian and English. In later stages, CACIP will include five Central Asian languages. Specific features included in CACIP are:

- Draws in relevant public data, making it available in one central location.
- Provides tools and interfaces for visualizing and interpreting data such as temperature, soil moisture, and desertification.
- Combines information from multiple sources, for example merging national-level datasets to generate a regional perspective.

Currently, CACIP is launched and available at the following address: http://centralasiaclimateportal.org/. CACIP's Knowledge hub, one of the sections of the platform, is harvesting information from dozens of open source resources that were inventoried during the preparation stage. The total number of documents at this writing approach 10,0000 (ten thousand), with thematic areas covering not only Central Asia but also globally so as to provide examples of approaches and results from other regions. The majority of these have been harvested through automatic protocols that allow accessing new information as soon as it is uploaded at the original resource address. The number of tools integrated on the platform expand from similar efforts done by the World Bank at Central Asia Water and Energy Data Portal available at http://spatialagent.org/CentralAsia/.

[1] http://centralasiaclimateportal.org/

Climate change will affect all BRI regions, and information and approach compiled on CACIP could become an already functioning demonstration model for other regions of BRI. While the CACIP platform is at an initial stage of operation, its presence in the region provides a good starting point to implement and expand with new capacities from the Big Earth Data System in Central Asia. Since all compiled materials on the platform are free, stakeholders and decision makers may access, analyze, and visualize public domain data to support improved awareness, assessment, and decision support.

Land Abandonment

The global impact of climate change is often reported as negative, and the impact of climate change on drylands is no exception. Dominant areal parts of Central Asia can be characterized by low precipitation, resulting in land cover with moisture-limited rangelands and irrigated, desert, and semi-desert ecosystems. Such fragile ecosystems are very prone to climate variabilities and anthropogenic activity. The loss of land cover in these ecosystems can enhance erosion and desertification processes. To react timely to such vagaries, one needs to have robust systems and approaches that provide evidence of changes happening on the ground.

Various approaches have been used to investigate the region's cropland area and cropland abandonment as a way to better inform prospects of food security in the region (Löw et al., 2018; Zhang et al., 2018). Big Earth Data platforms could provide further improvements to both scale and resolution for studies such as these, as well as address the limitations of individual methods.

Among recent efforts ICARDA conducted in the region integrating remote sensing data was looking at land cover change and to identify abandoned agricultural areas. Most of the products generated during these studies are made available at http://geoagro.icarda.org/cldd/index.html that can be explored and compared between different years. Since inputs used to derive such products are based on available and regularly updated data, the majority originating from satellite imagery, the approach can be used as a strong example for stakeholders to replicate and fine-tune for other relevant purposes.

Here we present a few use-cases; others can be found on http://geoagro.icarda.org. Zhang et al. (2018) used satellite data for analyses to provide comprehensive pictures of rangeland degradation and desertification in Central Asia from 2000 to 2014, also inferring improved understanding of its drivers. Analyses covering the whole region were able to discern a degradation trend gradually expanding northward (Figure 8). It also helped to identify sensitive and fragile regions within transitional rangeland zones where higher frequency of sparsely vegetated areas were occurring. Additionally, it identified significant browning within constant grass-covered areas. Such data illustrated that the loss of vegetative land cover is happening intensively in otherwise constantly grass-covered areas. These changes were linked to persistent droughts in Central Asia (Zhang et al., 2018).

Without large amount of data fed by earth observation sensors, able to instantly cover vast geographic regions and with high frequency, analyzing and discerning land cover trends would be arduous. Timely recognition of changes are paramount in order to develop mitigation options for decision makers that could involve grazing management, water supply, and other anthropogenic activities (Zhang et al., 2018).

In drylands of Central Asia, an irrigated agroecosystem is the backbone of food production, and any land that is not used causes substantial production losses. Often, land is fallowed between crop production for a short period of time; however, land abandonment is also frequently observed throughout irrigation schemes leaving the land untouched for long periods of time. The causes for land abandonment are diverse and often linked to marginal land that was initially hardly suitable for crop production as well as prolonged water shortage during irrigation season. Despite land's not being used for many years, it is usually still categorized as irrigated land and may go back into production whenever water supplies are abundant to reach these abandoned areas. Such dynamism makes temporal and spatial mapping complicated to determine if land in a particular region is abandoned or fallowed.

Tapping into big data provided by earth observation sensors coupled with a novel method of fusing with a locally weighted decision approach offers solutions to discerning abandoned land. Löw et al. (2018) analyzed time series of the Normalized Difference Vegetation Index (NDVI) from Moderate Resolution Imaging Spectroradiometer (MODIS) from 2003 to 2016. As an example, high-resolution images from 2016 clearly show typical indicators of land abandonment (Figure 9), such as advanced shrub encroachment, which supported the labeling process (Löw et al., 2018). Authors saw that abandoned cropland occurred particularly in the downstream regions of Uzbekistan (e.g., Karakalpakstan) and Kazakhstan (e.g., Kazalinsk and Kyzyl-Orda) and partially in some upstream regions in Uzbekistan (e.g., Kashkadarya, 16 percent) (Figure 10). Methods used in this study proved that a MODIS time series was well suited to tracking abandonment in arid areas where the difference between actively cultivated and abandoned cropland is subtle.

Study showed that abandonment is also common in areas where land demand is high. In total, 13 percent (1.15 Mha) of the irrigated agricultural land was abandoned by 2016, with a drastic difference in rates across the countries (Löw et al., 2018). The knowledge of the patterns of abandonment is important for land-use planning for accounting land and allocating for alternative purposes. Authors developed the map of abandoned irrigated cropland that provides a novel basis and the necessary baseline information to guide land-use and conservation planning support in the region, such as the assessment of environmental trade-offs and social constraints of recultivation (Löw et al., 2018).

With DBAR efforts, similar types of analyses of other aspects, such as yield gap, water use efficiency in irrigated areas, and change in woodland area, to name a few, could be conducted in more detailed resolution. A lessons learned from CACIP conceptualizing is that there is a great demand for digital services; however, augmentation with data from local sources can be challenging because of trust issues and lack of established and updated databases, as well as capacity and exposure of personnel to innovative solutions that big data and digitalization offer.

Geospatial Application Kazakhstan Climate Change

Exploring historic and future changes of environmental parameters in easy-to-use applications covering country scale is vital to develop mitigation and adaptation measures. Web-based geospatial application Kazakhstan Climate Change to explore climate change retrospective data and future scenarios is developed by the Institute of Geography and Water Security at https://geoportal.ingeo.kz/climate. It provides visualization and geospatial analysis of climate change data for Kazakhstan and neighboring basins of transboundary rivers.

Application includes several datasets such as daily maximum and minimum temperatures, precipitation, evapotranspiration, and drought indices consolidated from ensemble of twenty-one models computed within the fifth phase of Coupled Model Intercomparison Project (CMIP5). The latest, fifth report of Intergovernmental Panel on Climate Change (IPCC) utilizes outputs of the CMIP5 modeling efforts.

Kazakhstan Climate Change provides options to look at datasets covering the past 1950–2005 and to examine future climate projections from 2006 to 2100. It also allows one to choose projections with intermediate (RCP4.5) and high (RCP8.5) emission scenarios. Spatial scale of analyses is roughly 25x25 km, which results in processing a large amount of data to cover the entire country. To facilitate faster visualization and processing, the data can be averaged over a select number of years.

The focus of the application is very relevant for the research community to conduct studies on climate change regional impact, at spatial scales of river basins, districts, and watersheds. General public audience as well as government and nongovernment institutions can employ this tool to be aware of possible climate-change trends in Kazakhstan and integrate such information and knowledge in policymaking processes to develop plans and strategies to mitigate negative impacts in affected sectors of an economy.

Much of rural livelihoods in Kazakhstan and overall, of Central Asia, depends on agriculture, natural conditions, and resources to grow food and feed crops. Analysis of drought conditions under future climate change becomes vital to know in order to sustain livelihoods of rural population. The tool in Kazakhstan has no analogues in the country or likely in the region. The opportunity for DBAR will be to integrate outputs of modeling efforts originating in countries of BRI in such applications to cooperate and share more readily with stakeholders.

Policy Implications

The Big Earth Data system within the DBAR Initiative is in the form of the Big Earth Data Sharing Service Platform developed by CASEarth. The platform provides systemic, diversified, dynamic, continuous, and standardized Big Earth Data to global users and also promotes new data-sharing models by integrating data, computing, and services (Guo et al., 2020). The DBAR Big Earth Data system is designed for six activities: (1) handle vast amounts of satellite imagery and socioeconomic data; (2) provide web-based interactive data exploration; (3) offer distributed scientific computing algorithms; (4) provide a cloud computing environment for Big Earth Data science analytics; (5) offer specific APIs for various users; and (6) provide a new data model for sustainable development decision making (Guo et al., 2020). The policy implications for engaging Central Asian countries in the DBAR Big Earth Data Platform for the Chinese government, BRI countries, and Central Asian countries are vast. Infrastructure projects and other investments deriving from the BRI can have both positive and negative impacts on the environment. Without comprehensive and integrated data on environmental and social impacts on these investments, however, mitigation and adaptation measures cannot be effectively enacted. Participation and contribution to the Big Earth Data System of the DBAR by Central Asian countries can have a variety of positive effects, including the following.

Building Trust and Improved Collaboration among Central Asian Countries

It is widely known that there is a lack of trust in regard to environmental matters, especially transboundary water issues between Central Asian countries. Perceptions of intentionality and lack of effort to support water management have become major obstacles for policy making and coordination on a regional level. This lack of trust and disjointed coordination in regard to natural resource management has had a substantial impact on economies in the region because of their interdependent nature (Pohl et al., 2017). Big Earth Data frameworks in general rely on collaboration because of the aggregation and standardization of data based on the FAIRness and openness principles. In the Central Asia context, the sharing notion put forth by the Big Earth Data system within DBAR would be beneficial to regions that lack sufficient access or resources to earth observation (EO) infrastructure and capability. Both human and technological capacity to extract information from EO infrastructure and data varies differently across Belt and Road countries (Guo et al., 2020), including in the five countries in Central Asia. Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan, for example do not possess earth-observing satellites or facilities for mass data processing. Moreover, any local data that are available are rarely shared and are often not publicly accessible because of their storage in government or university archives (Guo, 2018). An open access and neutral environmental data platform can be used as a mechanism to gradually improve cooperation by providing a location to upload and share data freely. It also can work as a neutral informational tool to identify trends and manage regional threats based on accurate and verified data linked with the sustainable use of natural and cultural resources.

Support the Implementation of the SDGs on a Regional Level

The Sustainable Development Goals are interrelated and interconnected, providing a system's thinking approach to human development. Big Earth data and the Big Earth Data Platform work in a multidisciplinary, holistic, and transdisciplinary way (Guo et al., 2020). Therefore, these systems can and should play a critical role in analysis and sustainable management of natural and cultural resources. Regional challenges like sustainable water management, land management, and climate-change mitigation and adaption will require accurate, reliable, and integrated data not only on a regional level, but also on a global scale. The Big Earth Data System can also provide an important tool to measure and quantify the global indicators framework for the Sustainable Development Goals.

Build Capacities and Improve Knowledge of Central Asian Experts

Sustainability challenges in Central Asia are local, national, regional, and international. One cannot look at the issue of water scarcity without looking at the issue of climate-change dynamics or patterns of agricultural use on one scale. These topics must be looked at at the national, regional, and international levels in order to understanding patterns and dynamics driving emerging trends. Therefore, the DBAR Science Plan provides a holistic approach to looking at sustainability challenges through various lenses. It will provide the opportunity for policymakers and academics to look at data cross-sectorally, but also on multiple scales. Having more capacity to conduct earth observation through the Big Earth Data Platform can present opportunities to further scale previous environmental studies covering Central Asia, such as in ecological security (Li et al., 2019), precipitation

estimates (Guo et al., 2015), and climate adaptation in mountainous regions (Xenarios et al., 2019). As an earth observation system, the Big Earth Data Platform could also support studies addressing geographically related information such as those identifying landslide hazard (Roessner et al., 2005) and earthquake hazard (Mohadjer et al., 2016; Rebetsky et al., 2012). It is well known that Central Asia is of strategic importance for the Belt and Road Initiative—not only for geopolitics, but also for its strategic location and abundant natural resources. It's critical to understand cultural and environmental trends in time to respond to impending threats. Currently, empirical data is lacking on an international level. Sharing such data can promote work done on a national and regional level and also open doors to financiers looking to support capacity-building initiatives and solutions-based support projects. This can prove to be a useful resource for authorities in Central Asia to digest complex data into a format that can support integrated decision making.

Technological Advancements

With the development of the Belt and Road Initiative, it is also expected by participating countries that improvements will be made to information and communications technology (ICT) connectivity. Countries in Central Asia currently face a large digital divide. It is difficult to develop ICT infrastructure in the remote and rural areas because of desert and mountainous terrain (UNESCAP, 2017). These geographical factors have also limited Central Asia's development potential and integration into globalization as a result of insufficient international bandwidth and high transit costs to access international links (Kunavut et al., 2018). Thus, Central Asia could significantly benefit from the reinforcement of improved ICT infrastructure connectivity through the Belt and Road Initiative, and this could result in improved availability and affordability of broadband networks and services (Kunavut et al., 2018; UNESCAP, 2017). The technological advancements provided by ICT connectivity advancements would also likely help in better utilization of the DBAR Big Earth Data System. Improved ICT infrastructure and facilities could support activities in EO data collection, analysis, and modeling toward improved practices and methods in addressing environmental issues as well as coverage of earth observation in the region.

Barriers for the Implementation of the DBAR in Central Asia

Transboundary Water

Although the development of the Belt and Road Initiative is seen to have brought economic advancements to the Central Asia region, arguments have been presented in which the implementation of the Initiative could bring more pressure to the already existing prominent transboundary water and energy problems in the region. There is a need for better maintenance for delicate balance among increasing pressures on water volumes and quality, focus on hydropower production, irrigation and agricultural production, and environmental services for flood control and disaster management. Water cooperation among countries becomes essential to guide efficient basin level management that goes beyond administrative borders. Guo et al. (2016) mentioned the key internal cause of the complexity of the region's transboundary water and energy problems is the contradiction and

coordination between water and energy resources. Numerous contradictions in water and energy distribution and demand exist among the five countries, as well as an imbalanced supply–demand of water and energy resources. Such contradictions arise from the focus of countries to use water energy production, as is the case for upstream countries, or receive water for agricultural production, as is the case with downstream countries that depend on irrigation for farming. The accelerated promotion of the Belt and Road Initiative poses severe challenges against environmental sustainability and further socioeconomic development of involved regions, particularly considering the fear of creating environmental risks in countries with predominantly poor records of environmental governance, including the former Soviet republics (Tracy et al., 2017). Although cooperation efforts have been established in the past, the complicated historical background and profound domestic implications of deciding upon water for agriculture and energy production make these problems difficult to solve. Thus, in order to gain the opportunities from the initiative, the Central Asia countries along the BR urgently need to coordinate and cooperate effectively and align common economic interests toward protection of water and energy resources.

Meanwhile, according to Howard and Howard (2016), the fundamental concern of the initiative to the Central Asia region is that it would place a great burden on the region's water management system, which is already in a dysfunctional state. The rapid growth from implementation of the initiative may cause a serious long-term threat to the region's sustainable water management if the issue is not addressed. Countries in Central Asia need to recognize that the opportunity of economic successes presented by the Belt and Road Initiative relies on their ability to ensure that the region's water resources are managed sustainably. Although this is a difficult challenge, cooperation and commitment among the countries is required beyond what it is currently. Additionally, major reforms that attach true value to natural resources are necessary, as well as essential support from sound science and good hydrological data, both of which the region still currently lacks.

The introduction of the Big Earth Data framework within DBAR, therefore, could be used to provide data and scientific evidence at a scale that was previously not possible and which could then be used to inform the development of the Belt and Road Initiative in conjunction with transboundary water and energy resource management within the region. This is in line with the purpose of DBAR, which also seeks to address environmental and societal challenges with decisions and policies based on sound information through assessment and monitoring of terrestrial and marine ecosystems requiring precise, accurate, and timely observations and measurements of processes across a range of spatial and temporal scales by establishing integrated networks for collection and analysis of earth observation (EO) data (Guo et al., 2018a). This opportunity however, must be realized within the context of the above-mentioned constraints to ensure that whatever value can emerge from such an initiative is not canceled out by the negative effects of infrastructure projects.

In addition to transboundary water and energy issues faced by the Central Asia region, another transboundary environmental issue has the potential to gain from the DBAR Big Earth Data system. The vastness in data types, formats, and variables that the Big Earth Data framework allows could provide additional analysis and interpretation of methods used in the past.

Other Barriers to DBAR's Implementation in Central Asia

The Plan provides a useful framework for cooperation by governments, academics, and policymakers in Central Asia on issues like transboundary water cooperation. However, there are barriers to its implementation. First, there is the lack of accurate and timely data needed to populate the Platform. Many countries do not have the financial means or expertise to train academics and professionals in earth observation techniques or monitoring of air and water quality. In Central Asia, for example, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan have no earth-observing satellites or facilities for mass data processing. Local data is also "localized" and rarely upscaled to regional or international platforms because of security concerns, lack of professional capacities, or desire to collaborate with external partners (Guo, 2018).

In order for the Belt and Road Science Plan to be effective, it not only needs to help build technical infrastructure and professional capacities within Central Asian countries, but it must also deal with the issue of trust between the Chinese government and the Central Asian states. Knowledge platforms such as the Big Earth Data Platform of the BRI require trusting relationships with dependencies and share responsibilities between partners in Central Asian countries. The data provided to the Big Earth Data Platform by experts must be openly accessible to all, and the proposed use of that data must be transparent (Nativi et al., 2019). However, trust between China and Central Asian countries is a limited commodity. Territorial disputes with China were resolved with Kazakhstan (1999), Kyrgyzstan (1999), and Tajikistan (2002) only about two decades ago. Cross-border river management issues are yet to be resolved for the Ili and Irtysh rivers, which originate in China but play a critical role for agriculture in Kazakhstan. Moreover, the Uyghur diaspora has about 300,000 members mainly in Kazakhstan and Kyrgyzstan. The conflict between the Uyghurs in the Xinjiang province and the Chinese government heightened in 1996. As a result, the Chinese government forced both countries to distance themselves from any political ambitions of the Uyghurs. This left feelings in Central Asia that China was willing to involve itself in their domestic affairs (Peyrouse, 2016). Reliability of data included into the platform and concerns over how the data will be used could pose a challenge for the Chinese government in regard to this initiative, and trust-building measures must be taken if this plan is to be taken seriously by Central Asian countries. Security and ethical concerns of stakeholders and society as a whole must be taken into consideration. Since the Science Plan is only in its second phase of implementation and the launch of its deliverables will continue until 2026, there is ample room for its creators to respond to these challenges to ensure its effective implementation (Guo et al., 2020).

Another vector of considering trust is the approach taken by BRI outside of China. As Tracy et al. (2017) conclude, China's approach to dealing with its growing global environmental impact is double-sided. Critical environmental assessments of domestic infrastructure projects give the impression that China exemplifies key elements of ecological modernization considering environmental and social impacts of projects. Internationally, however, transboundary and overseas infrastructure development initiatives sponsored by the Chinese government under the BRI show very little consideration for strategic environmental assessment or environmental impact assessment (Tracy et al., 2017). The DBAR could prove timely to demonstrate the Big Earth Data system's capacity for environmental monitoring and its suitability to rectify and shift such impressions through the systematic analysis of data and its subsequent application to address sustainability challenges in Central Asia and more broadly BRI-participating countries.

Conclusions

The consequences of not fully understanding regional environmental changes based on robust data sources are severe. Regional security, economic growth, and overall well-being of citizens residing in Central Asia are directly linked with the sustainable use of cultural and natural resources. Without effective transnational water management in Central Asia we will see increased salinization, desertification, and human migration out of water-scarce regions (Qi & Kulmatov, 2008). Unemployment will be further exacerbated by inadequate and disjoined management of natural resources.

The need for an entity like the Big Earth Data Platform of the DBAR Science Plan is clear. Ongoing projects in Central Asia have sought to try and manage these challenges through Big Earth Data technologies and platforms. The challenges, however, range from general mistrust between partners, insufficient human capacities, and lack of technological resources to conduct data collection (Pohl et al., 2017). Trust has also been to a large degree been a barrier to cooperation between Central Asia and China as well. As was mentioned, it's important to ensure the reliability of data included in the platform and address concerns over how the data will be used. Trust-building measures must be taken if this Plan is to be taken seriously by Central Asian countries that participate in its implementation. Security and ethical concerns of stakeholders and society as a whole must also be taken into consideration. It's an important step that the Big Earth Data System will be open source, allowing users to freely obtain data. In addition to this, however, the Platform would be more openly received if the FAIRness framework, where data must be Findable, Accessible, Interoperable, and Reusable, were enacted (Wilkinson et al., 2016). Moreover, ethics and security concerns regarding how this data will be used and interpreted must also be openly presented to potential contributors. The creators of the Platform should seriously consider adopting this approach in future iterations of the Platform. Awareness raising and capacity building must also be extensively expanded, as most experts we addressed in the context of our research were not familiar with the Science Plan and had little understanding of its scope and implications. It is also suggested by the authors that an International Center for Excellence be established in at least one Central Asian country. This could provide on-the-ground support to ensure that this initiative is supported continually through a permanent research center that can provide in-the-field support, identify synergies and opportunities for collaboration, and raise awareness of this initiative.

Now is the right time for the Secretariat of the DBAR to involve Central Asian countries in this initiative. The DBAR Science Program entered Phase II in 2018 and concrete projects are being funded to address the DBAR Foci. Phase III will then begin in 2023 with the aim of having the Big Earth Data Platform fully functional by 2023. This provides a unique opportunity for the region and other countries in the BRI to link a strategically important region (Central Asia) to a broader platform that can support the sustainable management of cultural and natural resources. Systematic data is critical to this goal, and the DBAR Science Plan provides a strategic and timely opportunity to obtain it.

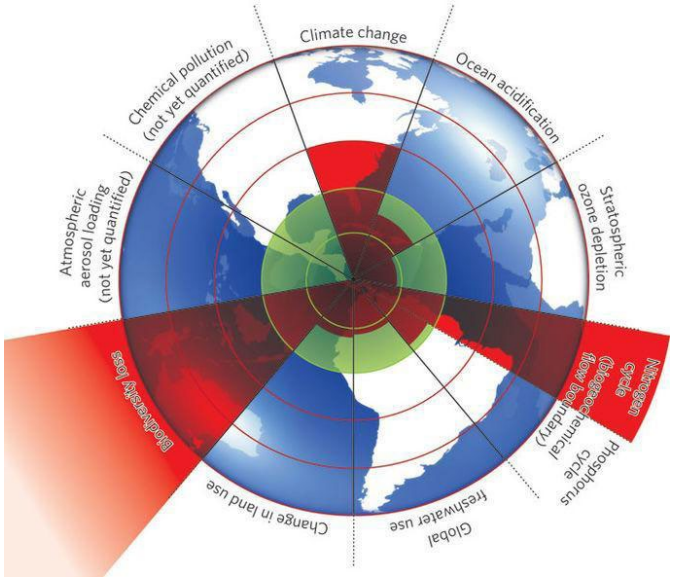


Figure 1. “A safe space for humanity”: ecological limits humanity must live within to survive. Red color indicates “overshoot,” meaning where we are today as a species. The green color indicates where we need to be in order to live sustainability. (Rockstrom et al., 2009)

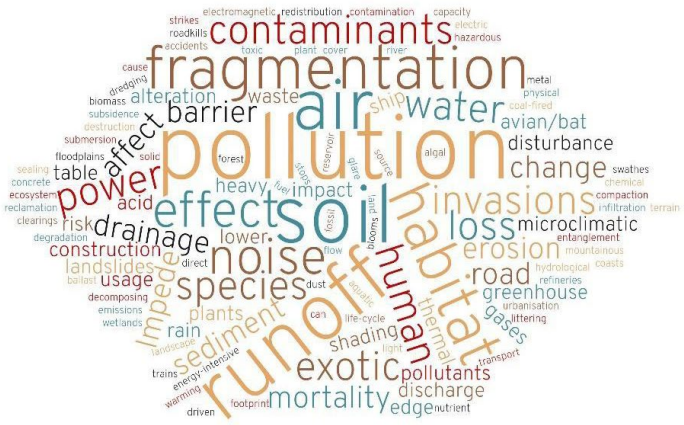


Figure 2. Key impacts on natural system from BRI infrastructure developments (generated from data from Teo et al., 2019)

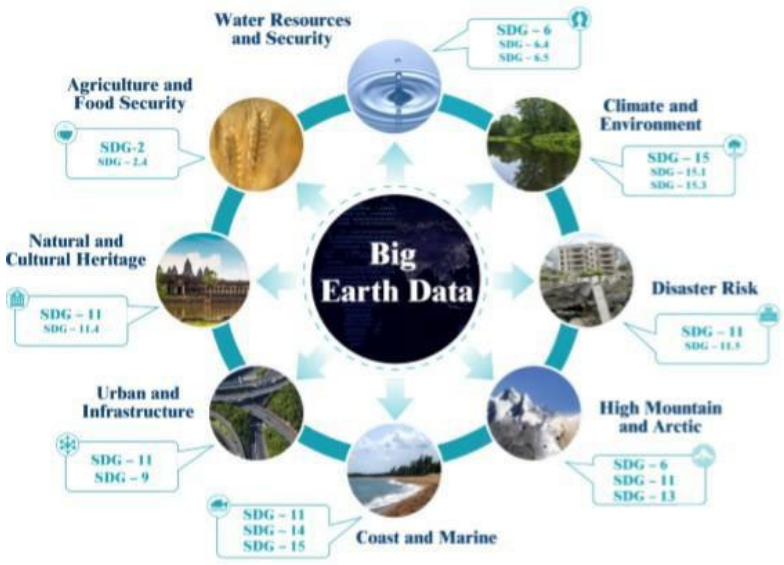


Figure 3. DBAR Foci (DBAR, 2017)

Figure 4. DBAR workflow (DBAR, 2017)

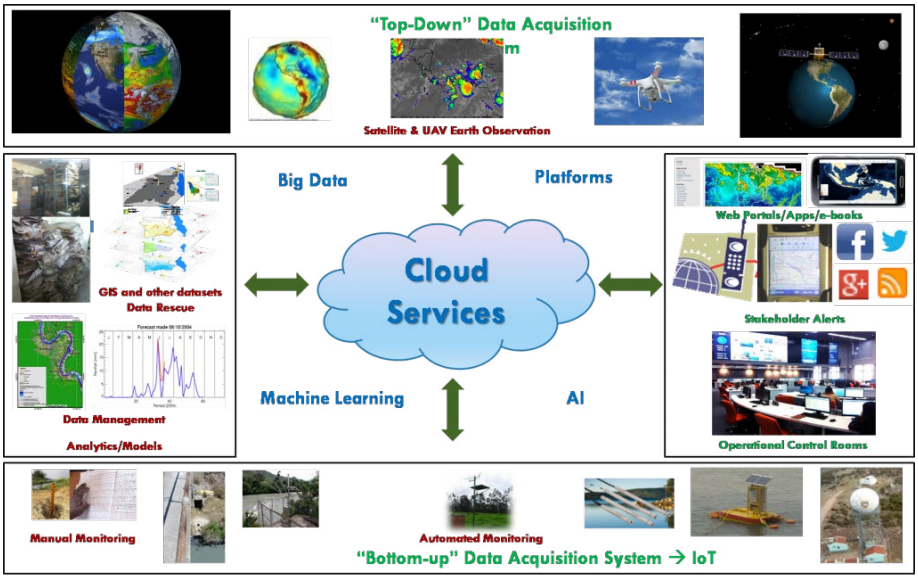


Figure 5. Initial concept of the Central Asia Climate Information Platform (CACIP) during program preparation (CAREC, 2018)

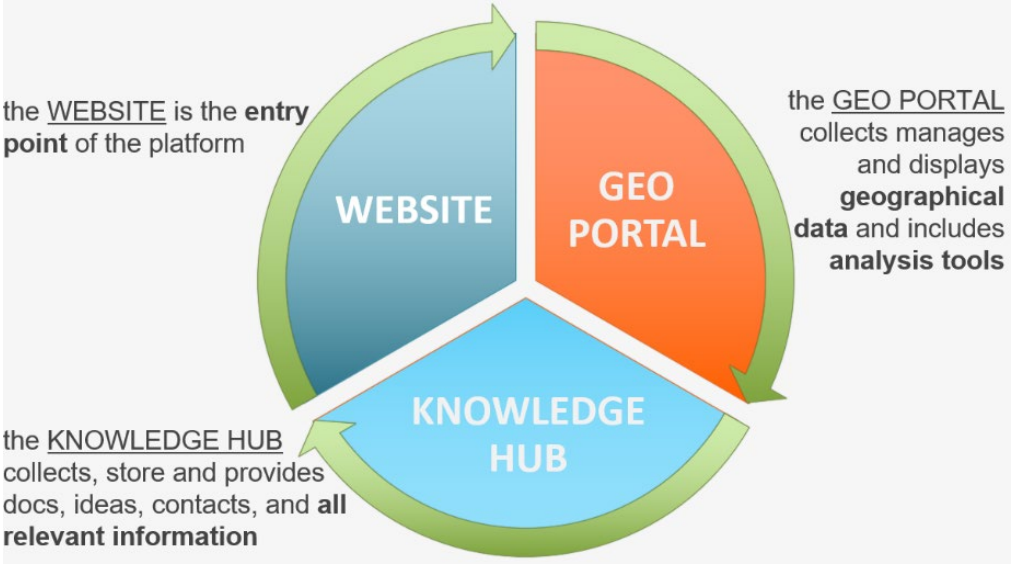


Figure 6. Logical architecture of the platform with three main blocks of information (Biradar & Akramkhanov, 2019)

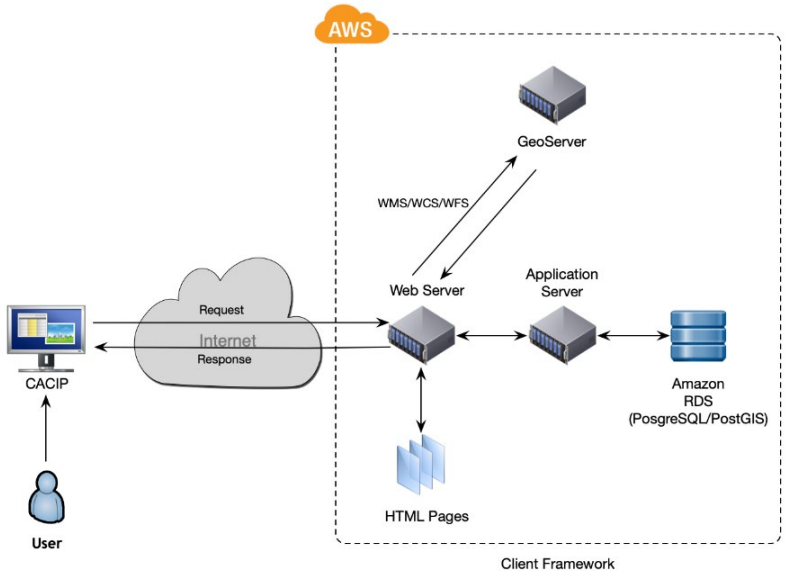


Figure 7. System architecture of the platform with information flow from server and cloud storage (Biradar & Akramkhanov, 2019).

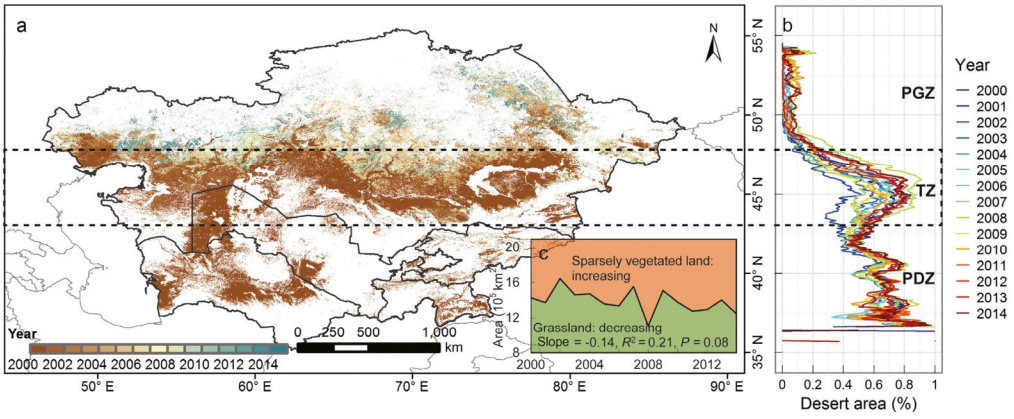


Figure 8. Changes in grassland desertification. (a) Spatial pattern of first occurrence of SDEVITGS-derived sparsely vegetated land for each pixel over the period 2000–2014; (b) distribution of SDEVITGS-derived sparsely vegetated land area along latitude gradients in each year; (c) inter-annual variation of SDEVITGS-derived grassland and sparsely vegetated land areas. PGZ, TZ, and PDZ in panel (b) mean persistent grassland zone, transition zone, and persistent desert zone, respectively. EVITGS means Enhanced Vegetation Index during thermal growing season. The resulting data is available from https://doi.org/10.5061/dryad.12bd9 (Zhang et al., 2018)

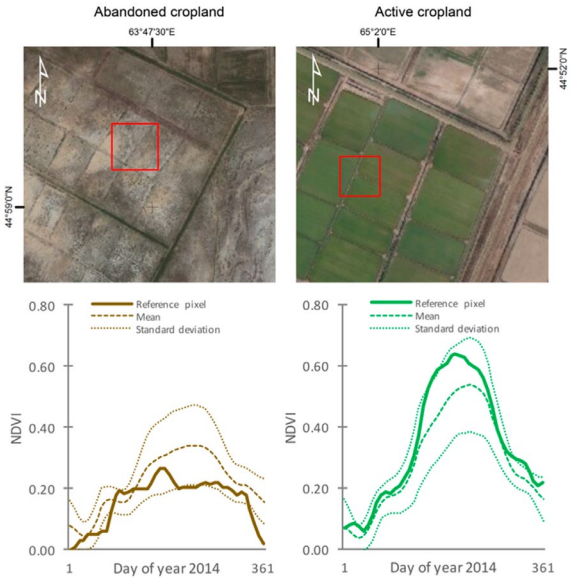


Figure 9. Abandoned (left) and active cropland (right) MODIS pixels (red squares). The graphs show the mean normalized difference vegetation index (NDVI) of all active and abandoned reference pixels (dashed signatures) and standard deviations (dotted lines). Bold lines represent the NDVI signatures of the two selected reference pixels (Löw et al., 2018; Google EarthTM, 2016)

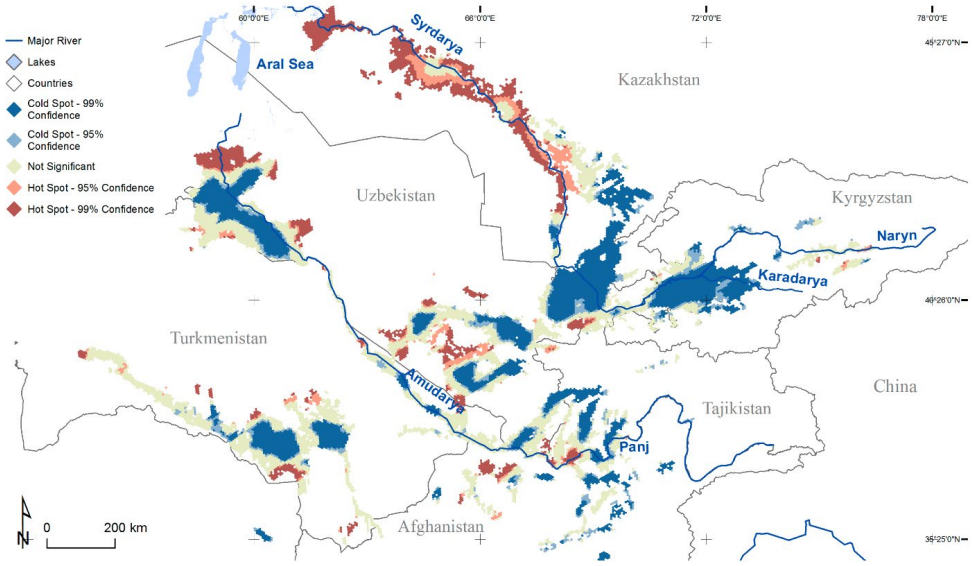


Figure 10. Hotspots of abandoned irrigated cropland (orange: 95 percent of confidence; red: 99 percent of confidence) and active irrigated cropland (light blue: 95 percent of confidence and dark blue: 99 percent of confidence) in the six countries of the Aral Sea Basin as derived by the stratified classifier method. (Löw et al., 2018)

Bibliography

Peyrouse, S. 2016. "Discussing China: Sinophilia and sinophobia in Central Asia." *Journal of Eurasian studies* 7: 14-23.

Birardar, C, and A Akramkhanov. 2019. *Country Consultations of Central Asian Climate Information Platform: Kazakhstan (CACIP).* Almaty : ICARDA.

CAREC. 2018. *Climate Adapation and Mitidation Program for Aral Sea Basin (CAMP4ASB). Development of a Central Asia Regional Climate Information Platform.* Almaty : CAREC.

CAS. 2019. *Big Earth Data in Support of the Sustainable Development Goals.* Beijing: Chinese Academy of Sciences .

Chamie, J. 2020. *World Population: 2020 Overview.* Accessed July 26, 2020. https://yaleglobal.yale.edu/content/world-population-2020-overview.

Crellin, C. 2018. *Global Fresh Water Availability Trends.* Accessed July 26, 2020. http://www.futuredirections.org.au/publication/global-freshwater-availability-trends-underlying-regional-security-threats/.

Eshonov, B., and I. Kamilov. 2013. *Urbanization in Central Asia: Challenges, Issues and Prospects.* Tashkent: UNESCAP. https://www.unescap.org/sites/default/files/Urbanization-in-CA-ENG.pdf.

2020. *European Bank for Reconstruction and Development: Belt and Road Initiatuve .* Accessed July 27, 2020. https://www.ebrd.com/what-we-do/belt-and-road/overview.html.

Farinotti, D., L. Longuevergne, G. Moholdt, D. Duethmann, T. Molg, T. Bolch, and S. Vorogushyn. 2015. "Substantial glacier mass loss in the Tien Shan over the past 50 years." *Nature Geoscience* 8: 716-722.

Fu, B H., F Yan, F. Yan, A. Zhang, P L. Shi, M. Ayinuer, and G. Xue. 2017. "Glacier retreat of the Tian Shan and its impact on the urban." *IOP Conference Series: Earth and Environmental Science* 74: 1-7.

Gore, A. 1998. "The Digital Earth: Understanding our planet in the 21st Century." Los Angeles: California Science Center. file:///C:/Users/User/Downloads/The_Digital_Earth_Understanding_Our_Planet_in_the_21st_Century%20(1).pdf.

Gou, L, H Zhou, Z Xia, and F Huang. 2016. "Evolution, opportunity and challenges of transboundary water and energy problems in Central Asia ." *Springerplus* 5: 1918.

Grooten, M., and R.E.A. Almond. 2018. *A Living Planet Report .* Gland: World Wildlife Fund.

Guo, H. 2015. "Inter-Comparison of High-Resolution Satellite Precipitation Products over Central Asia." *Remote Sensing* 76: 7181-7211.

Guo, H., S. Nativi, D. Liang, and M. Cragila. 2020. "Big Earth Data science: an information framework." *International Journal of Digital Earth* 13 (7): 743–767.

Guo, Huadong, Jig Liu, Yubao Qiu, Massimo Menenti, Fang Chen, Paul F. Uhlir, Li Zhang, et al. 2018. "The Digital Belt and Road Program in support of regional stability ." *International Journal of Digital Earth* 1-13.

Hamilton, S.H., S. ElSawah, J.H.A. Guillaume, A.J. Jakeman, and S.A. Pierce. 2015. "Integrated assessment and modeling: modelling: Overview and synthesis of salient dimensions." *Environ. Model. Softw* 64: 215-229.

Howard, K.W., and K.K. Howard . n.d. "The new "Silk Road Economic Belt" as a threat to the sustainable management of Central Asia's transboundary water resources." *Environmental Earth Sciences* 75: 976.

Huadong, G. 2018. "Steps to the digital Silk Road." *Nature* 554: 25-27.

Huadong, G., Z. Shirazi, L. Dong, and L. Jie. 2018. "DBAR – An International Science Program for the Belt and Road." *BCAS* 32 (3): 174-182.

Huadong, Guo. 2020. *Big Earth Data in Support of the Sustainable Development Goals.* Chinese Academy of Sciences .

Initiative, Digital Belt and Road. 2017. "A Science Plan for the Digital Belt and Road Initative (DBAR): An International Science Program for Sustainable Development Using Big Earth Data."

2020. *International Society for Digital Earth.* Accessed July 27, 2020. http://www.digitalearth-isde.org/society/54.

ISDE. 2020. "Inauguration of Big Earth Data." *International Society for Digital Earth.* Accessed July 27, 2020. http://www.digitalearth-isde.org/news/824#:~:text=Big%20Earth%20data%20refers%20to,complex%2C%20nonstationary%2C%20and%20unstructured.

Kunavut, K, A Okuda, and D Lee. 2018. "Belt and Road Initative (BRI): Enhancing ICT connectivity in China-Central Asia Corridor." *Journal of Infrastucture, Policy and Development* 2 (1): 116-141.

Li, J.-X., Y.-N. Chen, C.-C. Xu, and Z Li. 2019. "Evaluation and analysis of ecological security in arid areas of Central Asia based on the emergy ecological footprint (EEF) model." *Journal of Cleaner Production* 253: 664-677.

Low, F, and al. et. 2018. "Cropland Abandonment in the Aral Sea Basin with MODIS Time Series." *Remote Sensing* 10 (2): 159.

Masood, E. 2019. "All Roads Lead to China." *Nature* 569: 20-23. https://www.nature.com/immersive/d41586-019-01124-7/index.html .

Mohadjer, S, T Alan Ehiers, and R Benedick. n.d. "A Quaternary fault database for Central Asia." *Natural Hazards and Earth Systems* 16: 529-542.

Nativi, S, M. Santoro, G. Giuliani, and P. Mazzetti. 2019. "Towards a knowledge base to support global change policy goals." *International Journal of Digital Earth* 13 (2): 188-216.

Nativi, S., M. Santoro, G. Giuliani, and P. Mazzetti. 2019. "Towards a knowledge base to support global change policy goals." *International Journal of Digital Earth* 13 (2): 188-216.

Pohl, Benjamin, Annika Kramer, and William Hull . 2017. *Rethinking water in Central Asia: The costs of inaction and benefits of cooperation.* Regional Environmental Centre for Central Asia.

Qi, J. Jan 2008. "An overview of environmental issues in Central Asia." In *Environmental Problems of Central Asia and their Economic, Social and Security Impacts*, edited by J. Qi and K. Evered, 3-13. Springer.

Rebetsky, Y, O. Kuchai, N.A. Sycheva, and R.E. Tatevossian. 2012. "Development of inversion methods on fault slip data: Stress state in orogenes of Central Asia ." *Tectonophysics* 581: 114-131.

Reyer, C, I Otto, S. Ada, T Albrecht, F Baarsch, and M. Cartsburg. 2015. "Climate Impacts in Central Asia and their implications for development ." *Regional Environmental Change* 15 (8): 1639-1650.

Rockstrom, J., J. Steffen, and J. A. Foley. 2009. "A safe operating space for humanity." *Nature* 461: 472-475.

Roessner, S, H.-U. Wetzel, H. Kaufmann, and A Sarnagoev. 2005. "Potential Satellite Remote Sensing and GIS for Landslide Hazard Assessment in Southern Kyrgyzstan (Central Asia)." *Natural Hazards* 35: 395-416.

Sciences, Chinese Academy of. 2019. *Big Earth Data in Support of the Sustainable Development Goals. B: Chinese Academy of Sciences.* Beijing: Chinese Academy of Sciences.

Sciences, Chinese Academy of Sciences. 2019. *Big Earth Data in Support of the Sustainable Development Goals.* Chinese Academy of Sciences .

Summary, Digital Belt and Road Initative Science Plan. 2017. "A Science Plan for the Digital Belt and Road Initative (DBAR): An International Science Program for Sustainable Development Using Big Earth Data: Summary."

Teo, H. Chen, A. Mark Lechner, G. W. Walton, and Faith K.S. Chang. 2019. "Environmental Impacts of Infrastructure under the Belt and Road Initiative." *Envrionments* 6 (72): 1-22.

Tracy, E.F., E. Shvarts, E. Simonov, and M. Babenko . 2017. "China's new Eurasian ambitions: the envrionmental risks of the Silk Road Economic Belt." *Eurasian Geography and Economic* 58 (1): 56-88.

UNESCAP. 2017. "A Study of ICT Connectivity for the Belt and Road Initiative (BRI): Enhancing the Collaboration in the China–Central Asia Corridor. Bangkok: United Nations Economic and Social Commission for Asia and the Pacific."

Wilkinson, Mark D, Michel Dumontier, and Ijsbrand Jan Aalbersberg. 2016. "The FAIR Guiding Principles for scientific data management and stewardship." *Scientific Data* 3 (160018).

Xenarios, S., A. Gafurov, D. Schmidt-Vogt, J. Sehring, S. Manandhar, C. Hergarten, J. Shigaeva, and M. Foggin. 2019. "Climate change and adaptation of mountain societies in Central Asia: uncertainties, knowledge gaps, and data constraints." *Regional Envrionmental Change* 19 (1339-1352).

Yin, R. 1994. *Case Study Research: Design and methods .* Thousand Oaks: Sage Publications .

Zhang , G., C. Biradar, X. Xiao, J. Dong, Y. Zhou, Y. Quin, F. Liu, M. Ding , and R. Thomas. 2018. "Exacerbated grassland degradation and desertification in Central Asia during 2000–2014." *Ecological Applications* 28 (2): 442-456.

Zhang, Z.F., W.J. He, M An, D.M. Degefu, L Yuang, and X. WU. 2019. "Water security assessment of China's One Belt and One Road region." *Water* 11: 607.

About the Authors

Akmal Akramkhanov is a regional manager for Central Asia and the Caucasus at ICARDA. He has over 15 years' experience in natural resource management, with current research interests in knowledge management to promote sustainable land management, land degradation, sand and dust storm effects, climate change effects on agriculture. Earlier studies dealt with soil salinity mapping, conservation agriculture, greenhouse gas emissions. Dr. Akramkhanov holds a PhD in Agricultural Sciences from the Center for Development Research (ZEF) at the University of Bonn, Germany.

Brendan Duprey is the founding Director of the Sustainable Kazakhstan Research Institute. He is a practitioner and academic with over a decade of experience in the sustainability research and application sector. His research looks at environmental policy outcomes and how the implementation process can be streamlined to ensure they are achieved efficiently and effectively. Other research interests include global environmental governance, Sustainable Development Goals, environmental policy implementation, environmental ethics, educational reforms through education for sustainable development, outcome-based policy evaluation, and transformational change management.

Anna Gussarova is Director of the Central Asia Institute for Strategic Studies and holds the Chevening scholarship from King's College London War Studies. Gussarova has served as a visiting adjunct professor at the George C. Marshall European Center for Security Studies, the OSCE Academy in Bishkek and the German-Kazakh University in Almaty (courses on counterterrorism and cybersecurity). She has extensive practical experience and expertise in fieldwork and research, policy and strategy development, teaching, mentorship and facilitation, public policy and advocacy, counterterrorism, cybersecurity, strategic communication, information environment and irregular warfare research. Her academic interests include P/CVE and transnational security studies, Central Asia and Russia, political warfare, soft power, information operations, cyber hygiene, privacy, and political activism in non-democracies.

Nargis Kassenova is Senior Fellow at the Davis Center for Russian and Eurasian Studies (Harvard University), leading its Program on Central Asia. She is also Associate Professor at the Department of International Relations and Regional Studies of KIMEP University (Almaty, Kazakhstan), where she created two centers – Central Asian Studies Center (CASC) and China and Central Asia Studies Center (CCASC). She holds a PhD in International Cooperation Studies from the Graduate School of International Development, Nagoya University (Japan). Her areas of research include Central Asian politics and security, Eurasian geopolitics, China's Belt and Road Initiative and governance in Central Asia, and history of state-making in Central Asia.

Chia-Chi Liao is an alumna of King's College London Department of Digital Humanities. She has been working as a researcher in the Digisilk project led by Dr. Oreglia since 2019, focusing on the Chinese policies and financial investments related to the Digital Silk Road. Alongside her interest in the DSR, she is a human-computer interaction specialist.

Miranda Lupion was the 2019-2020 Innovation Fellow for the Imperiia Project, where she pioneered a novel approach to toponym extraction from Imperial Russian maps. More broadly, she is interested in the intersection of technology and international relations. In May, Miranda completed her M.A. in regional studies at Harvard. Her thesis analyzed Russian regulation of decentralized and privacy-promoting technologies. She earned her B.A. in Russian and international relations from the University of Pennsylvania.

Rustam Muhamedov is an independent researcher focusing on political and security developments in Central Asia and particularly in Turkmenistan. His research interests include digitalization and governance (digital authoritarianism), cybersecurity and (cyber)securitization, Central Asia and China relations, youth activism and societal security. He has broad and diverse academic and professional experience, currently being a Research Fellow of the Central Asia Azerbaijan Fellowship Program at the George Washington University. Rustam holds a Master's degree in International Relations from the OSCE Academy in Bishkek (2019).

Elisa Oreglia is a lecturer in Global Digital Cultures in the Department of Digital Humanities at King's College London. She studies the diffusion and appropriation of digital technologies in emerging economies, with a focus on China and Southeast Asia. Recently, she began Digisilk, a 5-year project supported by the European Research Council to study the expansion of the Chinese internet and related technologies in China's neighboring countries, in particular Cambodia, Myanmar and Kazakhstan. Dr. Oreglia holds a PhD in Information Management & Systems from UC Berkeley, and an MA in Asian Studies from the University of San Francisco.

Hongyi Ren is a student in King's College London Department of Digital Humanities. She is a researcher in the Digisilk Project led by Dr. Oreglia, and is particularly interested in understanding Alibaba's commercial expansion in Central Asia and in emerging economies.

Cian Stryker was the 2019-2020 Innovation Fellow for the Davis Center Program on Central Asia with a research focus on the development of digital surveillance within Central Asia. He is pursuing a Master's in Russian, Eastern European, and Central Asian studies at Harvard University. Cian also previously interned with the UN's World Food Programme in Dushanbe, Tajikistan as well as the Westminster Foundation for Democracy in Bishkek, Kyrgyzstan. He received a Bachelor's of Philosophy at the University of Pittsburgh in Political Science and Russian, Eastern European Studies.

ISBN 978-0-578-93435-8