Importing Chinese Surveillance Technology: Are Central Asian States on the Path to Digital Authoritarianism?

A thesis presented

by

Cian Stryker

to

The Standing Committee on Regional Studies–Russia,

Eastern Europe, and Central Asia

in partial fulfillment of the requirements

for the degree of

Master of Arts

in Regional Studies–Russia, Eastern Europe, and Central Asia

Harvard University

Cambridge, Massachusetts

April 2021

Table of Contents

Note: *The content from pages 24-72 and all figures will largely be published in a chapter for an upcoming report in the Spring of 2021. This content has not been used for any classes at Harvard University and were written primarily for this thesis.*

Abstract

Many states throughout the world have rapidly developed their digital surveillance networks over the last few years by building Safe City projects that utilize advanced facial recognition technology. While this is not surprising within the developed world, the developing world has been able to access advanced surveillance technology largely by purchasing that technology from Chinese Information Communication Technology companies, who are operating within the framework of the Belt and Road Initiative. This thesis explores how regime type, state-capacity, and regulatory environments affect the potential for developing digital surveillance capacity by examining surveillance networks in four Central Asian states and Ecuador. I find that state-capacity has a positive relationship to the development of digital surveillance capacity, while democratization has little impact when paired with an ineffective regulatory environment.

Introduction

Today states across the globe utilize technology to monitor domestic activity in every way imaginable. States monitor emails, listen in on phone calls, collect purchasing history data, and use facial recognition technology (FRT) to monitor behavior in public spaces. Facial recognition technology equipped with artificial intelligence capabilities—perhaps the most Orwellian method of modern surveillance—is the prime example of a technology that exponentially improves suppressive capacity. These systems allow states, using relatively modest amounts of human labor, to immediately identify individuals in public spaces and notify authorities. They accomplish this through the extensive use of closed-circuit television (CCTV) cameras, drone surveillance, and extensive bioinformatics registries. City-wide surveillance systems that use FRT are often known as Safe City projects and are present in hundreds of cities across the world in both developing and developed regions.

Safe Cities best represent the extent of modern surveillance technology and the possibilities the model of governance known as Digital Authoritarianism, which is "the use of digital information technology to surveil, repress, and manipulate domestic and foreign populations".[1] Digital Authoritarianism is a poorly defined term, however, because it describes the broad use of technology to control a citizenry, which can include the fragmentation of the internet, corporate espionage, disinformation, and the use of surveillance technology.[2] This term is often used in reference to mass-surveillance systems within China, but the use of widespread surveillance technology exists in both authoritarian and democratic.

---

[1] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (Brookings, August 26, 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.
[2] "Promote and Build: A Strategic Approach to Digital Authoritarianism" (Center for Strategic and International Studies, October 15, 2020), https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.

Democratic regimes interact with state surveillance differently than authoritarian regimes and are often resistant to developing intrusive surveillance apparatuses on a mass scale. Authoritarian regimes lack this resistance, but they often have other inhibitions to developing such systems, specifically state-capacity. In both cases, effective regulations could greatly impede the development and use of wide-spread state-surveillance. State interactions with surveillance technology is therefore affected by regime type, state-capacity, and regulations. Digital Authoritarianism is only possible within highly advanced, developed, authoritarian regimes that are actively developing and utilizing advanced surveillance technology, often relying on the Safe City model.

Most countries, therefore, are unable to effectively develop Digital Authoritarianism independently. Chinese Information Communication Technology (ICT) companies, however, are now exporting advanced surveillance technology and Safe City projects for affordable prices, which has caused imported digital surveillance technology to become common place throughout the world. This has not resulted in the development of Orwellian Digital Authoritarianism in in every society, but it has resulted in many developing countries quickly developing their surveillance capacity and their potential for achieving Digital Authoritarianism.

Considering this, it is important to understand how the development of digital surveillance capacity might differ between countries and what factors affect that development. As mentioned before, there are three factors that substantially affect the development of digital surveillance and the potential for Digital Authoritarianism: regime type, state-capacity, and regulatory environment. Regime type because democratic regimes tend to mitigate the full development of digital surveillance through greater transparency and public resistance. State capacity because the development, installation, and management of country wide surveillance

systems requires capital, technical expertise, and effective governance. Finally, regulatory environment because effective regulations can greatly limit or legitimize the use of digital surveillance by the state. Regulations, however, are in turn affected both by regime type and state-capacity and so are somewhat in between the two. How these three factors impact the potential for Digital Authoritarianism is most easily seen in analyzing the extent of digital surveillance development in developing countries actively importing digital surveillance technology from Chinese ICT companies.

In this thesis, I examine and compare the development of digital surveillance capacity in Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan, and Ecuador. Using those five cases I will analyze the extent of imported digital surveillance in each country to see whether regime type, state-capacity, and regulatory environment meaningfully impact the potential for Digital Authoritarianism. It is clear that digital surveillance apparatuses are developing and quickly expanding in Central Asia. I hypothesize, however, that low state-capacity mitigates the scale and sophistication of digital surveillance because these systems still rely on effective state institutions and access to capital. I also hypothesize that more democratic regimes mitigate the use of digital surveillance because higher transparency and accountability within democratic states incentives the creation of regulations to protect private citizens' data and civil liberties.

Background and Conceptual Framework

Digital Authoritarianism: China as a Model and Exporter

The Chinese state has developed advanced digital technology to create a surveillance apparatus in which the government's position is far more secure than ever in the past. The Chinese government uses facial recognition technology, biometric registries, internet monitoring, and internet-based disinformation campaigns to control its citizenry.[3] The apex of China's use of surveillance technology can be seen in their creation of the "Social Credit System" that quantifies citizens' behavior. It is also clearly seen in the repression of the Uighur minority in Xingang where the Chinese government has used facial recognition technology to help systematically gather Uighurs into reeducation camps.[4] China represents the possibilities and extent to which authoritarian regimes can build and utilize surveillance technology. China is likely the only country in the world that can be said to have a Digital Authoritarian regime.

While China is able to domestically develop Digital Authoritarianism, not all authoritarian regimes are capable of that feat. Regimes differ tremendously in their ability to implement wide scale surveillance. Most developing states, for example, lack the technological and economic capacity to develop mass surveillance systems, but would benefit from the use of digital tools. With advanced surveillance tools a country can greatly expand its state-capacity, improving its ability to respond to crime, for example, but at the same time it allows that country to drastically increase its suppressive capacity. Considering the benefits, therefore, there is a massive demand for digital surveillance technology with both state actors and private companies selling

[3] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (Brookings, August 26, 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.
[4] Robert Mendez, "The New Big Brother: China and Digital Authoritarianism" (Committee on Foreign Relations United States Senate, July 21, 2010), https://www.foreign.senate.gov/download/2020-sfrc-minority-report_-the-new-big-brother---china-and-digital-authoritarianism.

installment, management, and long-term maintenance services. This market has grown rapidly within the last decade and China yet again enjoys significant market share as the largest global exporter of digital surveillance technology in the world.[5] While there are other countries that export digital authoritarian tools such as Russia, who exports internet monitoring technology, China is the most influential exporter in the sphere of surveillance technology and cooperates with a quantity of countries on a scale largely impossible for Russia.[6]

China became the largest exporter of surveillance technology in part through the Belt and Road Initiative (BRI), and more specifically, its subsidiary known as the Digital Silk Road (DSR). Although BRI was formally announced in 2013 by President Xi in Astana, Kazakhstan, the Chinese government began funding infrastructural projects in developing countries beginning in the early 2000's.[7] BRI is a massive investment strategy with a focus on infrastructure projects whose goal is to create a world-wide market in which China plays the leading role. This initiative now extends to over sixty-eight countries and impacts over sixty five percent of the world's population.[8] Its scale has only expanded in scope since 2013 as China's economy continues to grow.

The Digital Silk Road became the name for any digital infastrucutral aspects of BRI. Most activity considered part of the DSR deals with exporting common technology such as internet and telecommunications equipment. In addition, however, China has also become the leading exporter of surveillance systems that use AI capabilities to quickly identify criminal actions,

---

[5] Yiju Liu and E.F., Avdokushin, "Forming the Foundations of the 'Digital Silk Road,'" *Miir Novoi Ekonomiki* 13, no. 4 (2019): 62–71;
Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.
[6] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (Brookings, August 26, 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.
[7] Adrian Brona, "One Belt, One Road: New Framework for International Relations", *Polish Journal of Political Science* 4, no. 2 (2018): 57–76.
[8] Ibid

collect data, and report to governmental authorities.[9] Full-scale surveillance systems that include facial recognition cameras, high speed internet, data management systems, and data storage systems are commonly referred to as "Safe City" packages and have become a specialty of Chinese Information and Technology (ICT) companies.[10] Safe City packages equipped with facial recognition technology represent the cutting edge in surveillance capacity available today and they are sold wholesale by Chinese ICT companies ostensibly operating within the broad, but undefined framework of the DSR.

Regimes across the world have bought Safe City packages from the Chinese government, often relying on loans also from the Chinese government to underwrite the installation and management. Most authoritarian regimes want to drastically improve their suppressive capabilities, but until recently they could not achieve these goals themselves. Developing states usually lack the strong domestic technology sectors that would allow them produce advanced surveillance systems or implement them on a wide scale. Chinese ICT companies make these systems available and affordable. Regimes that lack the technical ability to implement facial recognition software or properly manage the data can now outsource this labor to Chinese ICT companies. Countries such as Ecuador, for example, have invested heavily in Chinese built Safe City projects and now report significant reductions in crime rates ostensibly because of their

[9] Yiju Liu and E.F., Avdokushin, "Forming the Foundations of the 'Digital Silk Road,'" *Miir Novoi Ekonomiki* 13, no. 4 (2019): 62–71.
Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.
[10] Alvaro Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets" (Barcelona, Institut Barcelona Estudis Internacionals, 2017).

use.[11] Even developed countries are increasingly relying on Chinese ICT companies to create Safe City projects because of the low price and obvious benefits to local governance.[12]

Every state, regardless of economic development, can now develop and improve its surveillance capacity, but reliance on Chinese surveillance technology does not come without certain risks. Data breaches and hidden backdoors have been frequently found in the hardware and software of Chinese ICT companies.[13] These risks, however, have not prevented the popularity of importing surveillance technology growing rapidly over the last ten years.[14] The expansion of sophisticated surveillance technology poses a variety of risks to both democratic and authoritarian regimes, risks that are exacerbated within the developing world.[15] The adoption of digital surveillance tools and techniques within democratic regimes is eroding public trust, personal privacy, and civil liberties. In authoritarian regimes, surveillance technology is increasing regime stability and suppressive capacity.[16]

Digital Infrastructure and Technical Background

Since the most common form of exported digital technology from Chinese ICT companies is the Safe City project, examining how it operates and its technological components is necessary

[11] 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/.
[12] Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.
[13] Ibid
[14] Adrian Shahbaz, "The Rise of Digital Authoritarianism" (Freedom House, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.
[15] "Promote and Build: A Strategic Approach to Digital Authoritarianism" (Center for Strategic and International Studies, October 15, 2020), https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.
[16] Marlies Glasius and Marcus Michaelsen, "Illiberal and Authoritarian Practices in the Digital Sphere" 12 (2018): 3795–3813.

to analyze modern digital surveillance practices. Safe Cities' fundamental component is the internet, which essentially is comprised of computers and connections.[17] Computers, routers, cloud storage systems, printers, and cameras are all computers. Fiber optic cables, ethernet cords, and mobile networks such as 4G or 5G are connections.[18] The entirety of the digital world can fit into these two categories. Subcategories, such as software, enhance a computer's ability to perform operations. Safe City packages are simply a more complicated extension of this concept.

It is important, therefore, to understand who provides the internet in any given state. China's Digital Silk Road involves building underwater fiberoptic cables to connect developing parts of the world to the internet.[19] It also responsible for developing and selling 5G technology. Exporting these systems creates advantages for China, such as market capture in importing regions. Much of the internet in Central Asia, for example, is provided or supported by Chinese ICT companies investing in cellular networks and fiberoptic cables.[20] This means that future digital technology on a large scale, such as Safe City projects, will be easier to integrate seamlessly into Central Asian digitals networks because the region has experience working with and relying on Chinese ICT companies. Central Asia will then become somewhat reliant on China for digital technology and China will enjoy a larger and larger share of the regional technology market.

Safe City projects are a scalable addition to this already-installed infrastructure. It is a system of cameras that use AI powered facial recognition technology, a management center, a data

---

[17] Bruce Schneier, "Security and the Internet of Things," *Schneier on Security*, https://www.schneier.com/blog/archives/2017/02/security_and_th.html.
[18] Ibid
[19] Priscilla Moriuchi, "The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture," *Recorded Future*, June 10, 2019, https://www.recordedfuture.com/huawei-technology-risks/.
[20] Sarah O'Meara, "Taking the Silk Road to High-Tech Growth," *Nature* 563, no. 7729 (2018): S25–27.

storage center, and connections between these three main components.[21] In simpler terms, a Safe City project combines computers as cameras, computers for storage, computers for management, and wires and/or wireless connections to allow functionality.

The cameras of the Safe City project are the most visible aspect of the entire system. These are closed-circuit television (CCTV) cameras installed with FRT technology. CCTV cameras can exist without FRT and this was the most common form of surveillance before FRT became viable.[22] The limitation of a typical CCTV camera is that it cannot process information independent of a human operator. It functions like any camera would. It can record videos, send them to a management center where the video can be watched, and then that video can be stored for future use. Facial recognition technology functions in a similar manner, but with fundamental difference: it can operate without of operators.[23] FRT uses complex algorithms that measure facial structures and license plates. It measures and identifies the unique information of everything that passes in view. If it has access to a citizen registry that includes images and/or license plates, it will automatically match data.[24] With CCTV systems, individual employees had to manually shift through immense amounts of information. FRT does the same work almost instantaneously.

A Safe City project requires data management, storage, and connections. Management often takes the form of data processing centers. Data storage involves data centers where computers store the data gathered by the system. Data management and storage is now often Cloud based, which requires the use of physical computers, but computers that could be located almost

[21] Vlado Damjanovski, *CCTV: From Light to Pixels*, 3rd ed. (Waltham, Massachusetts: Butterworth-Heinemann, 2014).
[22] Ibid
[23] Serign Modou Bah and Fang Ming, "An Improved Face Recognition Algorithm and Its Application in Attendance Management System," *Elsevier*, no. 5 (2020).
[24] Ibid

anywhere in the world.[25] It is not necessarily the case, therefore, that a Safe City's data streams must be managed and stored within the same country the project is located. Finally, the connections in a Safe City project rely on wireless connections such as 4G and 5G, as well as conventional, physical wires. Depending on who owns and operates these management sites, storage sites, and especially the connections, data can be easily accessed.

Data security concerns aside, Safe City projects function using scalable technology. The capabilities of such a system are enormous. If combined with enough cameras and surveillance drones, Safe City projects can accurately measure any and all activity within their operational area. Considering the skill and level of sophistication of Chinese ICT companies, the technical limit on how these systems can be used depends on human error, the lack of capital to expand the system, or attacks—both physical and cyber—against the systems themselves. Another fundamental limitation to how a state uses Safe City projects, however, is whether a government is limited by its regime, state-capacity, and/or regulations.

Regime Type and Digital Surveillance

Regime type inherently affects how digital surveillance is developed and managed within any state. Similarly, society's interaction with surveillance in any given country is heavily dependent on regime type. Regime type, however, is difficult to classify since there are a range of regime classifications with a variety of distinguishing features. In general, however, regimes

[25] M. Lakshimi Neelima and M Padma, "A Study on Cloud Storage," *International Journal of Computer Science and Mobile Computing* 3, no. 5 (May 2014): 966–71.

exist on a spectrum between authoritarianism and democracy.[26] Within that spectrum there is a wide range of possibilities. For example, many authoritarian regimes differ as much between other authoritarian regimes as they do from democracies, with the reverse equally true as well.[27] For the purposes of this thesis though, the nuanced differences between regimes is less important than their overall placement on the spectrum, in other words, whether they are closer to authoritarianism or democracy.

Authoritarian and democratic regimes differ from each other in their relationship to security and surveillance. An authoritarian regime is characterized in part by centralized government power maintained by political repression and a range of social controls, including the military and the government bureaucracy.[28] In other words, the political sphere in a country is under the regime's direct control and the security apparatus is used to monitor and control the political sphere. In democratic states, the political sphere, with guaranteed civil liberties, exists largely separately from the regime.[29] In democratic states, therefore, there are limits to how a state can use surveillance. Most people have an aversion to being surveilled and so in democratic regimes there is often public resistance to extensive domestic state surveillance which results in legislation, regulations, etc. that limit domestic surveillance. This often disincentives, mitigates or outright prevents the creation of widespread, intensive domestic surveillance. Since state surveillance systems are tools of regime bureaucracy and often the security apparatus, authoritarian regimes use surveillance to suppress the political sphere. Without a separate political sphere, a citizenry has less leverage against the government's use of domestic

[26] Barbara Geddes, "What Do We Know About Democratization After Twenty Years?," *Annual Reviews* 2 (June 1999): 115–44.
[27] Ibid
[28] Theodore Vestal, *Ethiopia: A Post-Cold War African State*, Non-Series (Santa Barbara: ABC-CLIO, Praeger, 1999).
[29] Ibid

surveillance. In comparison to democracies, authoritarian regimes have far more options and opportunities to develop and use widespread domestic surveillance.

The NSA's use of widespread surveillance in the US and the Chinese government's creation of a surveillance state are examples of two highly developed states utilizing widespread surveillance technology, but they differ strongly due to their regime types.[30] The extent of the US's use of surveillance is much smaller than China's largely due to its democratic government. While the US government uses surveillance, it cannot develop widespread, invasive surveillance apparatuses to the extent that China has without pushback from civil society and the general public. China, however, is the prime example of the level of sophistication and societal penetration that is possible if a regime decides to invest entirely in the creation of Digital Authoritarianism. What differentiates the two is not the sophistication of technology, but the scale of use, regulations, and the willingness of the government to intrude upon the rights of their citizens.

State-Capacity and Digital Surveillance

Beyond regime type, state-capacity impacts the potential for developing highly effective digital surveillance. State-capacity, however, is difficult to define with a variety of measures and theoretical models potentially applicable.[31] State-capacity can encompass economic development, international security, stability, military capacity, and social welfare, to name only

[30] Robert Mendez, "The New Big Brother: China and Digital Authoritarianism" (Committee on Foreign Relations United States Senate, July 21, 2010), https://www.foreign.senate.gov/download/2020-sfrc-minority-report_-the-new-big-brother---china-and-digital-authoritarianism.

[31] Nafisa Akbar and Susan L. Ostermann, "Understanding, Defining, and Measuring State Capacity in India: Traditional, Modern, and Everything in Between," *Asian Survey* 55, no. 5 (2015): 845–61.

a few possibilities.[32] In order to use the term state-capacity, therefore, it is important to take the context of the issue into consideration. For the purposes of this thesis, only the dimensions of state-capacity that affect the ability of a state to implement, manage, and expand a surveillance system are pertinent.

With this context in mind, I argue that the ability of a government to expand and maintain an imported surveillance system is dependent on administrative capacity and economic development.[33] Without efficient administrative capacity, importing surveillance technology is insufficient. Unless a government decides to entirely rely on foreign companies to manage and expand their surveillance networks forever, the government in question must be capable of management and long-term expansion. There are cases, for example, of governments that invested in developing Safe City projects through Chinese ICT companies, but were unable to sustain the projects after the initial installment.[34] Similarly, without economic development a country cannot afford the day-to-day management costs associated with Safe City projects or be able to fund expansions in the future. State-capacity as defined by these two dimensions, therefore, is a fundamental factor in a country's potential for developing digital surveillance capacity.

---

[32] Ibid

[33] Cullen S Hendrix, "Measuring State Capacity: Theoretical and Empirical Implications for the Study of Civil Conflict," *Journal of Peace Research* 47, no. 3 (May 1, 2010): 273–85, https://doi.org/10.1177/0022343310361838.

[34] Aamir Saeed, "Islamabad's Multi-Million-Dollar 'Safe City Project' Fails to Deliver Results," Arab News PK, December 4, 2017, https://www.arabnews.pk/node/1203516/metropolitan.

Regulations and Digital Surveillance

Another factor that affects the potential for Digital Authoritarianism is the regulatory environment within a country that addresses how surveillance technology is used and what protections are afforded to the citizenry. Regulations have been defined as governmental intervention in the affairs of society and laws that implement such interventions.[35] What the government can do, what it cannot do, and what it must enforce, are all things defined by regulations. Often, governments create regulations to define what rights citizens have and what role the government plays in guaranteeing those rights. Effective regulations, therefore, help create cohesion between the state and society through legitimizing and defining their social contract.[36] Regulations operate very differently, however, within various regime types.

As stated before, democratic regimes differ from authoritarian regimes in that they have strong regulatory environments that limit the use of digital surveillance. In authoritarian regimes, however, regulations are created that often legitimize the use of state control and suppression.[37] In either regime, it is possible for proper regulations to exist, but lack any implementation or enforcement mechanisms. Effective regulations, therefore, are dependent on both regime type and state-capacity, i.e. a country must be willing to create regulations that limit and define the state's use of surveillance, but it must also have the state-capacity to enforce those regulations.

In examining digital surveillance it is important to address the regulatory environment that has been developed to either limit the state's use of surveillance or legitimize its abuse. Beyond that, it is important to also analyze whether the regulations in question are actually followed,

---

[35] John Stuart Mill, *Principles of Political Economy*, 1848.
[36] Tamir Moustafa, "Law and Courts in Authoritarian Regimes," *Annual Review of Law and Social Science* 10 (2014): 281–99.
[37] Ibid

enforced, or meaningfully impact the state's behavior. How regulations are developed can offer insight into whether a regime is legitimately concerned with protecting its citizenry's rights, whether they want to create a legal structure in which the regime is given the right to abuse surveillance, or whether they adopted regulations that sound legitimate, but the state has no intention to enforce.

There is a major issue worldwide in that little legislation defends personal data from state intrusions, which is true even within the developed world.[38] State obligations to protect personal data differ from country to country and can almost always be circumvented in the interest of national security. The lack of standardization of legal protections for data is the greatest roadblock to separating the state from the everyday lives of citizens. This is because the digital sphere is now global in nature, meaning surveillance is no longer the tool of a single state or even necessarily the tool of governments.[39] Transnational corporations provide internet, technology, and hardware that allows digital life to function and extend beyond national borders. This creates a complicated network of digital infrastructure that allows the internet to function globally, but which in turn opens avenues for state surveillance.

Some states, however, have attempted to develop legislation to protect citizens' data from companies and governments accessing and misusing their data. Of particular note is the European Union's General Data Protection Regulation (GDPR) which is considered a gold

---

[38] Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8 (2014): 121–44;
A notable exception to this statement would be the European Union's General Data Protection Requirement legislation, which is an attempt to protect people from the misuse of their data by companies and governments. It is far too early, however, to rate its effectiveness as a regulatory model.

[39] Kirstie Ball, *Routledge Handbook of Surveillance Studies* (Routledge, 2012).

standard for data privacy regulation.[40] Strong regulations protecting digital privacy rights were almost non-existent before GDPR, which was passed in 2018. The EU has strong informal political practices to ensure that regulations are respected by state authorities, who will in turn force compliance from private companies.

Many states have adopted similar legislation to GDPR, but many also lack the political practices that ensure compliance. It is important to note that even the GDPR contains clauses that allow European governments to access and use the data of citizens without permission, often for national security reasons. The effectiveness of GDPR, therefore, relies on the political norms in European society to ensure the EU does not abuse those stipulations. These norms often do not exist in the developing world. In many authoritarian regimes, the interpretation of national security is broad enough to render personal privacy regulations effectively useless. In democratic, but developing states, personal privacy regulations may be legitimate, but state-capacity is weak to the point that regulations are often ignored by the government and corporations entirely. Overall, therefore, regulatory environment is an important factor for the development of surveillance capacity, but it in turn is greatly impacted by regime type and state-capacity.

[40] Samuel Greengard, "Weighing the Impact of GDPR: The EU Data Regulation Will Affect Computer, Internet, and Technology Usage within and Outside the EU; How It Will Play out Remains to Be Seen," *Communications of the ACM* 61, no. 11 (November 2018): 16–18, https://doi.org/10.1145/3276744.

Methodology

To study how regime type, state-capacity, and regulatory environments affect the potential for Digital Authoritarianism, this thesis will examine five countries: Kazakhstan, Uzbekistan, Tajikistan, Kyrgyzstan, and Ecuador in that order. The first three will be used to test state-capacity and economic development's effect within authoritarian regimes, while Kyrgyzstan and Ecuador will explore the same but within democratic regimes. All five cases will also be used to analyze the effect of regulatory environment.

The four Central Asian countries in question have all begun to heavily invest in developing their surveillance capacity by importing technology. Kazakhstan, Uzbekistan, and Tajikistan are authoritarian regimes that exist on a high-to-low spectrum of state-capacity and economic development. All three began developing surveillance capacity by relying on Chinese ICT companies along a similar timeline. Kyrgyzstan, however, is the sole semi-democratic country in the region and has a comparable level of state-capacity and economic development to the region. Kyrgyzstan also began developing its Safe City projects around the same time. Using Kyrgyzstan, therefore, offers an opportunity to examine how regime type affects the development of Digital Authoritarianism while controlling for state-capacity and economic development.

To improve the robustness of the study, I include Ecuador into my analysis. Ecuador is also a democratic state, which has comparable levels of state-capacity and economic development to the Central Asia cases. Ecuador has also had longer exposure to imported digital surveillance technology than the Central Asian cases because Chinese ICT companies used Ecuador as a pilot

program to test the feasibility of exporting surveillance as a commodity. Finally, all five cases have similar regulatory environments surrounding personal data privacy and surveillance.

Each country will begin with an overview of regime type and state-capacity. Then I will analyze the extent of digital surveillance development by exploring Safe City projects and overall digital infrastructure. Following this, I will explore the regulatory environment in each country surrounding surveillance and personal data privacy. Finally, I will discuss the likely trajectory for digital surveillance capacity and each country's potential to develop Digital Authoritarianism. I use primary journalistic sources from the region, many of which are in Russian, to analyze the technologies involved, foreign companies present, changes in legislation, and adaptations in governance. To the extent possible, I will explore surveillance management practices and insecurities in the systems.

For the analysis of regime type and state-capacity I will use descriptive statistics including economic climate, regime type, and indictors of governance depicted through visualizations.[41] Economic development will be represented using GDP data from the World Bank.[42] Regime descriptions will be taken from Freedom House's "Freedom in the World" Index, which is measured on a 100 point scale.[43] Administrative capacity will be measured using "Rule of Law" and "Government Effectiveness", which are two of the six indicators the World Bank uses for analyzing governance, both of which are also measured on a 100 point scale.[44] 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,

[41] All visualization code can be found at https://github.com/CianStryker/Thesis_Project.
[42] "World Bank Open Data | Data," accessed May 15, 2020, https://data.worldbank.org/.
[43] "Freedom in the World," Freedom House, accessed May 15, 2020, https://freedomhouse.org/report/freedom-world.
[44] "WGI 2019 Interactive > Documentation," accessed May 15, 2020, https://info.worldbank.org/governance/wgi/Home/Documents.

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.

With this approach, I hope to address my overall research questions and test my hypothesis that low state-capacity and democratic regime types paired with effective regulations mitigate the scale and intrusiveness of digital surveillance, ultimately preventing the development of Digital Authoritarianism. Beyond that, my goal is to predict what digital surveillance may look like in Central Asia in the future, based off of how it has developed within Ecuador. Finally, in using my five cases, I aim to understand how imported digital surveillance will develop throughout the broader developing world and whether a Chinese model of Digital Authoritarianism is possible on a wider scale.

Kazakhstan

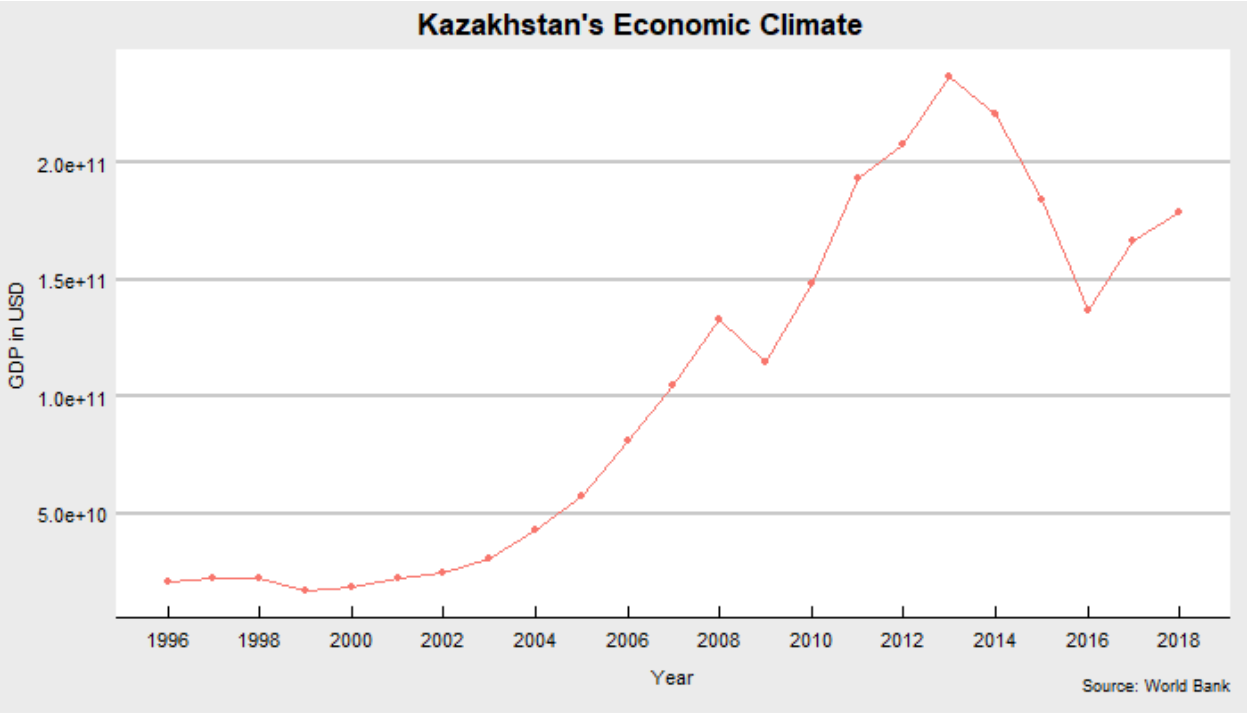
Regime Type and State-Capacity

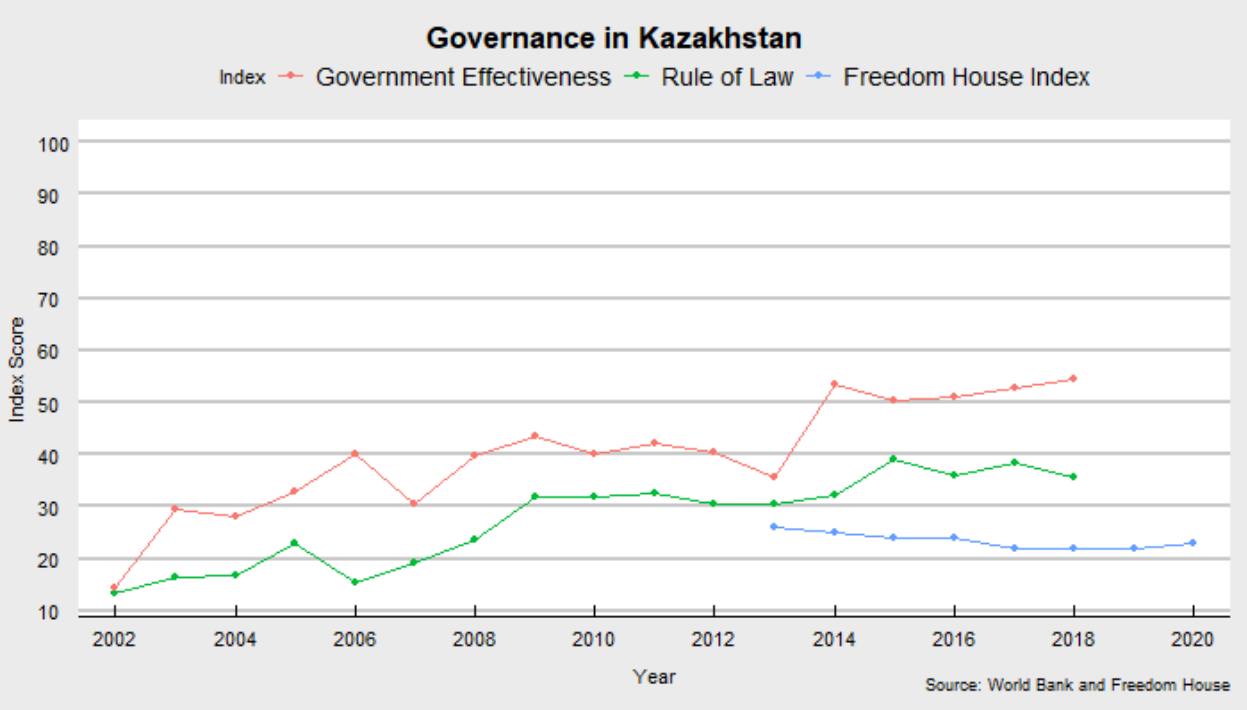
Kazakhstan is an authoritarian regime with the highest state-capacity in Central Asia. Kazakhstan, like the rest of the region, achieved independence in 1991 following the collapse of the Soviet Union. Throughout its post-independence history, Kazakhstan has primarily had a centralized, authoritarian regime under the leadership of its first president, Nursultan Nazarbayev.[45] Nazarbayev remained president until he voluntarily left the position in 2019 and his successor Kassym-Jomart Tokayev became president. Kazakhstan has enjoyed continual economic growth and relatively high levels of state-capacity due to the natural resource wealth within the country, which is largely petroleum based.[46] Kazakhstan has eagerly pursued digitization efforts, including the development of Safe City projects to ostensibly improve domestic governance. Considering the authoritarian and often repressive nature of the Kazakh regime, however, the goal may be more focused on regime stability than improved governance.

In more specific terms, Kazakhstan has the largest GDP in the region and typically scores the best in the region for the World Bank's "Rule of Law" and "Government Effectiveness" governance indicators. In terms of regime type, Kazakhstan has consistently scored low on Freedom House's "Freedom in the World" Index and has been determined to be "Not Free" throughout its history. Kazakhstan in general, therefore, is an authoritarian state with the strongest economy and the best governance in the region, but governance that is still relatively low per global standards.

---

[45] "Kazakhstan: Freedom in the World 2020 Country Report," Freedom House, accessed March 29, 2021, https://freedomhouse.org/country/kazakhstan/freedom-world/2020.
[46] "Kazakhstan," The World Factbook, accessed March 29, 2021, https://www.cia.gov/the-world-factbook/countries/kazakhstan/.


Kazakhstan's Economic Climate
GDP in USD
2.0e+11
1.5e+11
1.0e+11
5.0e+10
1996
1998
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
Year
Source: World Bank


Governance in Kazakhstan
Index
Government Effectiveness
Rule of Law
Freedom House Index
Index Score
100
90
80
70
60
50
40
30
20
10
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
Year
Source: World Bank and Freedom House

Digital Surveillance Development

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

The wealthiest and most developed state within Central Asia has been aggressively pursuing digitization to improve domestic governance for years. These efforts have also included investments into digital surveillance capacity, which Kazakhstan has done largely through cooperation with Chinese ICT companies. This is unsurprising considering that Chinese President Xi decided to officially announce the Belt and Road Initiative in Astana, signifying China's belief that Central Asia will play an important role in the BRI. It also demonstrated that China sees Kazakhstan as an important economic partner in the region. In fact, China has been one of the most important trade partners for Kazakhstan throughout the post-Independence period. So the large extent of Chinese ICT companies' involvement in Kazakhstan's developing digital surveillance apparatus is unsurprising. Despite this, Kazakhstan more so than any other regional state, has attempted to balance Chinese involvement by pushing for domestic control of

most surveillance systems. With that being said, however, while the government promises Kazakh data is securely in Kazakh hands, the extent of Chinese involvement suggests that complete domestic autonomy is unlikely.

Internet is more widely available in Kazakhstan than in any other Central Asian republic, with around 75% of the population having access.[47] Although originally under state monopoly, the Kazakh government pursued market liberalization in 2004 which led to greater competition among multiple licensed operators.[48] Internet in Kazakhstan is provided by a combination of domestic mobile internet providers and cooperation with foreign companies, which include fiberoptic landline and submarine routes to China.[49]

Kazakhstan began to develop a biometric registry in 2009, when the government announced the creation of biometric passports that would include basic information such as a digital signature, photograph, etc.[50] This registry was then expanded in 2016 when the Interior Ministry announced plans to create a national fingerprint database that would include all citizens by 2021.[51] This has since expanded again in 2019 when the government began to launch pilot programs using biometric data to deliver public services and grant access by simply scanning fingerprints or allowing a facial scan.[52] Biometric registries are common globally and often necessary for improving domestic governance, but their expansion is also a requirement for constructing effective Safe City projects.

---

[47] 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.
[48] Ibid
[49] Ibid
[50] Aktan Rysaliev, "Kazakhstan Introducing Compulsory Fingerprinting Program," *Eurasianet*, November 15, 2016, https://eurasianet.org/kazakhstan-introducing-compulsory-fingerprinting-program.
[51] Ibid
[52] 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/.

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. [53] This pilot project was under the jurisdiction of a domestic actor named "Sergek" and it was the one of the most expensive public-private partnership projects in Kazakhstan.[54] Sergek has plans to install around 13 thousand modern surveillance cameras in Nur-Sultan, all of which will be tied into a single surveillance system. According to Astana Police Department, from January to November of 2018, 831 thousand traffic violations were identified by Sergek. [55] This system can monitor an entire city from a single operational center.[56] Sergek has since expanded operations to Almaty and Shymkent, although Nur-Sultan remains the core of Kazakhstan's facial recognition system development. Sergek was also used to help stop purposeless journeys during the COVID-19 pandemic by identifying drivers' place of residence and work to judge if they had changed routes without good reason.[57] Sergek is not the only Kazakh experimentation with building a Safe City, in 2018 a different pilot program was launched in the city of Akqol called "Smart Akqol" to study the effectiveness of Safe City projects in a smaller study.[58]

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

---

[53] Ibid
[54] Nikolai Enelane, "Kak Rabotaet Proekt 'Sergek'"[How the 'Sergek' Project Works], *Informbiuro*, 2019, https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html.
[55] Ibid
[56] Ibid
[57] Alyona Ryzhikova et al., "Limitations on Digital Rights and Civic Freedoms in a Pandemic," *Roskomsvoboda*, 2020, 37.
[58] "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?], *Bluescreen*, accessed May 27, 2019, https://bluescreen.kz/digital-kazakhstan/chto-slozhnee-sozdat-umnyj-gorod-ili-nauchitsja-v-nem-zhit/.

transportation in the capital.[59] 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 the regime's eagerness to expand Sergek's work country-wide.[60] Sergek's success in Nur-Sultan, Almaty, and Shymkent has proven the benefits of Safe City surveillance systems to the Kazakh government. 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 that promises Kazakh data is stored domestically within Kazakhstan, but 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.[61] Also another larger data center is being built by the Chinese company CETC near Nur Sultan.[62] This suggests that Chinese ICT companies may be playing a larger role in Kazakhstan's digital surveillance apparatus than 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

---

[59] Chris Rickleton, "Kazakhstan Embraces Facial Recognition, Civil Society Recoils," *Eurasianet*, October 17, 2019, https://eurasianet.org/kazakhstan-embraces-facial-recognition-civil-society-recoils.
[60] 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/.

[61]Lukpan Akhmediarov, "Kitaiskaia kompaniia stroit v ZKO tsentr khraneniia informatsii" ["A Chinese Company is Building an Information Storage Center in WKO], *Ural'skaia Nedelia*, 2019, https://www.uralskweek.kz/2020/02/12/kitajskaya-kompaniya-stroit-v-zko-centr-xraneniya-informacii/.
[62] Nazerke Syundyukova, "Data Center to Be Built in Nur Sultan," *The Qazaq Times*, September 12, 2019, https://qazaqtimes.com/en/article/69113.

Huawei for developing, providing, and producing internet and/or telecommunications technology.[63] Sergek has disclosed that they heavily relied upon the Chinese company Dahua to develop their surveillance network.[64] President Tokaev 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.[65] Hikvision is an ICT company specifically sanctioned by the U.S. for its role in helping with the persecution of Uighurs in Western China. [66] 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.[67] Dahua is a partially state-owned Chinese company that has become one of the largest providers of video surveillance.[68] They are also the primary company involved with repressive actions against the Uighurs and have had a backdoor in their hardware discovered leaking data to the Chinese government.[69] Finally CETC (China Electronics Technology Group Corporation) is a state-

---

[63] 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/.
[64] Nikolai Enelane, "Kak Rabotaet Proekt 'Sergek'"[How the 'Sergek' Project Works], *Informbiuro*, 2019, https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html.
[65]Asemgul Mukhitkyzy, "«Raspoznaet 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-surveliance-camera/30210035.html.
[66] 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/.
[67]Murakami David Wood, "The Global Turn to Authoritarianism and After," *Surveillance & Society* 15, no. 3/4 (2017): 357–70.
[68] Nikolai Enelane, "Kak Rabotaet Proekt 'Sergek'"[How the 'Sergek' Project Works], *Informbiuro*, 2019, https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html.
[69] 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/.

owned company that produces and manages digital equipment, communications devices, software development, and asset management for civil applications. CETC has been tasked with developing software to identify terrorists using data on jobs, hobbies, habits, and behavior.[70]

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 Chinese-built IT network of the African Union headquarters.[71] Even more surprising is that the African Union was supposedly aware of China's access to their confidential data network, but unwilling to risk damaging relations with China and so decided to ignore the insecurity. The level of Chinese ICT company involvement in Kazakh surveillance is not entirely clear, but it is likely more substantial than officially reported by the Kazakh government and that involvement may include Chinese access to Kazakh data.

Regulatory Environment

In terms of legislation that addresses internet surveillance practices, the government retains the right to monitor internet activity in the interest of national security as detailed by a 1995 law.[72] The government 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

[70] 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.
[71] 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.
[72] "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.

national space" in 2017 for analyzing domestic digital data.[73] Finally, officially implemented in 2019, the Kazakh government requires all ISPs to force users to install a root certificate into their devices, which essentially allows the government to carry out man-in-the-middle attacks on Kazakh internet traffic.[74]

Regarding personal data regulations, however, in 2013 Kazakhstan created a law on "Personal Data and their Protection".[75] The stated purpose of the law is to protect human rights during the collection and processing of 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.[76] It defines personal data into two categories. The first is public data, or data such as biographical directories, addresses, telephone books, public information resources, etc. 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.[77]

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 mediums, or even clouds. Related hardware and

---

[73] Daniiar Moldabekov, "Evraziiskii kibersoiuz: Istoriia o nesamostoiatel′nosti 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.
[74] 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/.
[75] "Zakon Respubliki Kazakhstan Ot 21 Maia 2013 Goda № 94-V «O Personalnykh Dannykh i Ikh Zashchite» (s Izmeneniiami i Dopolneniiami Po Sostoi͡aniiu 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.
[76] Ibid
[77] Ibid

software must be physically present in the territory of Kazakhstan.[78] There are exceptions to when personal data is allowed to be distributed since the government has the right to access personal data in the interest of national security, intelligence, security measures, or counterintelligence.[79] 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.

Kazakhstan's data regulatory environment grants the government access to personal data for national security reasons and generally legitimizes state surveillance. Personal data privacy regulations exist, but have failed to actually protect the citizenry's data. In 2019 a database with roughly11 million people's data, almost the entire population of the country, was leaked in a massive data scandal.[80] This evidences the insecurity of Kazak personal security despite seemingly strong legislation. In spite of these insecurities, however, the Kazakh has eagerly developed its digital surveillance capacity.

Kazakhstan's Potential for Digital Authoritarianism

Overall the enthusiasm of the Kazakh government to develop its surveillance capacity is clearly visible. It has announced large-scale plans for expanding facial recognition surveillance systems nationwide, while promising that domestic companies have full autonomy over Kazakh

[78] Ibid
[79] Ibid
[80] "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.

data and regulations exist to protect citizens' rights to privacy. In terms of regulations, 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, in comparison to other Central Asian republics, the Kazakh government has been the most successful in balancing foreign involvement within their domestic surveillance network. The Kazakh government has also been the most successful in developing Safe City projects in multiple cities and using multiple companies. The scale of Kazakhstan's use of digital surveillance technology is by far the most developed in the region.

Kazakhstan likely has the greatest potential for developing its digital surveillance capacity due to its relatively high economic development, effective governance, and personal data regulations that legitimize state access to data. Still, in comparison to China, Kazakhstan's state-capacity is still lacking, which suggests that adopting a Chinese model of Digital Authoritarianism is still unlikely. Similarly, while Kazakhstan may be an authoritarian regime, it is still more vulnerable than the Chinese government, which makes it somewhat more sensitive to public opinion turning against surveillance practices. Kazakhstan, therefore, will likely continue developing its digital surveillance network, which will eventually become highly effective and widespread. Kazakhstan, however, will not be able to adopt Digital Authoritarianism in the same manner that the Chinese government has.

Uzbekistan

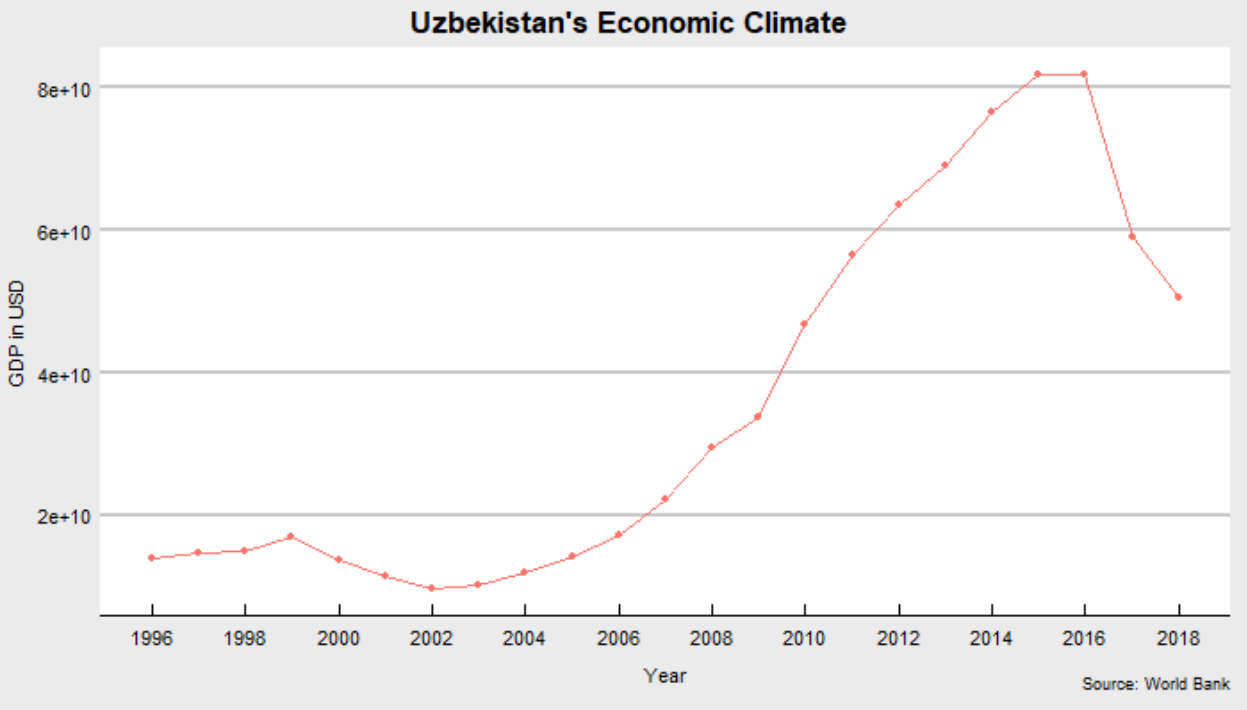
Regime Type and State-Capacity

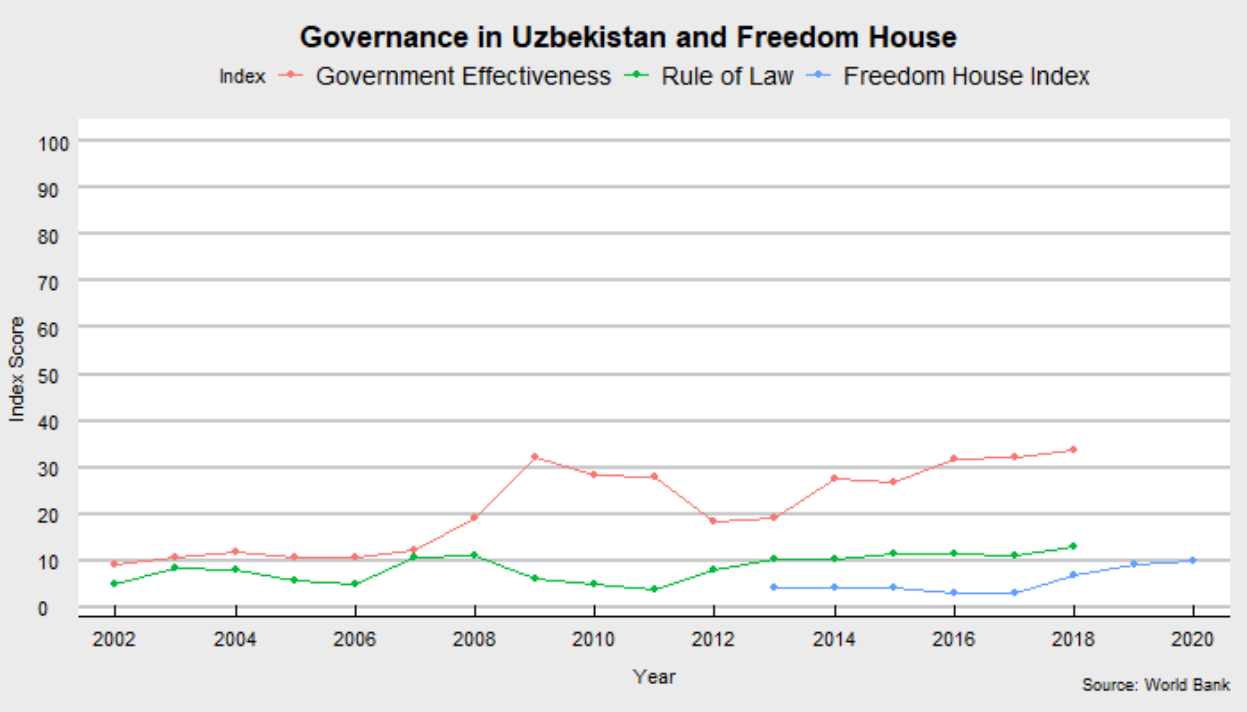
Uzbekistan is an authoritarian regime with the second highest state-capacity in Central Asia. Uzbekistan also achieved independence in 1991 following the collapse of the Soviet Union. Throughout its post-independence history, Uzbekistan has been an authoritarian regime first under the leadership of Islam Karimov, but then under Shavkat Mirziyoyev after Karimov's death in 2016.[81] Uzbekistan's regime under Mirziyoyev has enacted certain reforms that have improved governance and scaled back some repressive policies. Uzbekistan has seen fairly stable economic growth and relatively high levels of state-capacity largely due to the natural resource wealth within the country that includes natural gas and cotton.[82] Uzbekistan also has the highest population in the region. Uzbekistan has pursued digitization including the development of Safe City projects at a similar rate to Kazakhstan. The official government stance is that these projects are to improve overall governance and state-societal relations, but considering the highly repressive nature of the Uzbek government, these developments may also be an excuse to improve surveillance capacity and regime stability.

Uzbekistan has the second largest GDP in the region, which means it is the second strongest regional economy behind 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. 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". Uzbekistan is

[81] "Uzbekistan: Freedom in the World 2020 Country Report," Freedom House, accessed March 29, 2021, https://freedomhouse.org/country/uzbekistan/freedom-world/2020.
[82] "Uzbekistan," The World Factbook, accessed March 29, 2021, https://www.cia.gov/the-world-factbook/countries/uzbekistan/.

an authoritarian state with an overall poor governance record, but a stronger economic climate than most of its neighbors.





Digital Surveillance and State-Capacity

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

Similar to the other Central Asian states, Uzbekistan is an active partner in BRI. 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 worked with multiple foreign ICT companies to achieve this goal, but has chosen to not involve domestic companies at all. The foreign companies involved with Uzbekistan's developing surveillance network include Huawei, CITIC, COSTAR, and Hikvision. They all partner directly with the Uzbek government.

Around 46% of Uzbekistan's population has access to internet of some variety.[83] Much of the telecommunications market is controlled by the state through the state-owned company Uztelecom, but there are partially owned foreign companies that also operate in country. Regarding international internet access, Uzbekistan has several landline routes through Kazakhstan, Kyrgyzstan, Tajikistan, and Afghanistan and so has been largely successful in diversifying its internet access points.[84] Huawei is the most influential foreign telecommunications company in Uzbekistan. In 2008, Huawei modernized the Uzbek national telecommunications network for $21 million dollars and in 2011 Uzbekistan signed a $18 million-dollar technology purchasing deal using loans from the China Development Bank.[85] Huawei has already begun incorporating 5G technology into both Uzmobile and Ucel systems. demonstrating the degree of access Huawei has in Uzbekistan's telecommunications sphere.

Uzbekistan created a comprehensive biometric registry in 2011 when it began transitioning to biometric passports that included biographical information, fingerprints, and photographs.[86] The government continued to promote using a biometric passport and by 2017 around 80% of the population had transitioned to one.[87] In 2020 the government announced that only those with the biometric passport would be able to travel abroad and that ID cards would

---

[83] "Refworld | Freedom on the Net 2018 - Uzbekistan," November 1, 2018, https://www.refworld.org/docid/5be16aed4.html.
[84] 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.
[85] 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/.
[86] "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/.
[87] "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/..

only be acceptable within the territory of Uzbekistan.[88] This system, similar to the other biometric registries in the region, provides the backbone for nascent Safe City projects to be implemented.

While traffic cameras began appearing in Tashkent in 2015, Uzbekistan's first Safe City project officially began in 2018 and has so far been limited to just the capital of Tashkent, but has four phases for implementation.[89] While Tashkent's project began with a surveillance system installed by Huawei and began operating in 2019, it has expanded to include investments from CITIC and COSTAR, although the hardware for the system itself is still provided by Huawei.[90] CITIC and Costar became involved with the project after President Shavkat Mirziyoyev signed a $1 billion agreement in Beijing.[91] A deal that was further expanded upon with an additional $300 million investment to create an Uzbek-Chinese joint venture for implementing and maintaining the Safe City project in Tashkent.[92] The Uzbek government wants to further expand this system by including smart transport, smart education, smart healthcare, smart ride, smart water/sewage,

---

[88] "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.

[89] 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.

[90] 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," *Eurasianet*, accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia;
Zhadmoliddin Turdimov, "Uzbekistan privlechet svyshe $1 milliarda kitaĭskikh 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.

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

[92] UzDaily, "A new joint venture is being created as part of the project to create the Safe City complex," UzDaily.uz, June 21, 2019, http://www.uzdaily.com/en/post/50440.

and smart house capabilities.[93] 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.[94] Uzbekistan's plans for expanding its Safe City project into a country wide Safe City system is one of the most ambitious of the region and the government has already moved towards actualizing this goal. Much like with Kazakhstan, however, information regarding management practices and data storage has not been released.

There is a significant amount of information not provided by the government or companies developing these surveillance systems. Examining the profiles of the companies involved may indicate insecurities and personal privacy concerns. 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.[95] COSTAR Group is another Chinese company that researches, manufactures, and markets optical elements, which includes monitoring systems.[96] Finally, ZTE is one of the leading Chinese ICT companies that has been criticized for its close relationship to the Chinese government.[97] These companies all have close ties to the Chinese government, suggesting yet again that Beijing has a

---

[93] "Uzbekistan to Develop Smart Cities," Dentons, January 28, 2019, https://www.dentons.com/en/insights/alerts/2019/january/28/uzbekistan-to-develop-smart-cities.
[94] 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/.
[95] "CITIC Limited," accessed April 2, 2020, https://www.citic.com/en/.
[96] "Costar Group Co Ltd - Company Profile and News," Bloomberg.com, accessed April 2, 2020, https://www.bloomberg.com/profile/company/002189:CH.
[97] 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/.

degree of access to Uzbek personal data. The Uzbek government, however, has only recently created legislation that creates any formal protections for Uzbek data.

Regulatory Environment

Surveillance and restrictions on the internet in Uzbekistan is extensive. Certain websites that the government perceives as threats are inaccessible in Uzbekistan, including the BBC and Radio Free Europe.[98] 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 even greater control.[99] The state also periodically limits internet access to suppress narratives it deems anti-government. While Skype, WhatsApp, and Viber becoming available in 2018 suggests some liberal developments for Uzbekistan's internet environment, the degree of surveillance and control enjoyed by the regime still classifies it as illiberal in nature.[100]

Uzbekistan did not have specific legislation on personal data before 2019, when it passed the Law on Personal Data.[101] According to the law, the processing of personal data includes collection, systematization, storage, modification, addition, use, provision, dissemination,

---

[98] "Refworld | Freedom on the Net 2018 - Uzbekistan," November 1, 2018, https://www.refworld.org/docid/5be16aed4.html.
[99] "Tashkent Forcing Internet Firms To Locate Uzbek User Data Within Uzbekistan," RadioFreeEurope/RadioLiberty, February 21, 2020, https://www.rferl.org/a/internet-firms-user-data-within-uzbekistan/30447111.html.
[100] "Refworld | Freedom on the Net 2018 - Uzbekistan," November 1, 2018, https://www.refworld.org/docid/5be16aed4.html.
[101] "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.

transfer, depersonalization, and destruction.[102] 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 its needed for research, or when it is taken from public sources.[103]

Regarding data movement, 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 even 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, health or morality of the population.

In general, much like other Central Asian states, formal regulations exist, but the degree of access given to the regime is high. Also general state internet surveillance practices suggest much of this legislation will not be adhered to by governing bodies. The lack of data protections for citizens is worrisome when viewing the rapid expansion of digital surveillance within Uzbekistan over the last few years.

[102] Ibid
[103] Ibid

Uzbekistan's Potential for Digital Authoritarianism

Uzbekistan differs from Kazakhstan in how it has approached the development of its digital surveillance network. It has decided to entirely rely on Chinese ICT companies and has created public-private partnerships to implement and manage Safe City projects. It has also not attempted integrate domestic IT companies like Kazakhstan. More than any other state, however, the Uzbek government has the most ambitious plan for developing its surveillance system, hidden under official rhetoric for developing a nation-wide 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. There is little doubt that the Uzbek personal data is in the possession of the Chinese government, which further demonstrates that Uzbekistan is less concerned with full autonomy than with improving domestic suppressive capacity.

Overall, Uzbekistan's implementation of Safe City projects is only rivaled by Kazakhstan in terms of scale. The Uzbek government's plans for expanding those projects, however, are equal if not slightly more ambitious than the Kazakh government. Uzbekistan's authoritarian regime, higher state-capacity, and regulatory environment that legitimizes state surveillance will likely allow it to develop a highly effective surveillance apparatus. Much like with Kazakhstan, however, there is a limit to Uzbekistan's digital surveillance potential when you compare its state-capacity to China's. While Digital Authoritarianism is unlikely, Uzbekistan's digital surveillance capacity will continue growing quickly and improve in terms of both scale and effectiveness.

Tajikistan

Regime Type and State-Capacity

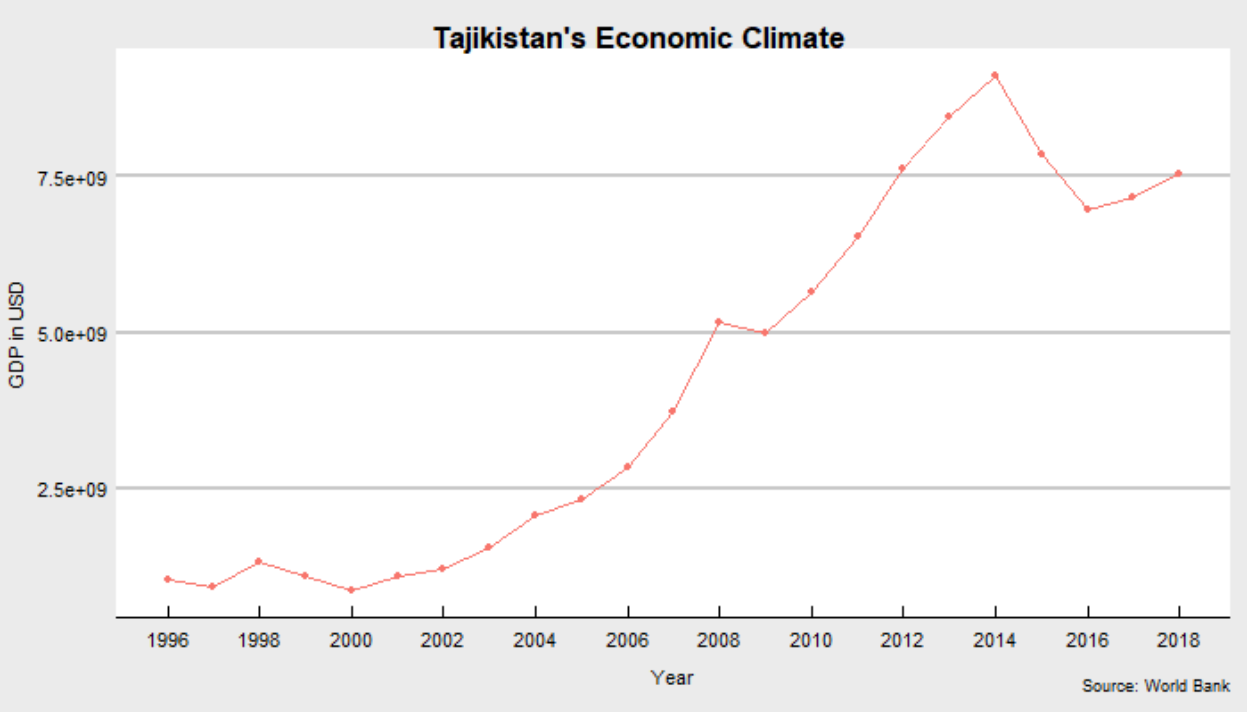
Tajikistan is the last fully authoritarian regime considered in this thesis and it has the lowest state-capacity of any other case. After achieving independence in 1991, Tajikistan quickly descended into a civil war that lasted between 1992-1997.[104] Since 1992, Emomali Rakhmon has been the president of the country, led an overly repressive regime, and successfully marginalized his political opposition.[105] In comparison to Uzbekistan and Kazakhstan, Tajikistan has a much lower level of economic development and suffers from comparatively low levels of state-capacity. The Tajik economy is largely based off of hydroelectric energy, minerals, and remittances.[106] The Tajik government has pursued digitization and Safe City projects for much longer than any of its neighbors, but the results of its investments are less clear. The official government statement behind these efforts is to improve overall governance, but there are obvious benefits to regime stability.

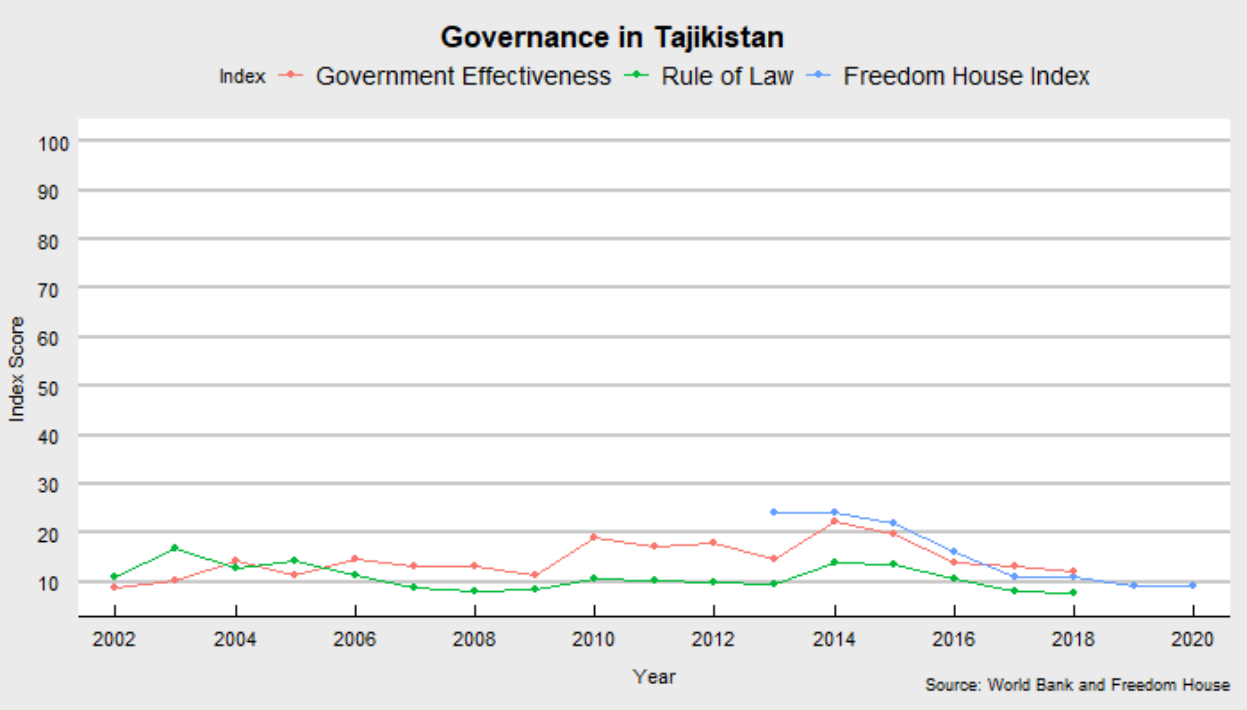
Tajikistan is the poorest state in Central Asia and has one of the region's worst track records for human rights, political freedoms, and civil society.[107] Tajikistan has the lowest GDP in the entire region. Tajikistan's governance record is also worse than its neighbors, as it has regularly scored the worse than its neighbors 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 is

---

[104] "Tajikistan," The World Factbook, accessed March 29, 2021, https://www.cia.gov/the-world-factbook/countries/tajikistan/.
[105] "Tajikistan: Freedom in the World 2020 Country Report," Freedom House, accessed March 29, 2021, https://freedomhouse.org/country/tajikistan/freedom-world/2020.
[106] "Tajikistan," The World Factbook, accessed March 29, 2021, https://www.cia.gov/the-world-factbook/countries/tajikistan/.
[107] "World Report 2020: Rights Trends in Tajikistan," Human Rights Watch, December 10, 2019, https://www.hrw.org/world-report/2020/country-chapters/tajikistan.

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.





Digital Surveillance Development

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 has been one of the major BRI targets for developmental projects for many years, to which the Tajik government has been largely receptive. Tajikistan has paid for Chiense development projects through loans or by directly signing away land or mining rights.[108] This has resulted in large-scale dependencies issues on China, with digital surveillance being no exception. While only one Chinese ICT company, Huawei is active in Tajikistan, it has a near monopoly on the domestic internet environment and the nascent sphere of digital surveillance.

The domestic fixed communications market of Tajikistan is reasonably competitive with a variety of domestic companies that provide internet service.[109] Of those companies, however,

[108] 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.
[109] "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/.

only the state owned Tajiktelecom is operational throughout the whole country. Mobile communications is growing quickly and enjoys a relatively open and competitive market with domestic and foreign companies at play.[110] In terms of international internet connectivity, Tajikistan is reliant on cable connections through Kyrgyzstan, Uzbekistan, and China, which raises network travel security issues.[111] Finally, over 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.[112] Internet surveillance is very common in Tajikistan where internet access is routinely blocked or cancelled depending on domestic circumstances.[113] Since 2001, the Tajik government has mandated that all companies install system of operational search measures in their equipment to allow full government access to data.[114] 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 photograph and fingerprints.[115] The Tajik government decided to expand this data system by

---

[110] Ibid
[111] Ibid
[112] 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.
[113] "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/.
[114] Ibid
[115] 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%D0%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.

mass finger printing citizens in 2016.[116] According to government sources in 2019, this effort was largely successful and as of 2020 there were around 2.5 million citizens who had biometric passports.[117]

The implementation of Tajikistan's Safe City project is more straightforward than other Central Asian republic and began much earlier. Dushanbe's Safe City initiative began in 2013 after Tajikistan spent $22 million dollars on a Huawei contract.[118] Huawei installed hundreds of CCTV and traffic cameras around Dushanbe, but these cameras lacked the facial recognition systems that are more common with current Safe City projects. This system reportedly generated over $14 million dollars in traffic fines in the fall of 2019 alone, which speaks to its overall effectiveness. [119] The Tajik government decided to upgrade the original system also in 2019 when it announced that new Huawei cameras, equipped with facial recognition systems, would be installed not only throughout Dushanbe, but also in every major city of Tajikistan.[120] The contract for this large-scale expansion was granted entirely to Huawei with no domestic company involved whatsoever.

Interestingly, there have been no reports of data management centers being constructed in Tajikistan. This suggests that either local journalists and experts have failed to recognize the

---

[116] "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/.
[117] 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.
[118] 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/.
[119] Tsz Yau Yan, "China Taking Big Brother to Central Asia," Eurasianet, accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia.
[120] "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/.

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 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 land, mineral rights, and domestic factories to Chinese companies, it does not seem impossible that domestic data is handled remotely by Huawei. In fact, this practice would be consistent with Chinese company activities in Tajikistan as the majority of Chinese projects in the country are managed, worked, and completed entirely with Chinese labor.[121]

Tajikistan's Digital Surveillance Development

The most recent and comprehensive piece of data privacy legislation is the 2018 law on the protection of personal data, which defines a legal basis for the collection, storage, and processing of data. This unifies and replaces the previous "scattered" legislations including Law 10 (2002), Law 6 (2001), and Law 15 (2002) which dealt with varying aspects of data protection. The new law contains provisions for consent requirements, biometric data, and subject access requests.[122] This law also defines what constitutes data collection and processing personal data. Data collection is any action aimed at receiving personal data while processing personal data includes recording, systematization, storage, amendment, replenishment, extraction, usage,

[121] 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.

[122] "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.

spread, impersonation, blocking, or destruction of data that is taken from individuals.[123] The law states that the collection and processing of personal data is 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.

Article 11 stipulates, however, that access to personal data without consent is allowed if it is necessary for governmental authorities to carry out their function or when in the interests of protecting the rights and freedom of citizens.[124] Cross border transfers are allowed when the government determines a foreign body has sufficient protection for personal data, subject consent is obtained, or the transfer is necessary for the protection of citizens' rights, freedom, health, morality, or public order. This legislation is similar to other countries in the region, but with even broader stipulations for when data can be collected or used without consent. Considering the reputation that the Tajik government has for adhering to its own legislation as well as its track record of suppressing political dissent, this law only suggests the regimes of global personal privacy norms. It in no way demonstrates any adherence to its principals.

Tajikistan's Potential for Digital Authoritarianism

Generally speaking, Tajikistan 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. Huawei enjoys a near monopoly both within Tajikistan's

[123] Ibid
[124] Ibid

telecommunications hardware market, but 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 storage in a variety of Huawei facilities which 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.

Despite having invested in a Safe City project before any other country in the region, the scale of Tajikistan's Dushanbe project is much smaller than its neighbors. While the Tajik government plans on expanding to other major urban centers, the limited extent of Dushanbe's surveillance system after many years indicates future expansion may be similarly behind schedule. The Tajik government, unlike the Uzbek or Kazakh government, has no plans to incorporate Safe City technology into different societal spheres or governmental programs. Tajikistan will likely continue investing in Safe city Technology, but it will most probably lag behind the region in terms of scale and ambition. Not only is a Chinese model of Digital Authoritarianism impossible for Tajikistan, it will likely struggle to develop a system that is effective outside of Dushanbe, or even within some parts of the. Effective surveillance capacity cannot be entirely imported. It still requires a degree of state-capacity to be properly implemented and expanded. Tajikistan proves that low state-capacity prevents the development of effective surveillance capacity, even when the state in question imports technology, is an authoritarian regime, and has weak regulations that legitimize state surveillance.

Kyrgyzstan

Regime Type and State-Capacity

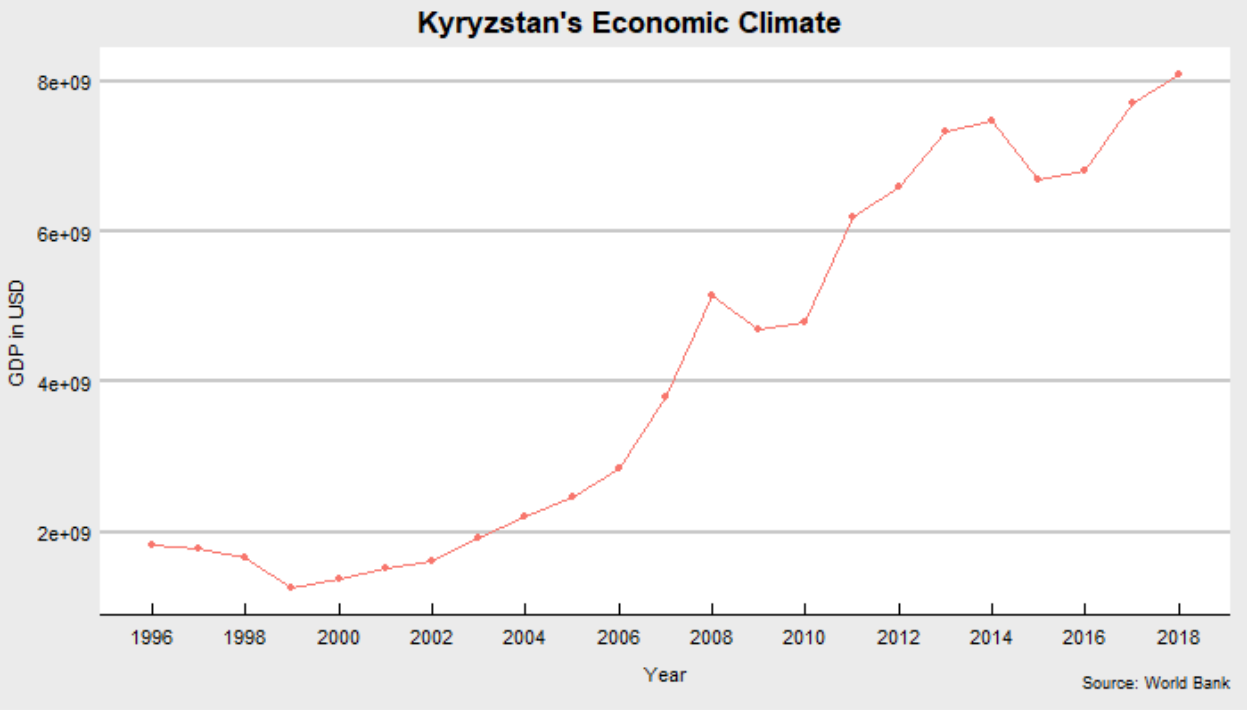
Kyrgyzstan has often been labelled the "Island of Democracy" within Central Asia due to it being the only country in the region with meaningful elections and democratic procedures. Kyrgyzstan has also undergone three separate periods of domestic unrest where the sitting president was removed from power.[125] Kyrgyzstan may be more democratic than its neighbors, but it also has the second lowest state-capacity in the region with high levels of corruption, poor governance, and low economic development. Perhaps as a result of these larger capacity issues, but also because of the flawed transition of power to the current president Sadyr Japarov in 2021, the quality of Kyrgyzstan's democratic regime is increasingly under question.[126] Despite this, however, Kyrgyzstan is still the most democratic state within Central Asia, whose government sees digitization and Safe City projects as potential solutions to the issues of poor governance and low state-capacity.

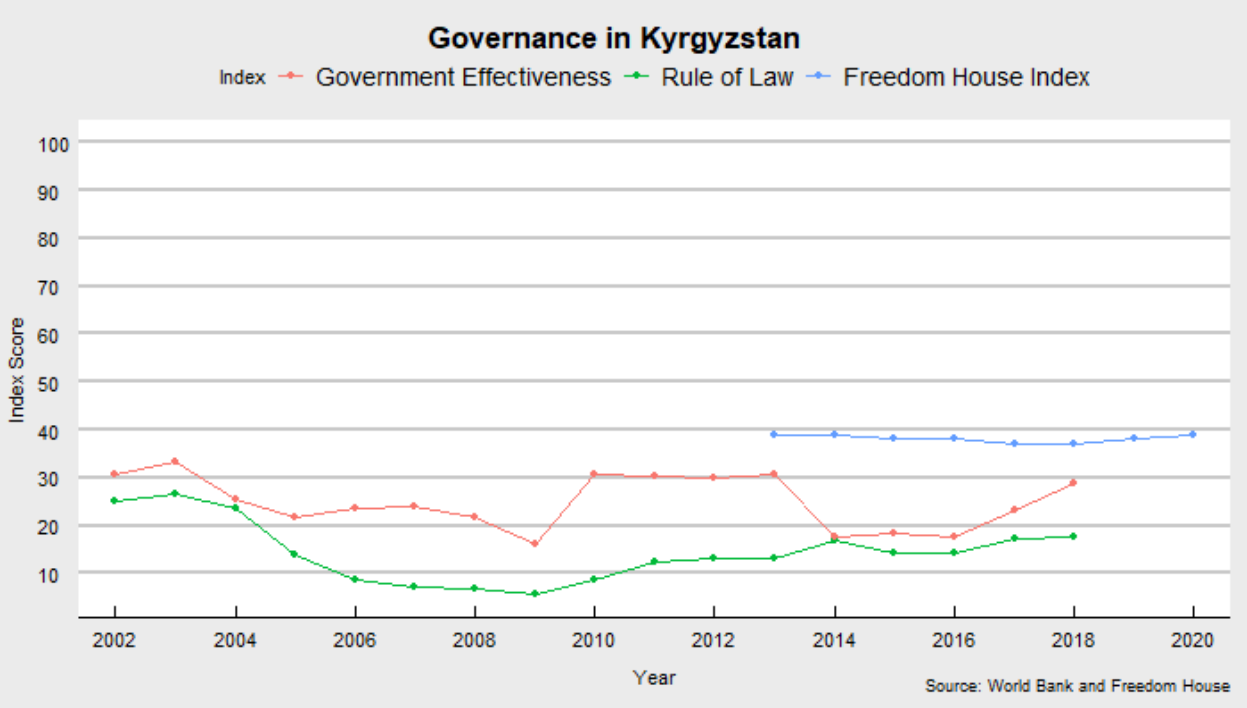
Kyrgyzstan has the second lowest GDP of the region, only ahead of Tajikistan in terms of economic output. It performs poorly in terms of "Government Effectiveness" although it does have the second highest "Rule of Law" score in the region, behind Kazakhstan. In terms of regime type, however, Kyrgyzstan has the highest score for Freedom House's "Freedom in the World" Index in Central Asia and is considered the sole democracy within the region. Freedom House considered Kyrgyzstan to be "Partially Free" in 2020, but following the flawed transition to President Japarov, Freedom House lowered its rating to "Not Free" in 20201.[127] Overall,

---

[125] "Kyrgyzstan: Freedom in the World 2021 Country Report," Freedom House, accessed March 29, 2021, https://freedomhouse.org/country/kyrgyzstan/freedom-world/2021.
[126] Ibid
[127] Ibid

Kyrgyzstan is the most liberal state in the region, but still has poor governance and a very weak economic climate.





Digital Surveillance Development

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 may be Central Asia's only democratic state, but this label is often misleading since the regime has fundamental issues with political rights and civil society.[128] That being said, Kyrgyzstan's democratic tendencies makes its relationship with surveillance technology interesting for making comparisons. Overall, Kyrgyzstan was one of the first to cooperate with China through BRI. China is Kyrgyzstan's most important economic partner and the Kyrgyz government has been eager for Chinese infrastructure projects.[129] Kyrgyzstan has also made some attempts to balance Chinese ICT involvement in its digital surveillance sphere

[128] "World Report 2020: Rights Trends in Kyrgyzstan," Human Rights Watch, December 10, 2019, https://www.hrw.org/world-report/2020/country-chapters/kyrgyzstan.
[129] Roman Mogilevskii, "Kyrgyzstan and the Belt and Road Initiative" (Bishkek, Kyrgyzstan: University of Central Asia: Graduate School of Development, 2019).

but has generally been less successful than Kazakhstan. Local IT companies play little role in Kyrgyz Safe City projects and debt to China suggests long-term dependency issues. Also despite being a democratic state, the lack of transparency surrounding digital surveillance development indicates the Kyrgyz government is moving toward more illiberal practices.

Internet is much less widely available in Kyrgyzstan than it is in Kazakhstan, for example, with less than 35 percent of the population having access.[130] 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.[131] Similar to Kazakhstan, domestic internet providers in Kyrgyzstan are divided between 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.[132] The government has a large degree of access to all communications networks and has a known history of wiretapping.[133]

Kyrgyzstan began to develop a nation-wide biometric database with the introduction of a biometric data registration program in 2014.[134] Legislation announced plans to expand this system nationwide for the 2015 elections. By 2018 over 80% of the population was included in the registry, that includes fingerprints, photo identification, and various biometric data, which the Kyrgyz government hopes to use for expanding its eGovernance initiatives that will potentially

---

[130] 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

[131] Ibid

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

[133] Ibid

[134] Pingback: Kyrgyzstan's Biometric Election : The Corbett Report, "Kyrgyzstanis Skeptical about Government Biometric Data Drive · Global Voices," *Global Voices*, November 24, 2014, https://globalvoices.org/2014/11/24/kyrgyzstanis-skeptical-about-government-biometric-data-drive/.

include an electronic voting platform.[135] 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.[136]

Kyrgyzstan was initially interested in developing a Safe City program in 2011 with Russian company Stilsoft, but the deal fell through for unknown reasons.[137] Then in 2018 they tried again and oversaw a bidding war between Huawei and the Russian ICT company Vega.[138] 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.[139] Negotiations with Huawei to install hardware eventually fell through, however, without explanation and instead Kyrgyzstan granted a $33 million project to Vega to install traffic cameras.[140] The following year, however, Kyrgyzstan chose the Chinese defense equipment supplier CEIEC to install a network of facial recognition cameras and to create a police command center in Bishkek apparently free of cost.[141] While the system began functioning in 2019, there has been no information provided about where the data will be stored or who has

---

[135] 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/.
[136] 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/.
[137] Temur Umarov, "China Looms Large in Central Asia," Carnegie Moscow Center, accessed April 2, 2020, https://carnegie.ru/commentary/81402.
[138] Tsz Yau Yan, "China Taking Big Brother to Central Asia," Eurasianet, accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia.
[139] "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.
[140] Tsz Yau Yan, "China Taking Big Brother to Central Asia | Eurasianet," accessed April 1, 2020, https://eurasianet.org/china-taking-big-brother-to-central-asia.
[141] Bermet Zhumakadyr kyzy, "Right to Privacy in Kyrgyzstan," *EUCAM*, January 21, 2020, sec. Commentaries, https://eucentralasia.eu/2020/01/right-to-privacy-in-kyrgyzstan/.

access.[142] A second phase of the Safe City project began in 2019 which will install thousands of new cameras throughout the country.[143] 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.[144]

The bulk of Kyrgyzstan's surveillance network has been implemented using foreign ICT companies who partner directly with the Kyrgyz government as opposed to local companies. Huawei, much like in all Central Asian republics, plays a large role in Kyrgyz telecommunications companies, providing 90 and 70 percent of the hardware for major providers Sky Mobil and Alfa Telecom respectively.[145] Vega, the Russian company who won a contract to install traffic cameras over Huawei, is a company that specializes in military and surveillance systems.[146] The China National Electronics Import and Export Corporation (CEIEC) is a state owned enterprise that delivers defense and security solutions to foreign markets.[147] 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 has historically only operated

---

[142] 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.
[143] Temur Umarov, "China Looms Large in Central Asia," Carnegie Moscow Center, accessed April 2, 2020, https://carnegie.ru/commentary/81402.
[144] 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/.
[145] 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/.
[146] "About," Vega.su, accessed April 1, 2020, http://vega.su/en/about/.
[147] Tsz Yau Yan, "Smart Cities or Surveillance? Huawei in Central Asia: Chinese Surveillance Technologies Are Popular among Central Asia's Governments,"

domestically in China.[148] Finally, IZP group is a Chinese big-data company that has created a business network covering over 104 countries. One of their main goals is to compliment 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.[149] The nature of these companies in combination with the lack of transparency regarding the Safe City project's management suggests a high degree of Chinese penetration into Kyrgyzstan's domestic information sphere.

Regulatory Environment

Legislation on personal data privacy does promise a wide range of protections for citizens based on two major laws. The first is the 2014 law on biometric data, whose purpose was to create a database of citizens' biometric data defined as the physiological and biological characteristics based upon which you can establish identity.[150] It includes clauses that mandate the collection, promises transparency, and the protection of the data. Of specific note would be article 6 that describes the protections for biometric data. It promises that the database is the property of Kyrgyz Republic that it is subject to legislation concerning personal information, the field of informatization, and the protection of state secrets.[151] It also states that all procedures for ensuring the security of the database (i.e. collection, processing, storage, and use) is determined by the government. In Article 7, the law mandates that the gathering and use of biometric data

[148] "300044.SZ - Shenzhen Sunwin Intelligent Co.,Ltd. Profile | Reuters," accessed April 2, 2020, https://www.reuters.comundefined.
[149] 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.
[150] "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/.
[151] Ibid

requires 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.[152]

The other key piece of legislation is a 2008 law regarding personal data that created a state policy towards data management and collection.[153] 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 it has an "urgent" need to protect the interests of the subject, but only after requesting permission from 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.[154] 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 even assuming the government adheres to its own legislation, but two data related scandals occurred

[152] Ibid
[153] "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.
[154] Ibid

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. [155] Another notable scandal occurred in 2017 when it was uncovered that then Presidential candidate Sooronbay Jeenbekov's campaign was illegally accessing citizens' private data to help win the 2017 election. Hackers found a little-known, but free-to-access real estate website called "Samara" was listed as a major government server and included the personal data of 2 million citizens from the server of the State Registration Service, including PIN, passport, and phone numbers.[156]

Kyrgyzstan's democratic regime, paired with more robust personal data, would suggest some protections against the development of wide-spread surveillance systems. The Kyrgyz government, however, is ambitiously developing its surveillance capacity in a similar manner to the rest of the region and often without proper protections in place to safeguard personal data. The high level of insecurity within Kyrgyzstan's data management practices suggest the use of new surveillance systems may put Kyrgyz citizens' private data at risk.

Kyrgyzstan's Potential for Digital Authoritarianism

Kyrgyzstan has been less successful than Kazakhstan in balancing foreign involvement in its digital surveillance network. Being the most democratic state in the region, one would expect greater measures of transparency regarding this system, but that is not the case. Kyrgyzstan does

[155] 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/.

[156] Rinat Tukhvatshin, "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/.

have stronger legislation regarding personal privacy, but it also has well documented data abuse scandals and has not reported on the degree of access enjoyed by Chinese ICT companies, which is problematic as the government becomes 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 adhere to personal data regulations, the Kyrgyz government is improving its digital surveillance capacity at the cost of its citizenry's data privacy.

Overall, Kyrgyzstan's Safe City project is slightly larger in scale than Tajikistan's, but significantly behind either Uzbekistan or Kazakhstan. Much like Tajikistan, however, Kyrgyzstan began developing its Safe City project well before those two neighbors who have now exceeded it. Kyrgyzstan has the most vulnerable regime in the region and has some of the lowest state-capacity as well. Kyrgyzstan is also becoming less democratic over time and its weak regulatory environment fails to protect its citizenry from either foreign ICT companies or their own government. Ironically, the main limiting factor to the Kyrgyz government developing Digital Authoritarianism is not its democratic regime, which will likely continue becoming more illiberal under President Japarov. The more immediate impediment is actually Kyrgyzstan's lack of state-capacity and therefore its lack of ability to actually develop the country-wide surveillance system that it currently hopes to create.

Ecuador

Regime Type and State-Capacity

Ecuador can be used as a comparative for Central Asian states for a few key reasons. Demographically, Ecuador has a population slightly larger than Kazakhstan, but lower than Uzbekistan.[157] In terms of GDP, it is slightly below Kazakhstan, but overall comparable to the region. In terms of its government type, Ecuador is labelled as "Partly Free", similar to Kyrgyzstan, but Ecuador scores 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 countries in Central Asia.

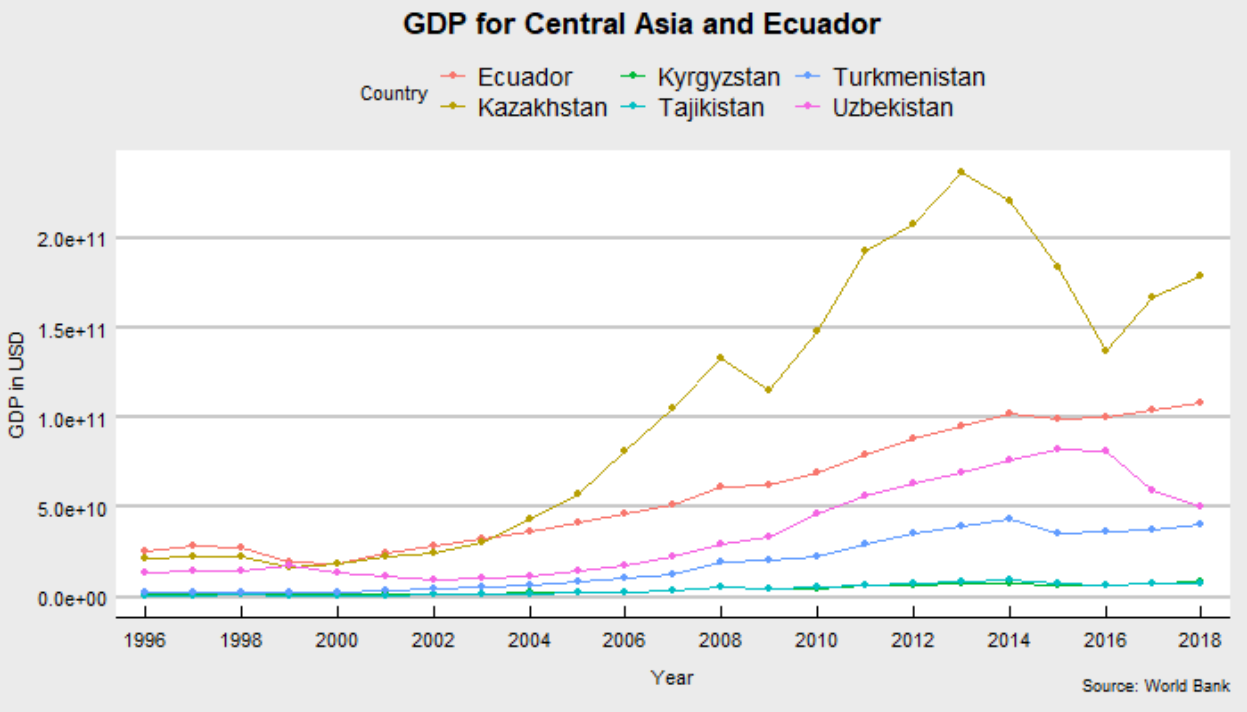
In comparison to the Central Asian cases, therefore, Ecuador has the second highest state-capacity, but is by far the most democratic country under consideration in this thesis. Ecuador has had a somewhat complicated history with democracy since 2007 when President Rafael Correa imposed restrictions on media and civil society, but after Lenin Moreno became President in 2017, he began reversing many of those repressive policies.[158] Interestingly, however, under both administrations the Ecuadorian government has aggressively built an advanced country-wide surveillance system through extensive cooperation with Chinese ICT companies.

South America was a target for Chinese investment before the Belt and Road Initiative was officially announced. China expanded its role in South America around the 2008 financial

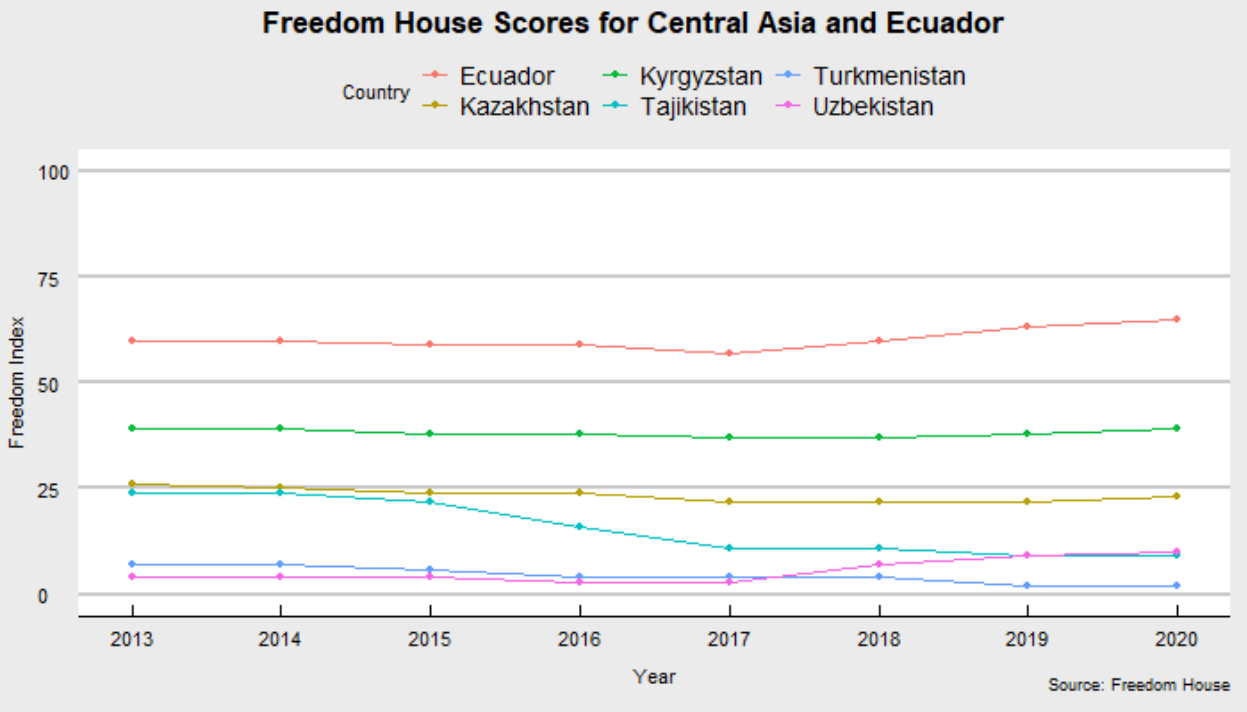
---

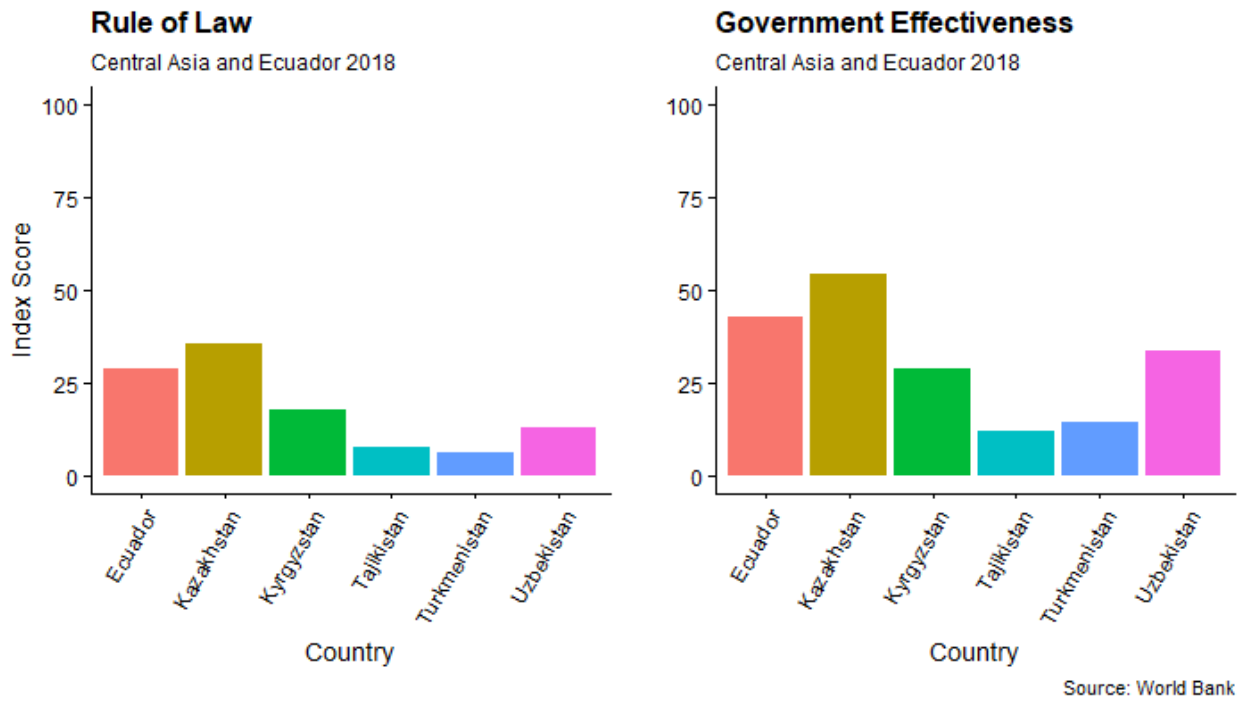
[157] "Population, Total - Tajikistan, Kyrgyz Republic, Ecuador, Turkmenistan, Uzbekistan, Kazakhstan | Data," accessed April 12, 2020, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=TJ-KG-EC-TM-UZ-KZ.
[158] "Ecuador: Country Profile," Freedom House, accessed March 29, 2021, https://freedomhouse.org/country/ecuador.

crisis and began offering South American countries economic assistance in the form of loans.[159] This resulted in China becoming South America's top trading partner, which has also caused many South American countries to cut their diplomatic relationships with Taiwan, which demonstrates the seriousness of Chinese relations for the region.[160] Ecuador specifically, however, began signing deals with China in 2011 for infrastructure projects, often backed by Chinese loans. Recently, the government exchanged 80 percent of Ecuador's oil exports in return for around $19 billion dollars in loans, which is only one of the many loan schemes the government has pursued with China.[161] This financial dependency can be seen across South America and more broadly, within countries that are participating in the Belt and Road Initiative, Central Asia included.



[159] 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.
[160] Ibid
[161] Ibid


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


Rule of Law
Central Asia and Ecuador 2018
Index Score
100
75
50
25
0
Ecuador
Kazakhstan
Kyrgyzstan
Tajikistan
Turkmenistan
Uzbekistan
Country
Government Effectiveness
Central Asia and Ecuador 2018
100
75
50
25
0
Ecuador
Kazakhstan
Kyrgyzstan
Tajikistan
Turkmenistan
Uzbekistan
Country
Source: World Bank

Digital Surveillance Development

	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 • Data Centers
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

Ecuador purchased a complete digital surveillance system from Chinese ICT companies before almost any other country. Chinese ICT companies treated Ecuador as a flagship program to see how effective and profitable exporting digital surveillance could be. Ecuador's eagerness for surveillance indicated they would find a high demand from the developing world. This sparked the now world-wide trend of Chinese ICT companies exporting digital surveillance to developing countries, including 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 Ecuador's surveillance apparatus, the use of multiple types of

technology, and the degree of Chinese ICT involvement in management is far greater due to Ecuador having cooperated with China for a much longer period of time. Analyzing Ecuador's development of digital surveillance and personal privacy regulations will demonstrate the similarities between it and Central Asia. Ecuador, therefore, offers an insight into what Central Asia might look like in the coming years.

In Ecuador around 57% of the population has access to the internet, which is considered partially free.[162] 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 internet service providers 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 mobile internet is dominated by a Brazilian company in addition to CNT's large market share.[163] There are multiple internet routes to Ecuador, which includes the newest Pacific Caribbean Cable System—a high speed fiber-optic cable—that was completed in 2015 by a consortium of companies.[164] Both wired and wireless internet are widely available in the country, although there have been difficulties in expanding internet access to rural areas. A variety of international companies are involved with Ecuador's internet sphere including ZTE who built a large-scale virtual IP Multimedia Subsystem partially in Ecuador.[165] CNT also began launching a 5G network in cooperation with Huawei in 2019.[166]

---

[162] "Refworld | Freedom on the Net 2018 - Ecuador," November 1, 2018, https://www.refworld.org/docid/5be16b1d6.html.
[163] Ibid
[164] Ibid
[165] "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/.
[166] "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.

Ecuador began creating its nationwide biometric database in 2012, which included photographs, personal information, employment information, financial records, and car ownership data.[167] This registration was used to issue Ecuadorian biometric passports that have chips containing facial data, fingerprints, and demographic information.[168] In 2019, however, the registration would be the subject of a massive data breach due to an unsecured server, which resulted in over 20 million Ecuadorians having their personal data exposed.[169]

Ecuador's nation-wide surveillance project that includes multiple Safe City systems was and is designed, built, and partially managed by Chinese ICT companies.[170] In 2011, an Ecuadorian delegation's tour of Beijing's surveillance system during the 2008 Olympic games partially convinced the Ecuadorian government to further develop its own surveillance capacity. Since then Ecuador's surveillance network has drastically expanded in size and was eventually given the name of ECU-911.[171] This system has been built and operated by two ICT companies: Huawei and CEIEC. ECU-911 now includes over 4,000 cameras, 16 monitoring centers, employs over 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 country-wide.[172] Its success supposedly inspired

---

[167] 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/.
[168] "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/.
[169] 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/.
[170] 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.
[171] Ibid
[172] 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/.

Venezuela, Bolivia, and Angola to purchase replica systems, which in turn sparked a wave of other developing countries purchasing digital surveillance technology from China.

ECU-911 was designed by CEIEC, but largely relies on hardware from Huawei. While it began from a $240 million loan and only intended to be in the capital Quito, the system has been expanded upon since 2011 with the support of additional Chinese loans.[173] CEIEC provided engineers and technicians who helped construct the overall 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.[174] This system grew again starting in 2016 by including thermal monitors, drones, and facial recognition cameras.[175] Before 2016, ECU-911 relied entirely on CCTV cameras and the use of 16 regional response centers where government employees would physically monitor the camera feeds to identify criminal activity.[176] 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

[173] 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/.
[174] Charles Rollet, "Chinese Government Builds Far-Reaching, Allegedly Corrupt, Surveillance System in Ecuador," IPVM, 27:47 400AD, https://ipvm.com/reports/china-ecuador.
[175] Frank Fang, "China Provides Technology for Ecuador's Mass-Surveillance ECU 911 Emergency System," *CuencaHighLife*, 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.
[176] 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.

ECU-911 to begin integrating facial recognition.[177] In 2019 it was officially announced that FRT would be used in Ecuador's airports and in major cities.[178]

Unlike the digital surveillance systems in Central Asia, the operation and management of ECU-911 is better understood due to some notable investigative journalism. Data storage and management happens at each regional management center and the system is fully scalable.[179] The hardware and expertise utilized to create and manage the system have come from Huawei and CEIEC respectively, which in combination with what is known of ECU-911's overall infrastructure, demonstrates that Chinese ICT companies enjoy a high degree of access. Having already explored 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 alongside Ecuadorian officials 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.

---

[177] Charles Rollet, "Chinese Government Builds Far-Reaching, Allegedly Corrupt, Surveillance System in Ecuador," IPVM, 27:47 400AD, https://ipvm.com/reports/china-ecuador.
[178] 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/.
[179] 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.

Regulatory Environment

Ecuador's legal environment and surveillance practices were generally on par with Central Asia during the previous administration, but they have improved under President Moreno. Ecuador passed a resolution that established data privacy as a right in 2008, but failed to implement regulations for that right until recently.[180] In 2019, due to the large-scale data breach, the Ecuadorian government began to fast track personal data privacy legislation similar to GDPR, but 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 citizen for "the integral security of the state, society, and democracy".[181] Recently revealed evidence suggests that SENAIAN actively spied on journalists, politicians, activists, and citizens while it was operating. In 2018, however, President Moreno abolished SENAIAN because of "citizen's ethical demands" and replaced it with a Coordinating Unit of Public Security under his own direct control.[182] It is unclear if this new government organ has actually ceased 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 SENAIN, Moreno's administration ordered all ISPs to keep an updated registry of subscriptions without providing any transparency for its use of personal data.[183] With Ecuador completing personal data privacy legislation soon, the new Ecuadorian government's surveillance measures may become more transparent. Even if this legislation is

---

[180] 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/.
[181] "Refworld | Freedom on the Net 2018 - Ecuador," November 1, 2018, https://www.refworld.org/docid/5be16b1d6.html.
[182] Ibid
[183] Ibid

adopted, however, its existence will not necessarily prevent surveillance practices. The lack of data protection legislation has not stopped the Ecuadorian government, under both an authoritarian and democratic leaning president, from heavily investing in the development of its digital surveillance capacity. A non-existent regulatory environment with weak implementation and enforcement measures, suggests there will be few limitations to state surveillance in Ecuador any time soon.

Ecuador's Potential for Digital Authoritarianism

Ecuador has continually expanded ECU-911 under both a previous autocratic-leaning president and the more liberal current president. Both have publicly supported the project and have actively sought greater Chinese investment. ECU-911 has also been credited with cutting down crime by 11.8% according to Ecuador's National Statistics and Census Institute.[184] Finally, according to the New York Time's report on ECU-911, the surveillance program generally enjoys high support among Ecuadorians, despite the degree of Chinese ICT cooperation being common knowledge.[185] Considering the signaled support of ECU-911 from two Ecuadorian presidents with opposing 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 its surveillance capacity. 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

[184] "Feature: Chinese Technology Brings Falling Crime Rate to Ecuador," *XinhuaNet*, January 19, 2018, http://www.xinhuanet.com/english/2018-01/19/c_136908255.htm.
[185] 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.

and it has successfully demonstrated the highest efficiency that a Chinese designed and operated surveillance apparatus can produce. Ecuador will continue to be the litmus test for predicting the trajectories of similar states who seek the benefits of improving surveillance 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.

More broadly, however, Ecuador indicates two major points. One, that a country with a relatively high state-capacity, similar to both Kazakhstan and Uzbekistan, can develop a highly effective, country-wide surveillance apparatus if it imports surveillance technology. Two, Ecuador indicates that having a democratic regime does not necessarily prevent a country from developing such a system, since surveillance can enjoy widespread public support and regulations can be underdeveloped or lack serious enforcement protocols. That being said, the Ecuadorian government is vulnerable to public opinion and if ECU-911 were to become a focus of public outrage, in the same way that SEINEN was, the government would likely be forced to limit its scale and operation. Ecuador, therefore, will most likely not develop Digital Authoritarianism because of these democratic tendencies. But while Ecuador will likely not develop Digital Authoritarianism, it has still developed a highly effective and sophisticated surveillance network that impacts every urban center within the entire country. More impressively, despite being unable to perform this feat independently, the Ecuadorian state was able to rival the developed world's surveillance capacity simply by relying almost entirely on Chinese ICT companies. If Central Asian states remain on their current trajectories, those that are in similar places to Ecuador, notably Kazakhstan and Uzbekistan, will likely have country-wide systems that can rival ECU-911 in scale within a relatively short amount of time.

Conclusions

Digital surveillance that relies on artificial intelligence and facial recognition technology has the potential to create totalitarian regimes. 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 country-wide level, but has also begun exporting this technology as a commodity. In fact, digital surveillance systems have become a major component of BRI partnerships worldwide.

Authoritarian or semi-democratic countries are frequent clients of this technology because they have the greatest incentives to improve suppressive capacity and the fewest constraints to implementing surveillance. Can this trend, therefore, be seen in Central Asia, which is a developing region that tends towards authoritarianism and has been a major target of BRI projects? In looking at four Central Asian republics the answer is clearly yes. Central Asian governments are eager to develop their digital surveillance systems largely through partnerships with Chinese ICT companies. In the four Central Asian republics analyzed, all have similar timelines for developing Safe City projects. Kazakhstan is the only country to have attempted to balance Chinese ICT involvement by integrating domestic IT companies into their surveillance system. 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 the region is rapidly expanding its digital surveillance capacity.

The ICT companies' Central Asian governments have decided to cooperate with, however, all are either owned directly by the Chinese government or have suspiciously close ties to the CCP. This suggests, broadly, that China has 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 at the cost of greater Chinese financial dependency and sacrificing autonomy over their citizens' data. Due to 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 proved the effectiveness of Chinese surveillance systems and inspired most of South America to purchase similar networks. Ecuador's eagerness for and policies towards Chinese digital surveillance in 2011 mirrors Central Asian states in 2019. It is probable, therefore, that surveillance systems on the same scale as ECU-911 will be adopted in Central Asia, but even more effective because they will utilize artificial intelligence from the beginning. Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan have already signaled their intention to move towards this direction by expanding their surveillance systems to other cities and announcing plans to create nation-wide systems. While this is unlikely for either Kyrgyzstan or Tajikistan due to low state-capacity, it is entirely possible, if not probable, for both Kazakhstan and Uzbekistan. 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 globally.

This trend has implications for both BRI recipient countries and China. As seen in Ecuador and Central Asia, these surveillance systems likely come at the cost of autonomy and financial dependency to China. Considering China is most likely the state to begin exporting 5G globally, BRI recipient countries will be largely dependent on Chinese ICT companies for the near future. This will create clear dependencies at multiple levels between the developing world and China. The Chinese government has made it an official 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.

But how do regime type, state-capacity, and regulatory environment impact the potential for Digital Authoritarianism? In examining Safe City projects in the authoritarian cases of Kazakhstan, Uzbekistan, and Tajikistan, the impact of state-capacity is clear. The most highly developed country, Kazakhstan, has been able to balance foreign interference to a much higher degree than either Uzbekistan or Tajikistan. Similarly, the scale of Kazakhstan's Safe City project is also much higher. Facial recognition technology is already in use by private companies and the Safe City systems in Nur-Sultan, Almaty, and Akqol are fully functional and ostensibly highly effective. In Uzbekistan, with slightly lower governance and economic development, only one Safe City project is actively in use. The Uzbek government, however, has aggressive plans to build Safe City projects in all urban centers and to involve them into almost every aspect of society. Tajikistan, with the lowest levels of governance and economic development, has been developing its Safe City initiative for much longer than either Kazakhstan or Uzbekistan, but the scale of its surveillance system is much smaller than either. While the Tajik government also has ambitious plans for expansion, its rate of development significantly lags behind the other authoritarian regimes with higher capacity.

It seems to be the case, therefore, that higher state-capacity allows a country to develop digital surveillance capacity more quickly and ambitiously. Low capacity somewhat mitigates the scale and sophistication of digital surveillance networks. It is not the case, therefore, that digital surveillance tools are an immediate solution to low capacity within authoritarian regimes. The fundamental issues of low capacity and regime weakness cannot be addressed entirely through the adoption of digital surveillance. Unsurprisingly therefore, digital surveillance, is more effective within higher functioning authoritarian regimes and will not automatically make a weaker authoritarian regime, strong. It is unlikely, however, that any authoritarian country in Central Asia can actually develop Digital Authoritarianism in a Chinese manner, as they all have more vulnerable regimes and are still inherently developing states.

How then does regime type affect the development of digital surveillance? In comparing the democratic – or at least semi-democratic – case of Kyrgyzstan to the authoritarian cases, it seems that regime type has little effect overall on the development of digital surveillance capacity. The scale of Safe City projects in Kyrgyzstan was not significantly different than its neighbors. The Kyrgyz government's Safe City initiative is larger and more ambitious than Tajikistan's, but less so than either Uzbekistan or Kazakhstan. In terms of digital infrastructure, therefore, regime type is seemingly less influential than state-capacity. Kyrgyzstan's democratic regime type, however, may likely prevent the full adoption of Digital Authoritarianism as the government is more vulnerable to public opinion than any other Central Asian government. As of now though, the greatest mitigating factor to Kyrgyzstan's development of digital surveillance capacity is poor governance and the lack of capital, not its democratic regime.

This is even more clear in comparing the Central Asian cases to Ecuador, which is the most democratic state but has the most sophisticated and widespread surveillance network.

Ecuador has the highest level of state-capacity and economic development besides Kazakhstan and the fact that it has a larger surveillance network than Kazakhstan is simply due to the fact that Chinese ICT companies have been involved in the country for much longer. Regime type seems, therefore, to result in little difference in terms of the development of surveillance capacity.

Finally, what role do regulatory environments play in this dynamic? In looking at all five cases it seems that most regulatory environments share similar limitations and stipulations. There are key differences, however, between democratic regimes and authoritarian regimes. In each of the authoritarian cases, the regulations regarding surveillance and personal data seem to legitimize the state's ability to use are surveillance without the consent of the people. In the democratic cases, such stipulations are rarer, and the threat of negative public opinion may force the regime to not abuse those stipulations that do exist. Unfortunately, even within democratic regimes there is little transparency regarding state surveillance practices and few measures that force state or private sector compliance with regulations. While personal data privacy regulations may exist, they often lack the strength to meaningfully impact surveillance.

This is very clear in Kyrgyzstan where there have been massive data scandals by the Kyrgyz government against its own citizenry. In Ecuador the issue is less weak regulations and more that regulations simply do not exist, despite it having an expansive surveillance system country wide. It may be the case that strong regulations with effective enforcement measures are very effective at limiting state-surveillance in a democratic country, but within the developing world strong regulations with enforcement measures are difficult to find. Even more common than weak regulations are regulatory environments in authoritarian regimes that help legitimize state surveillance entirely. Regulatory environment, therefore, are likely ineffective at mitigating

the development of digital surveillance capacity in the developing world because regulations are often affected too strongly by state-capacity and regime type.

In summation, digital surveillance capacity is developing quickly in Central Asia, but not equally. State-capacity seriously affects its scale and effectiveness, while democratic regimes in the developing world do not, largely due to weak regulatory environments. This is concerning because the expansion of digital surveillance in the developing will likely lead to the corrosion of democratic norms and the strengthening of state-capacity in authoritarian regimes. This thesis only includes five countries and is far from a representative sample. Those five cases do, however, demonstrate trends that are useful for future research. While it is very unlikely that a myriad of Digital Authoritarian Oceania's will come into existence, the development of digital surveillance will very likely expediate the global weakening of democracy, strengthen authoritarian regimes, and help proliferate illiberal practice.

Bibliography

Akhmediarov, Lukpan. “Kitaiskaia kompaniia stroit v ZKO tsentr khraneniia informatsii” [“A Chinese Company is Building an Information Storage Center in WKO]. Ural′skaia 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.

Akbar, Nafisa, and Susan L. Ostermann. “Understanding, Defining, and Measuring State Capacity in India: Traditional, Modern, and Everything in Between.” *Asian Survey* 55, no. 5 (2015): 845–61.

Artigas, Alvaro. “Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets.” Institut Barcelona Estudis Internacionals, 2017.

Bah, Serign Modou, and Fang Ming. “An Improved Face Recognition Algorithm and Its Application in Attendance Management System.” *Elsevier*, no. 5 (2020).

Ball, Kirstie. *Routledge Handbook of Surveillance Studies*. Routledge, 2012.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Gabri, David Lyon, and R.B.J Walker. “After Snowden: Rethinking the Impact of Surveillance.” *International Political Sociology* 8 (2014): 121–44.

Bernal, Paul. “Data Gathering, Surveillance and Human Rights: Recasting the Debate” 1, no. 2 (2016): 143–264.

Bhutia, Sam. “Data Show Kyrgyzstan Weathering Debt Load.” *Eurasianet*, September 12, 2019. https://eurasianet.org/data-show-kyrgyzstan-weathering-debt-load.

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/.

Brona, Adrian. “One Belt, One Road: New Framework for International Relations?” *Polish Journal of Political Science* 4, no. 2 (2018): 57–76.

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.

Damjanovski, Vlado. *CCTV: From Light to Pixels*. 3rd ed. Waltham, Massachusetts: Butterworth-Heinemann, 2014.

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%D0%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.

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/.

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

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

Feng, Emily, and Amy Cheng. "China's Tech Giant Huawei Spans Much of the Globe Despite U.S. Efforts to Ban It." *NPR*, October 24, 2019. https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it.

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.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. 1926-1984. New York: Pantheon Books, 1977.Freedom House. "Freedom in the World." Accessed May 15, 2020. https://freedomhouse.org/report/freedom-world.

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

———. "Ecuador: Country Profile." Accessed March 29, 2021. https://freedomhouse.org/country/ecuador.

———. "Freedom in the World." Accessed May 15, 2020. https://freedomhouse.org/report/freedom-world.

———. "Kazakhstan: Freedom in the World 2020 Country Report." Accessed March 29, 2021. https://freedomhouse.org/country/kazakhstan/freedom-world/2020.

———. "Kyrgyzstan: Freedom in the World 2021 Country Report." Accessed March 29, 2021. https://freedomhouse.org/country/kyrgyzstan/freedom-world/2021.

———. "Tajikistan: Freedom in the World 2020 Country Report." Accessed March 29, 2021. https://freedomhouse.org/country/tajikistan/freedom-world/2020.

———. "Uzbekistan: Freedom in the World 2020 Country Report." Accessed March 29, 2021. https://freedomhouse.org/country/uzbekistan/freedom-world/2020.

Furukawa, Eiji. "Belt and Road Debt Trap Spreads to Central Asia." Nikkei Asian Review, August 29, 2018. https://asia.nikkei.com/Spotlight/Belt-and-Road/Belt-and-Road-debt-trap-spreads-to-Central-Asia.

Geddes, Barbara. "What Do We Know About Democratization After Twenty Years?" *Annual Reviews* 2 (June 1999): 115–44.

Glasius, Marlies, and Marcus Michaelsen. "Illiberal and Authoritarian Practices in the Digital Sphere" 12 (2018): 3795–3813.

Gobel, Christian. "The Information Dilemma: How ICT Strengthen or Weaken Authoritarian Rule." *Statsvetenskaplig Tidskrif* 115, no. 4 (2013): 385–402.

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," June 28, 2019. https://thediplomat.com/2019/06/china-dominates-digital-infrastructure-in-uzbekistan/.

Hendrix, Cullen S. "Measuring State Capacity: Theoretical and Empirical Implications for the Study of Civil Conflict." *Journal of Peace Research* 47, no. 3 (May 1, 2010): 273–85. https://doi.org/10.1177/0022343310361838.

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 Sostoi̯aniiu 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.

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.

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. “Kyrgyzstanis Skeptical about Government Biometric Data Drive · Global Voices.” *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.

Liu, Yiju, and E.F. Avdokushin. “Forming the Foundations of the ‘Digital Silk Road.*” Miir Novoi Ekonomiki* 13, no. 4 (2019): 62–71.

Mendez, Robert. “The New Big Brother: China and Digital Authoritarianism.” Committee on Foreign Relations United States Senate, July 21, 2010. https://www.foreign.senate.gov/download/2020-sfrc-minority-report_-the-new-big-brother---china-and-digital-authoritarianism.

Mill, John Stuart. *Principles of Political Economy*, 1848.

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 nesamostoiatel′nosti 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.

Moriuchi, Priscilla. "The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture." *Recorded Future*, June 10, 2019. https://www.recordedfuture.com/huawei-technology-risks/.

Moustafa, Tamir. "Law and Courts in Authoritarian Regimes." *Annual Review of Law and Social Science* 10 (2014): 281–99.

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. "«Raspoznaet 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.

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.

Neelima, M. Lakshimi, and M Padma. "A Study on Cloud Storage." *International Journal of Computer Science and Mobile Computing* 3, no. 5 (May 2014): 966–71.

O'Meara, Sarah. "Taking the Silk Road to High-Tech Growth." *Nature* 563, no. 7729 (2018): S25–27.

Orwell, George. *1984*. London: Secker and Warburg, 1949.

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.

Polyakova, Alina, and Chris Meserole. "Exporting Digital Authoritarianism: The Russian and Chinese Models." Brookings, August 26, 2019. https://www.brookings.edu/research/exporting-digital-authoritarianism/.

Porter, Jon. "'Hidden Backdoors Were Found in Huawei Equipment, Reports Bloomberg." The Verge, April 30, 2019. https://www.theverge.com/2019/4/30/18523701/huawei-vodafone-italy-security-backdoors-vulnerabilities-routers-core-network-wide-area-local.

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.

Refworld.org. “Refworld | Freedom on the Net 2018 - Ecuador,” November 1, 2018. https://www.refworld.org/docid/5be16b1d6.html.

———. “Refworld | Freedom on the Net 2018 - Uzbekistan,” November 1, 2018. https://www.refworld.org/docid/5be16aed4.html.Reynolds, Sam. “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.

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*. The Center for 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.” *Eurasianet*, November 15, 2016. https://eurasianet.org/kazakhstan-introducing-compulsory-fingerprinting-program.

Ryzhikova, Alyona, Anna Karnaukhova, Artyom Kozlyuk, Aleksei Kozlyuk, Andrei Sushko, Natalya Malysheva, and Sarkis Darbinyan. “Limitations on Digital Rights and Civic Freedoms in a Pandemic.” *Roskomsvoboda*, 2020, 37.

Saeed, Aamir. “Islamabad’s Multi-Million-Dollar ‘Safe City Project’ Fails to Deliver Results.” Arab News PK, December 4, 2017. https://www.arabnews.pk/node/1203516/metropolitan.

Schneier, Bruce. “Security and the Internet of Things.” *Schneier on Security*, https://www.schneier.com/blog/archives/2017/02/security_and_th.html.

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/.

Shahbaz, Adrian. “The Rise of Digital Authoritarianism.” Freedom House, 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

Shen, Hong. “Building a Digital Silk Road? Situating the Internet in China’s Belt and Road Initiative.” *Carnegie Mellon University* 12 (2018): 2683–2701.

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.

Szkarlat, Monika, and Katarzyna Mojska. *New Technologies as a Factor of International Relations*. Newcastle-upon-Tyne: Cambridge Scholars Publisher, 2009.

The World Factbook. “Kazakhstan.” Accessed March 29, 2021. https://www.cia.gov/the-world-factbook/countries/kazakhstan/.

———. “Tajikistan.” Accessed March 29, 2021. https://www.cia.gov/the-world-factbook/countries/tajikistan/.

———. “Uzbekistan.” Accessed March 29, 2021. https://www.cia.gov/the-world-factbook/countries/uzbekistan/.

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 kitaĭskikh 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/.

UzDaily. “A new joint venture is being created as part of the project to create the Safe City complex.” UzDaily.uz, June 21, 2019. http://www.uzdaily.com/en/post/50440.

Vestal, Theodore. *Ethiopia: A Post-Cold War African State*. Non-Series. Santa Barbara: ABC-CLIO, Praeger, 1999.

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

World Bank. “GDP, PPP (Current International $) | Data.” Accessed November 22, 2019. https://data.worldbank.org/indicator/ny.gdp.mktp.pp.cd.

———. “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.World Bank. “GDP, PPP (Current International $) | Data.” Accessed November 22, 2019. https://data.worldbank.org/indicator/ny.gdp.mktp.pp.cd.

———. “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/.

Yan, Tsz Yau. “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: 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/.

Yayboke, Erol, and Samuel Brannen. “Promote and Build: A Strategic Approach to Digital Authoritarianism.” Center for Strategic and International Studies, October 15, 2020. https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.

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.

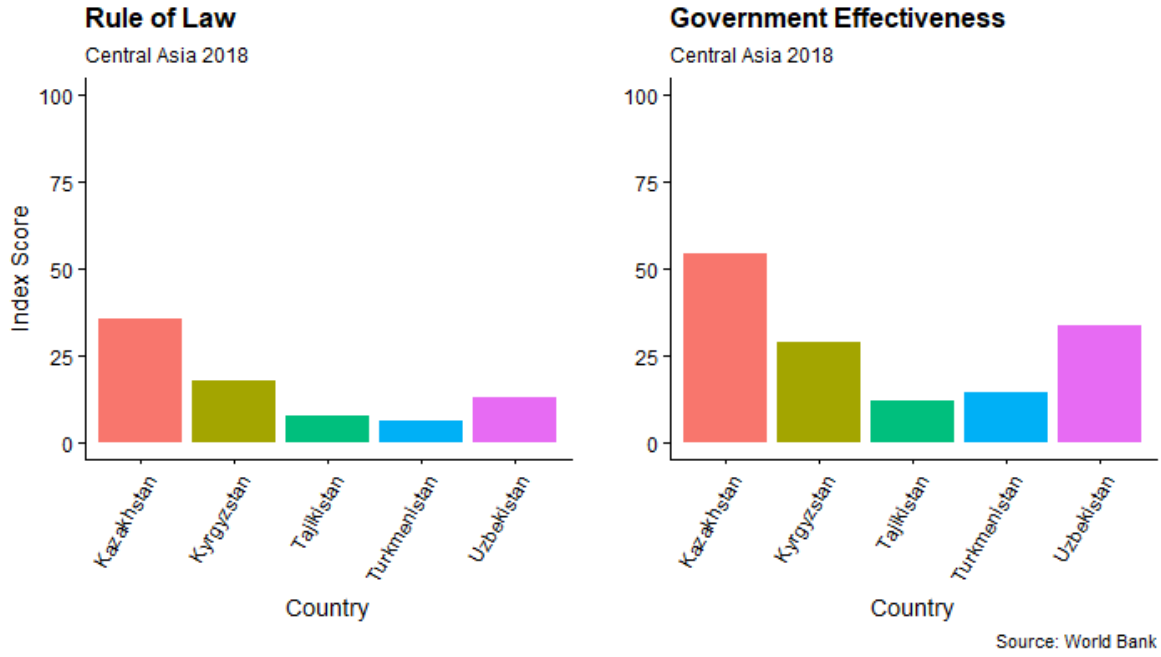
Yujian, Wu, Zhang Yuzhe, Yu Ning, Qu Yunxu, Lin Jinbing, and Han Wei. “How Did an Ambitious Cross-Border Settlement Firm’s Dream Turn Sour? - Caixin Global.” Accessed April 1, 2020.

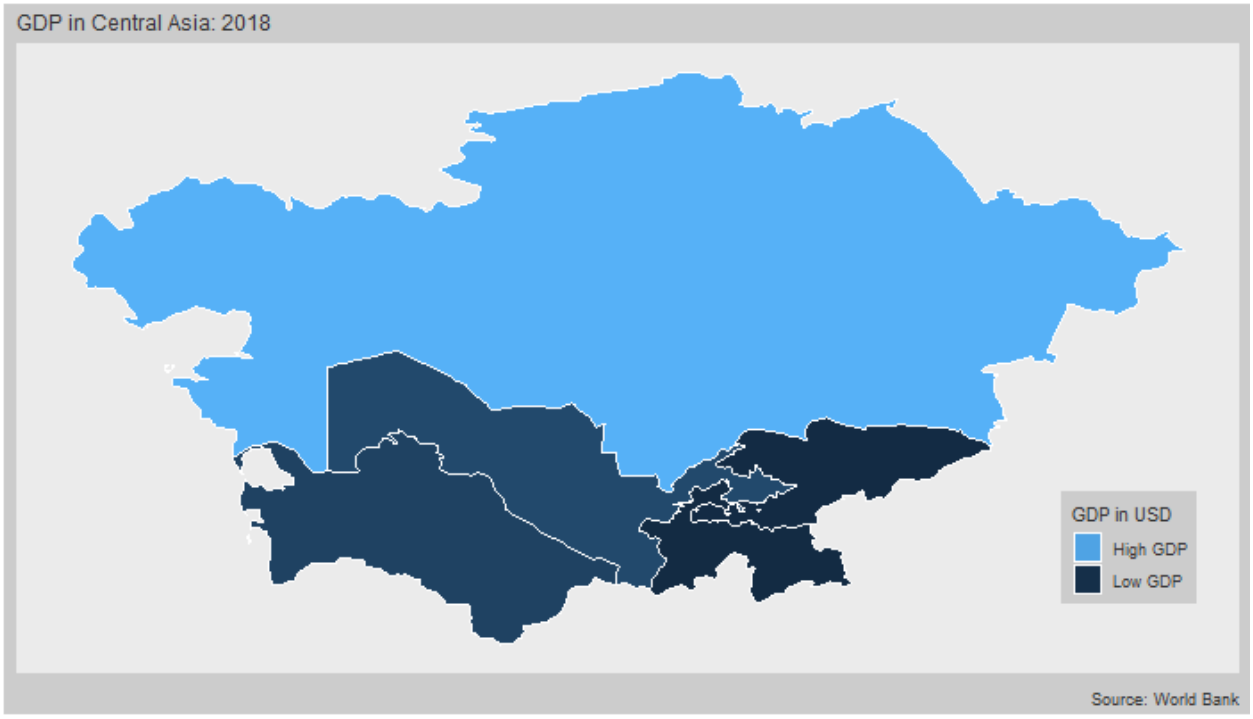
Zhumakadyr kyzy, Bermet. “Right to Privacy in Kyrgyzstan.” *EUCAM*, January 21, 2020, sec. Commentaries. https://eucentralasia.eu/2020/01/right-to-privacy-in-kyrgyzstan/.

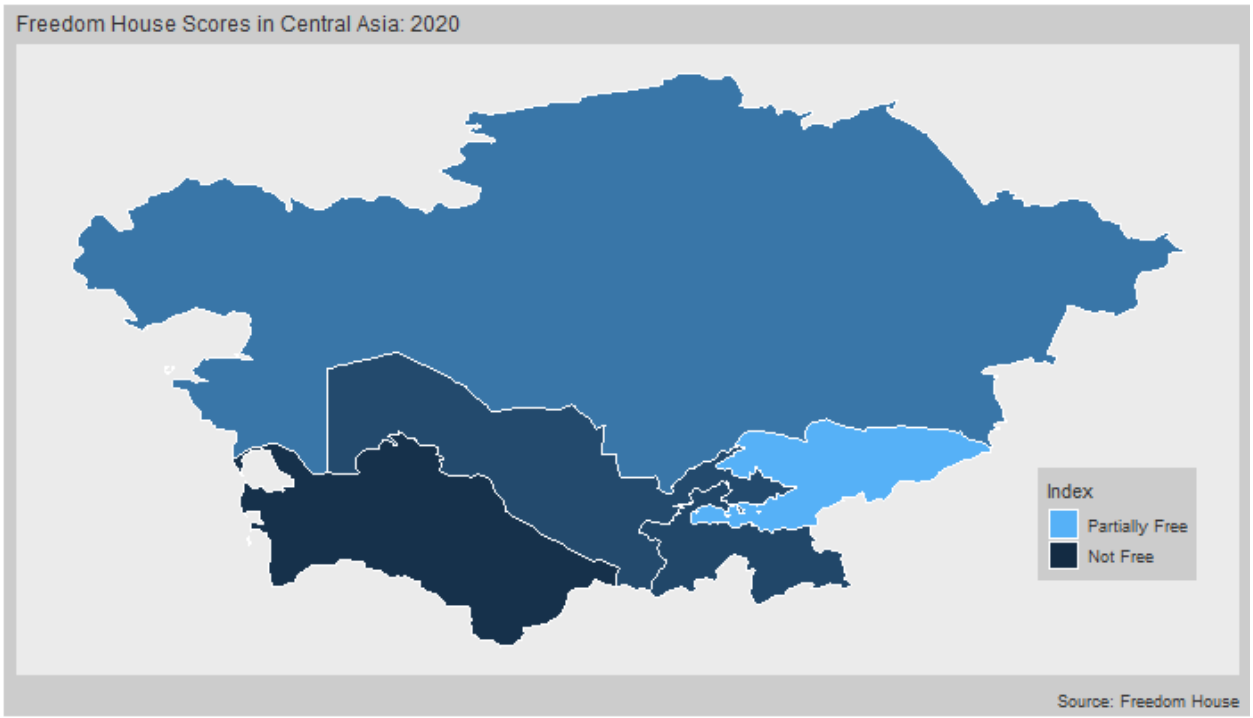
Appendix

Central Asian Overview Tables and Figures

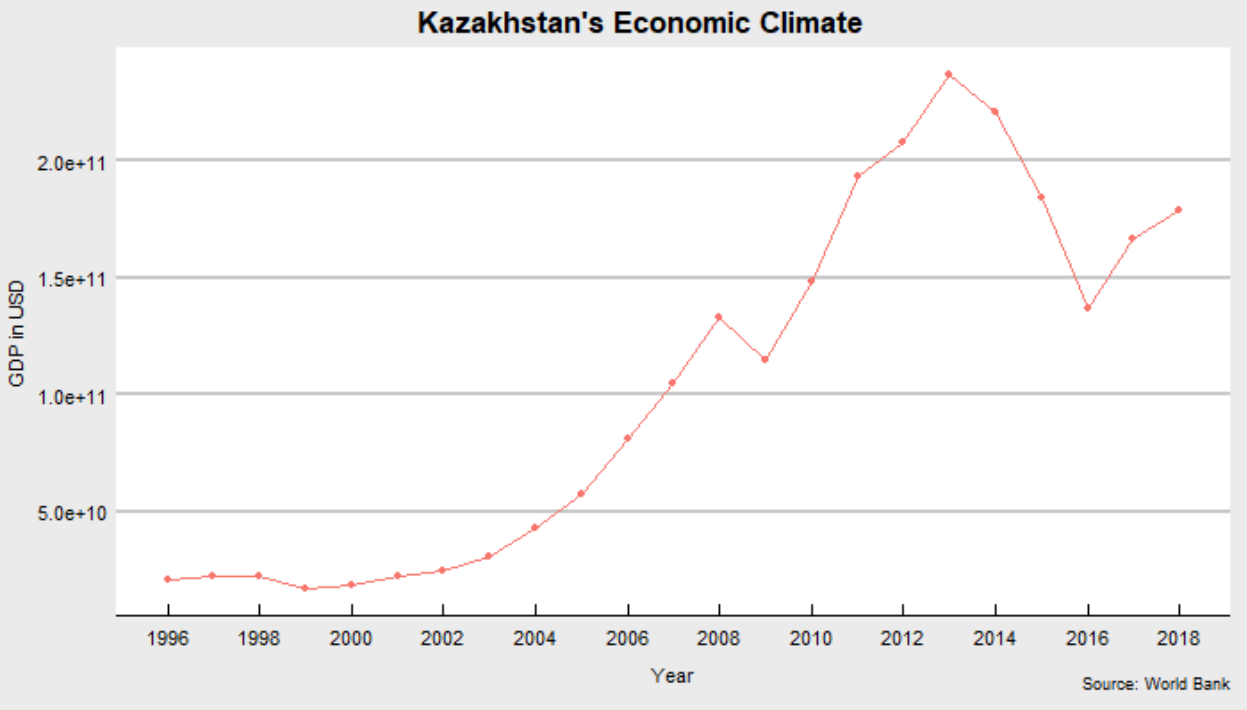
	Kazakhstan	Kyrgyzstan	Tajikistan	Uzbekistan
Technology	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers	• Internet • Biometric Database • Safe City Projects • Facial Recognition • Data Centers	• Internet • Biometric Database • Safe City Projects • Facial Recognition	• 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

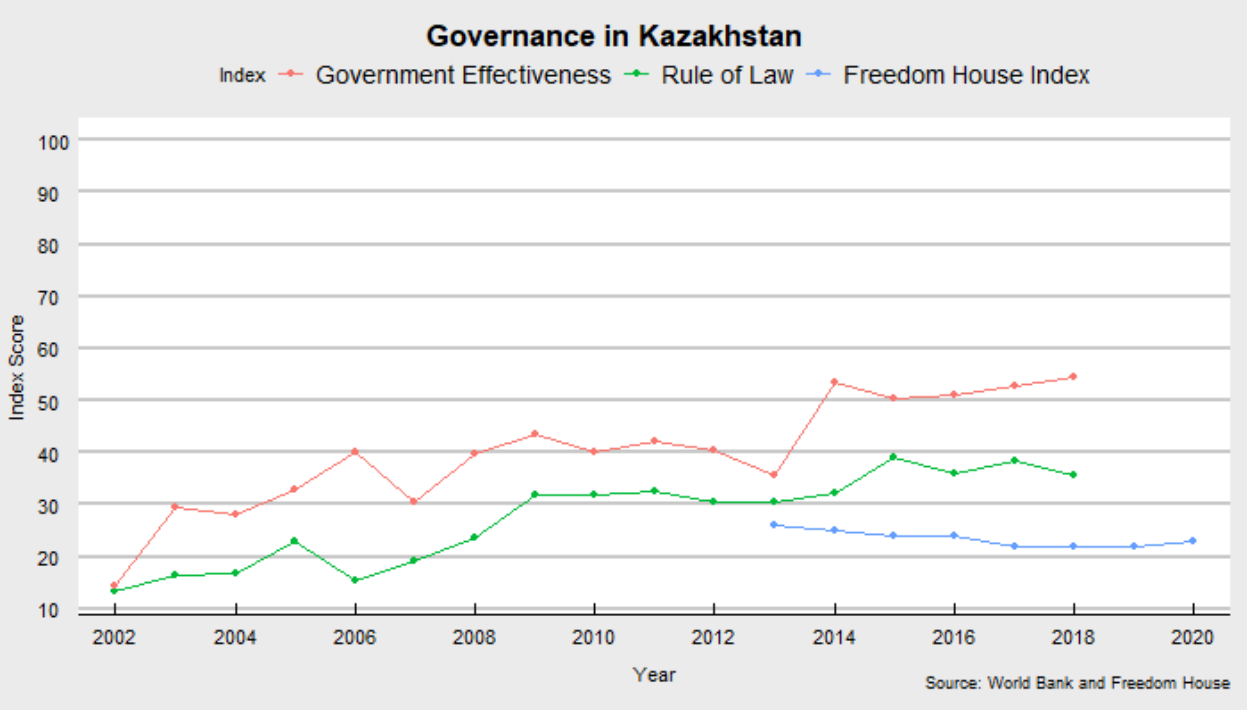



GDP in Central Asia: 2018
GDP in USD
High GDP
Low GDP
Source: World Bank

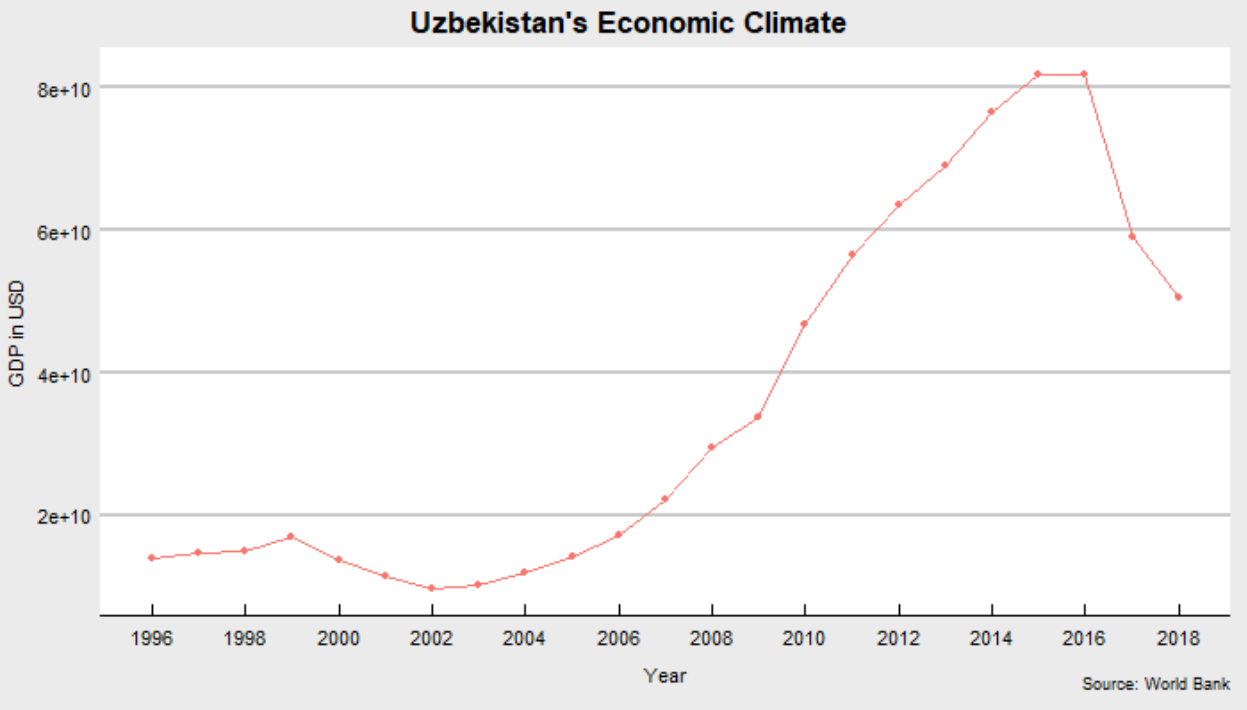

Freedom House Scores in Central Asia: 2020
Index
Partially Free
Not Free
Source: Freedom House

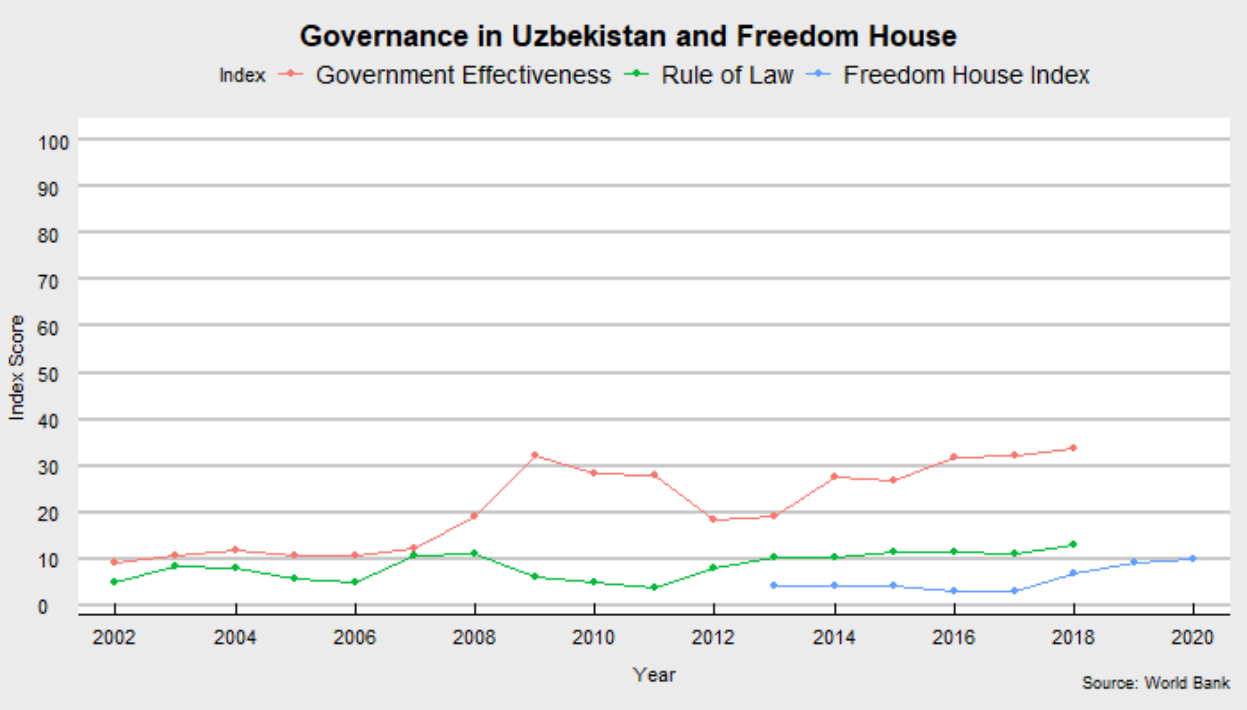
Kazakhstan Figures



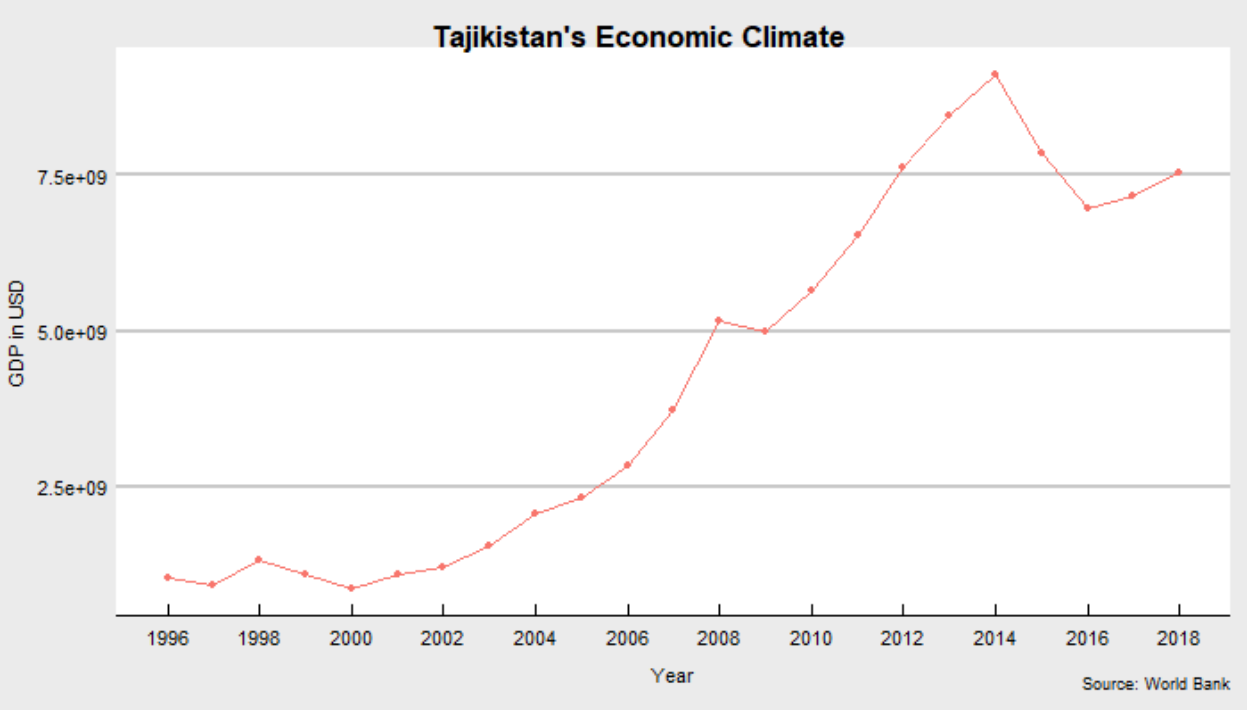


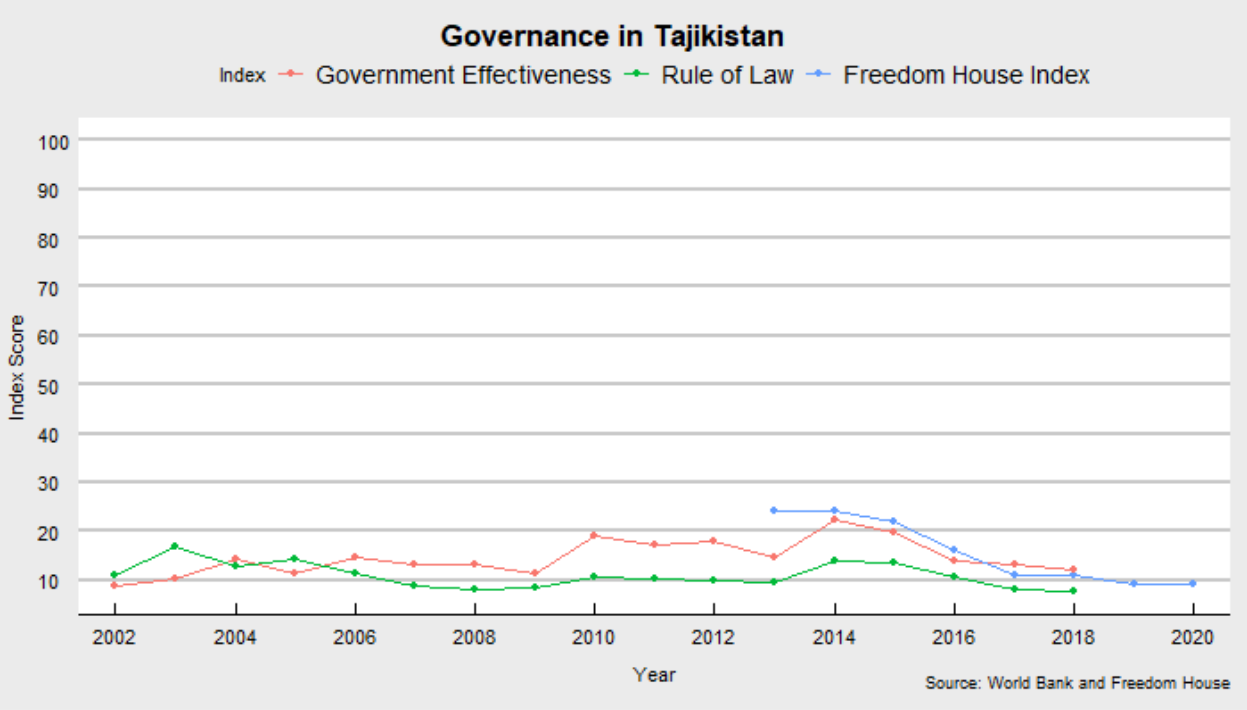
Uzbekistan Figures



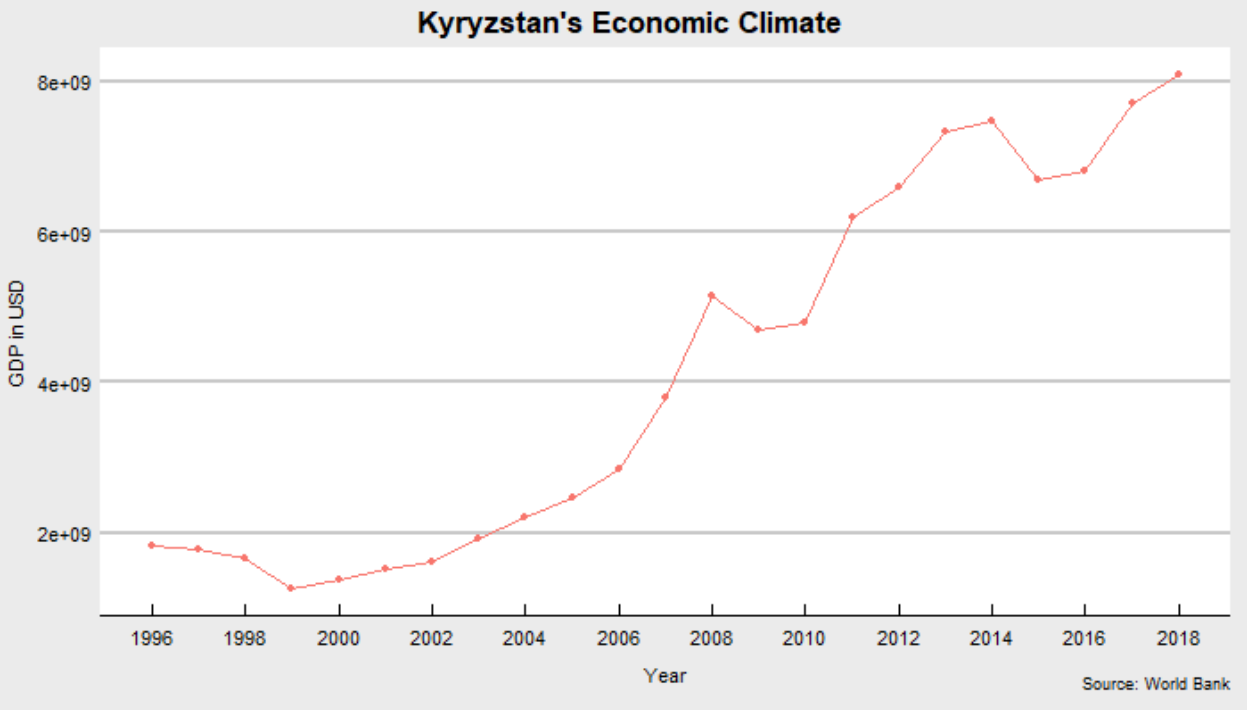


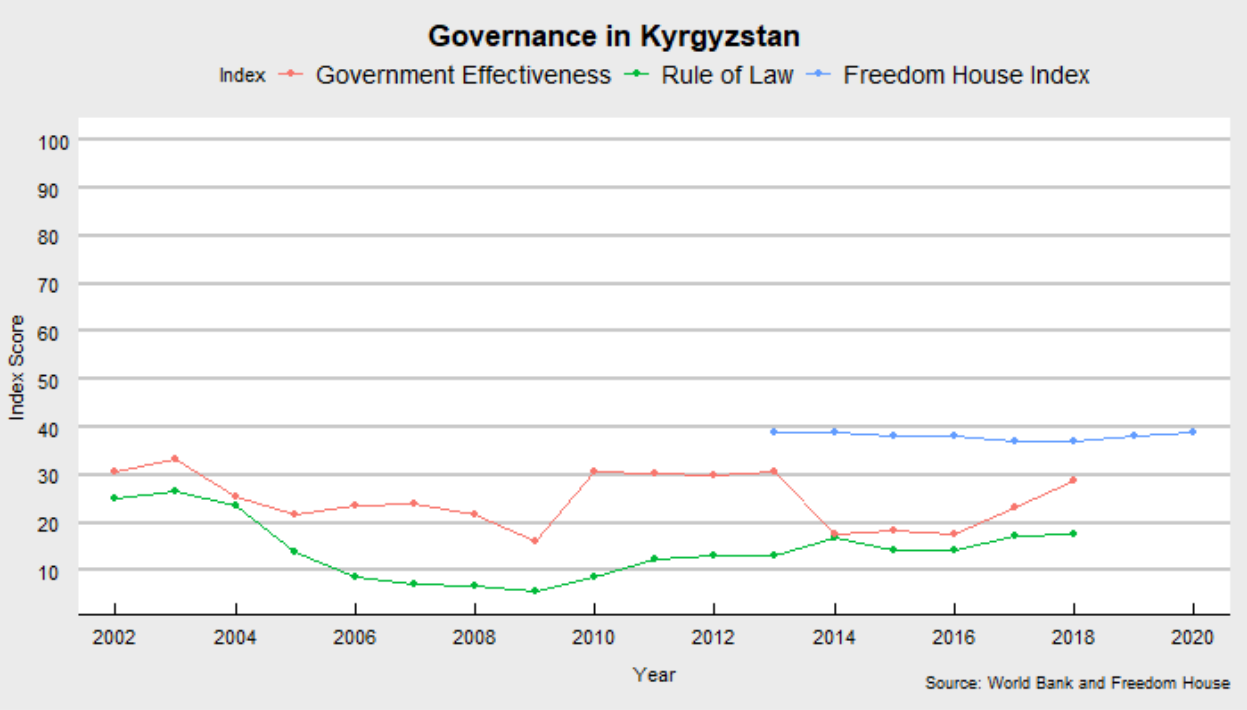
Tajikistan Figures



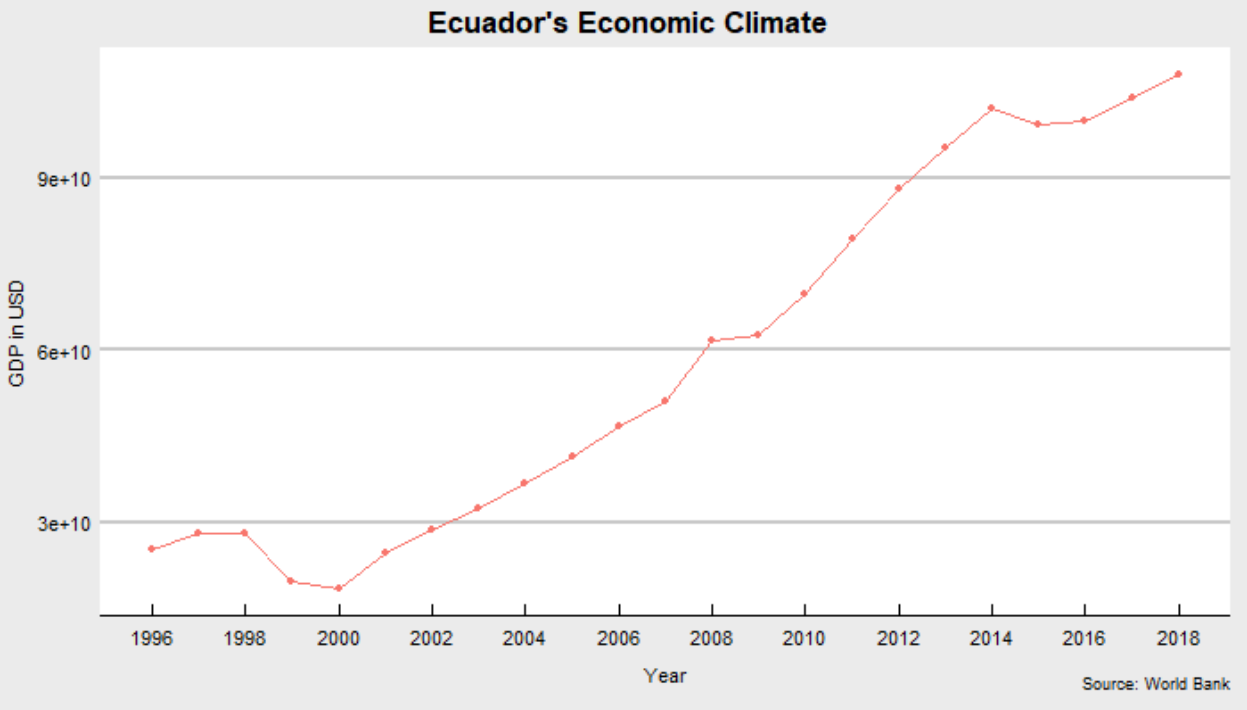


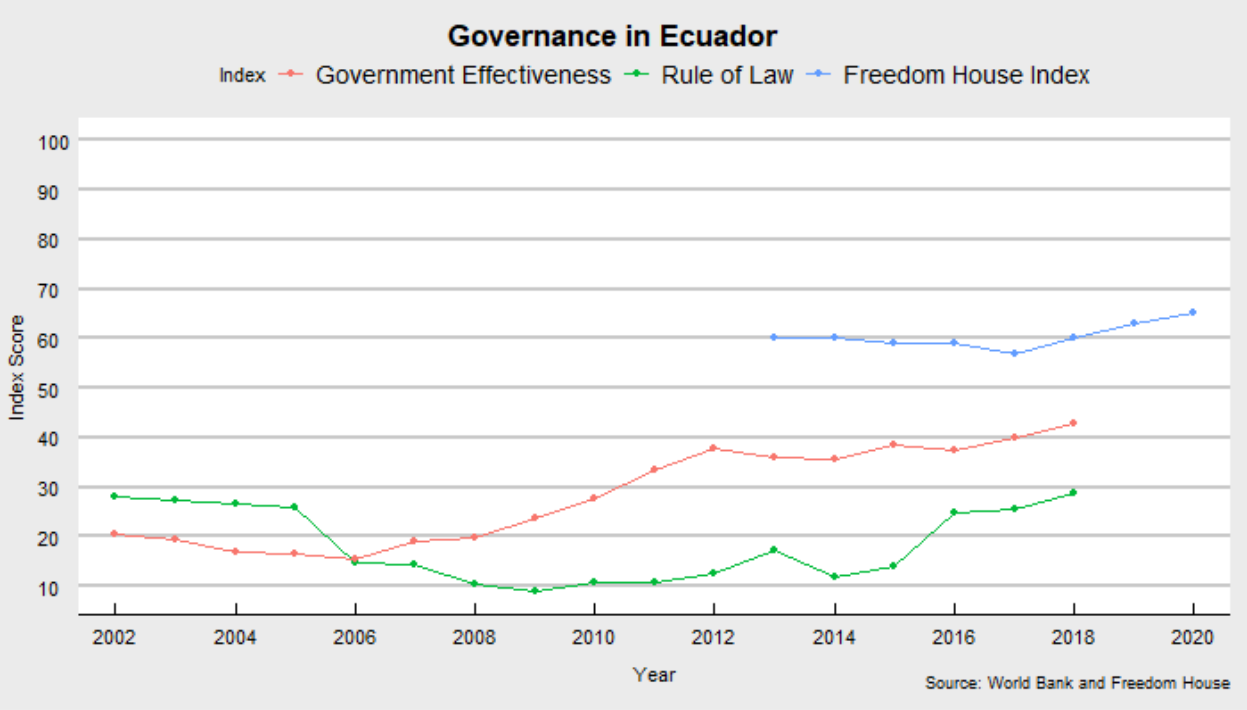
Kyrgyzstan Figures





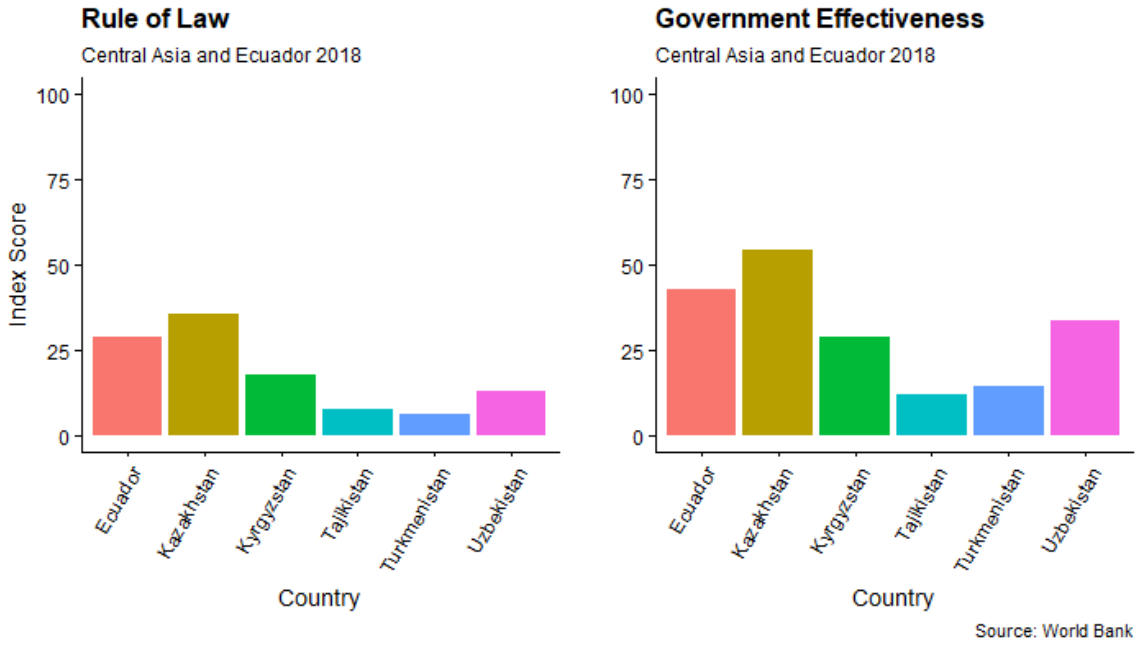
Ecuador Figures

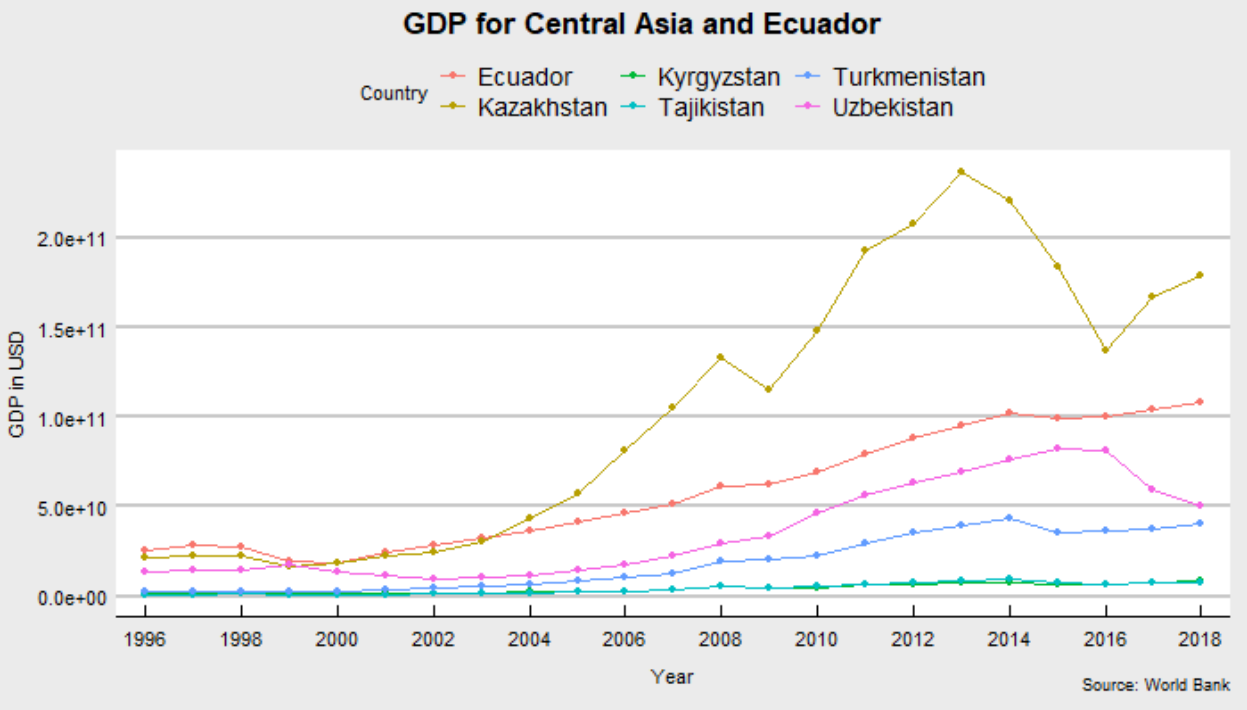


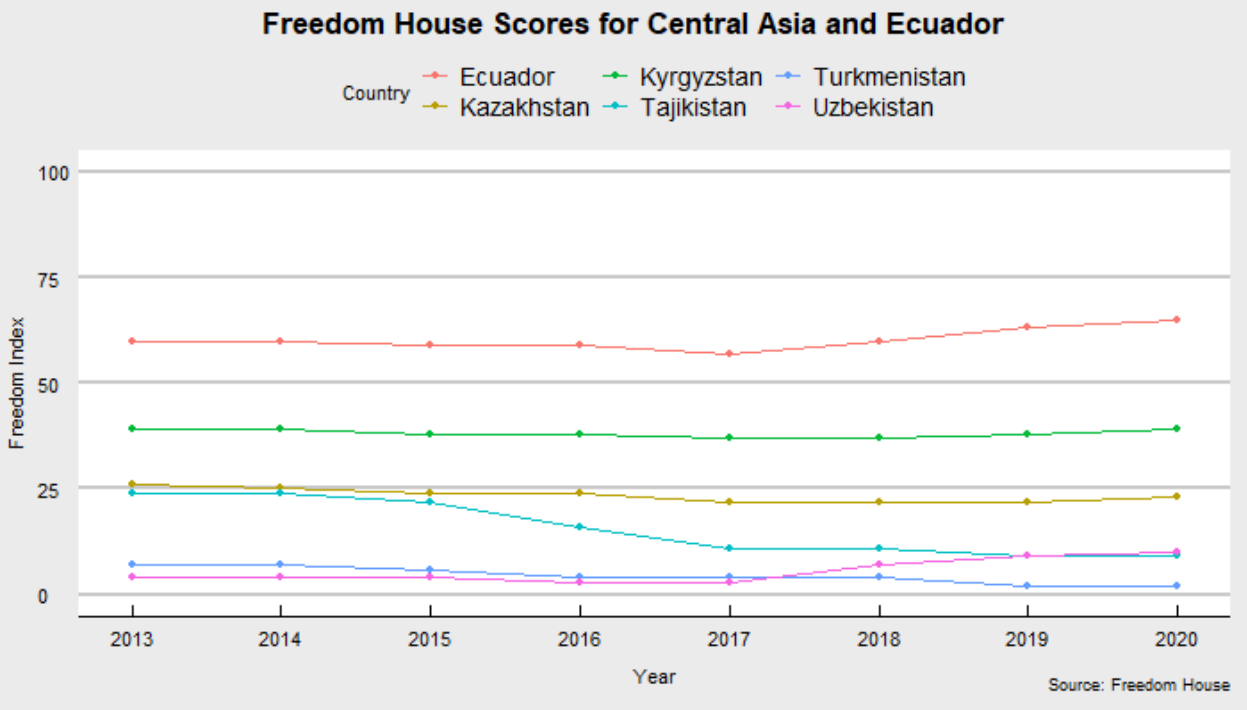


Ecuador and Central Asia Overview Tables and Figures

	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 • Data Centers
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