International Affairs Honors
Spring 2022
Anafrancesca Curry

Every Inch Covered: How China is Using Technology to Monitor and Surveil Its Citizens

Thesis Committee

Associate Professor & Primary Advisor: Dr. Robert Wyrod, Department of International Affairs, Women and Gender Studies

International Affairs Honors Council Instructor: Dr. Douglas Snyder

Second Instructor: Dr. Nancy Billica, Department of Political Science

Defense Date: March 30, 2022

Dedication

I would like to first thank every single one of my advisory board members who did nothing but affirm, support, and guide me along this process. Dr. Wyrod, although we did not know each other prior to this, you made it seem as though I had been your student for years and I immediately felt comfortable enough to ask questions and receive criticism from you (something that I am not usually the best at). I looked forward to your words of encouragement every time we had meetings. Dr. Billica, I knew the minute I received the email from the IAFS department I needed you on my board. Our brief, yet profound, encounters in my freshman year of college have continued to impact me even until today. Dr. Snyder, thank you for believing in my abilities not only as a student but as a person even when I did not believe in them myself. And lastly, I want to thank my father, David. You have done nothing but be my number one cheerleader, telling me everyday that you are proud of me and it will always be the fire beneath my feet.

TABLE OF CONTENTS

Introduction

As outdated methods of maintaining civil order, regime power and state sovereignty become less common, governments have turned to adopting new forms of technology in their place. In 2020 the People's Republic of China, PRC, was recorded to have the largest number of internet users with a projection of surpassing a platform of 1 billion before the end of 2021.[1] The sheer mass of quantitative and qualitative data the PRC has access to places high- tech surveillance methods as the most appealing way to limit threats to the state, prevent acts of terrorism, or establish a greater global- digital footprint. Under President Xi Jingping, Chinese citizens have been on the receiving end of an unavoidable network of surveillance systems that monitor them at the local, provincial, and nation-wide levels. The Chinese government's agenda of maintaining its desired social and political order is not a new phenomena as the concept of espionage dates back to the time of the Warring State in 475 B.C.[2] The idea that prosperous and successful Chinese regimes must be centered around a strong, inward looking, central government has expanded beyond the confines of basic party loyalty and now reaches to controlling the core beliefs of its citizens as well.

The rise of digital espionage within the PRC began as a domestic effort driven by government authorities' ability to collect significant information on its citizens. With official government led initiatives like Project Sharp Eyes and the Digital Silk Road becoming more

---

[1] Cheng, Evelyn. 2021. "China Now Says it has nearly 1 Billion Internet Users." CNBC. https://www.cnbc.com/2021/02/04/china-says-it-now-has-nearly-1-billion-internet-users.html.
[2] Cheng, Evelyn. 2021. "China Now Says it has nearly 1 Billion Internet Users." CNBC. https://www.cnbc.com/2021/02/04/china-says-it-now-has-nearly-1-billion-internet-users.html.

tailored to targeting specific groups in China, the question of how the PRC is using technology domestically remains.

The core of my research is to lead a descriptive and comparative analysis on the ongoing, internal efforts of China using technology as the medium to surveill and control its citizens. The current literature around the topic of China and technology is multifaceted and deeply historical, but my studies will begin following the 1980s. During this time period, China began to close their development gap with the rest of the world which sparked a surge of intellectual material and a more relaxed Communist administration. But, the years following also highlighted a time of prominent social change in China which drove Human Rights organizations such as *Human Rights Watch* and news outlets like *The Guardian* to follow and report on the events in China-making it possible for outside audiences' to be aware due to the PRC not publicizing domestic events thoroughly.

The primary goal of my research is to provide a comprehensive analysis of what is currently happening in China regarding the mass collection of citizens' data and domestic surveillance efforts through technology. I argue the goals of the PRC's increasingly invasive environment of digital espionage goes beyond its justification of maintaining international security. Furthermore, by the PRC placing political and social compliance over the privacy and rights of their citizens, the degree it has gone to is comparable to human rights violations. To support my arguments, this research will have two chapters dedicated to focusing on my primary case studies: an analysis of the current state of the surveillance network in China's capital city of Beijing, and the Uyghur minority group in the Xinjiang Uygur Autonomous Region (XUAR) located in Northwest China. The majority of this research will be an analysis on Chinese surveillance and monitoring of its citizens by the use of technology aiding as a form of

punishment towards political dissidents and ethnic minorities, while pushing for a completely secular belief system.

Research Question: How is China using technology to surveil and monitor its citizens?

Hypothesis: This research hypothesizes the PRC is using modern technology to uphold its desired society, with the Han ethnic group at the center, while using this technology to also target outside minority groups.

Literature Review

Background History of China and Methods of Surveillance

Following the Cultural Revolution in China that marked the end of Mao Zedong's rule, 1976 was a critical year for China bridging the development gap between them and other countries.[3] By the PRC reinstating the importance of maintaining control over their citizens, the appeal of cyber espionage grew as a cheap and effective means towards ensuring national security and improving industrial innovation.[4] It is imperative to present a brief overview on the history of the most significant changes in China (Early 1980- 2021) because of how deeply rooted China's policies are driven by past policies and beliefs. Scholarly research is connected through the common theme that Western entities will never be able to fully grasp the extent to which the PRC will go to maintain a " one-thought" citizen.

Historically, the first record of true technological surveillance in China occurred in 2005 when the PRC began engineering its first mass surveillance network called *Skynet.*[5] Although created in 2005, China did not reveal it to the public until 2013 when years of surveillance had

---

[3] Lindsay, et al 2015.
[4] *Ibid.,*
[5] IDG Communications. 2017. "Skynet in China: Real-time spying on citizens." CSO Online.
https://www.csoonline.com/article/3228444/skynet-in-china-real-life-person-of-interest-spying-in-real-time.html.

already passed and civil unrest began to grow within major metropolitan areas such as Xinjiang and Hong Kong due to the city's rapidly evolving security state.[6] The backlash that came with the citizen's growing knowledge on the degree to which the government was monitoring the public did not impact the government in any form and there were no direct policy changes or reaction from international entities.

By 2013 more than half of the total Chinese population had access to the internet which provided the PRC with not only the quantitative data that they wanted but also qualitative information.[7] By this fact, every citizen left a " digital footprint" where their every day movements and actions could be easily tracked and accessed. The early stages of surveillance methods in China were purely designed to monitor behavior in cities as a result of Mao Zedong restructuring the layout of towns and cities into distinct units. Within these factions, Chinese citizens each played an essential role in the newly introduced 'Project Sharp Eyes' where they reported on their neighbors activities to authorities or alerted the neighboring police forces of potential rebellion efforts. The surveillance capabilities of the PRC have evolved significantly, but the importance of data collection has remained steadfast since the concept itself was introduced. The ease in attaining mass information has become one of the many catalysts to why studying the years preceding the 21st century is crucial in answering my research question of how China is specifically using technology to monitor its citizens.

Treatment of Minorities in China

Chinese intelligence and security policies have reflected the use of technology to sustain social order by targeting ethnic minorities and or religious communities outside of the Han. The

---

[6] Zenz, Adrian, and James Leibold. 2017. "Xinjiang's Rapidly Evolving Security State." *Jamestown Foundation* 17, no. 4 (March). https://jamestown.org/program/xinjiangs-rapidly-evolving-security-state/.
[7] Lindsay, et al 2015.

primary ethnic group in China, the Han, has successfully avoided the immediate reverbations of what the PRC refers to as " battling the three evils of separatism, terrorism, and extremism."[8] According to the Official Ministry of Foreign Affairs of the People's Republic of China, 91.96 percent of China's population belong to the Han ethnic group and only 8.04 percent belong to minority ethnic groups.[9]Although my research will evaluate the PRC's treatment of minority groups from a contemporary lens that connects back to technological monitoring, that does not take away from the fact that this treatment is not a new phenomena in Chinese society. The Chinese Constitution indicates, " *All ethnic groups in the People's Republic of China are equal. The state protects the lawful rights and interests of the ethnic minorities and upholds and develops a relationship of equality, unity and mutual assistance among all of China's ethnic groups. Discrimination against and oppression of any ethnic group are prohibited*."[10] However, present day Xinjiang, which is now a hotbed of invasive technologies that harvest information for the use of the PRC, proves the state is not protecting the Uyghurs but doing the direct opposite.

The current methods of maintaining power over minorities throughout the PRC are supported by Maoist ideals dating back to his reign from 1943 to 1976. Beginning with the establishment of the PRC, Muslims and other religious minorities were initially left alone and lived away from the Han majority due to the immense influx of immigrants to China during this time period. The Cultural Revolution of 1966 in China was the start of a new wave of religious oppression as Communist Red Guards began to deface mosques, destroy copies of the Quran,

---

[8] Lindsay, et al 2015.

[9] Information Office of the State Council of People's Republic of China. 1999. "National Minorities Policy and Its Practice in China." Ministry of Foreign Affairs of People's Republic of China. https://www.mfa.gov.cn/ce/cegv//eng/bjzl/t176942.htm.

[10] Information Office of the State Council of People's Republic of China. 1999. "National Minorities Policy and Its Practice in China." Ministry of Foreign Affairs of People's Republic of China. https://www.mfa.gov.cn/ce/cegv//eng/bjzl/t176942.htm.

and outlaw the ability of Muslims to embark on the hajj religious pilgrimage.[11] The treatment and prosecution of minorities, specifically Muslim minorities, faced in China initially had the goals of maintaining civil order and preventing rebellion. This research will aim to show the role of the Chinese government in continuing the hierarchy of the Han-dominanted party in comparison to the Uyghur Muslim minority group through the medium of technilogical monitoring as a mode of instilling fear. China's governmental efforts towards its mass collection of data has significantly increased in recent years because of a perceived spike of threats towards regime stability and is justified in the name of fighting terrorism.[12] Yet, the internal efforts of the Chinese government in regards to executing power in diaspora communities reach beyond the defense of maintaining social stratification.[13]

The degree to which technology is used in the lives of individuals today makes it nearly impossible to monitor. China, in a bid to keep up with its maturing high-growth industry, has leveraged information technology to integrate its firms into the global economy, modernize its infrastructure to instill security measures, and continues to prioritize Internet usage to penetrate into the data of its citizens.[14] This event is referred to as the ' *Informatization of China*' and is how China hopes they will solidify its presence as a formidable world power and maintain its desired civil and social society. By 2013 China was on record as the world's fastest growing Internet population with over 600 million users, and despite the Chinese government's continued censorship of content its internet population has currently hit almost 1 billion users.[15] A CNN

---

[11] Hammond, Kelly A. 2019. "The history of China's Muslims and what's behind their persecution." The Conversation.
https://theconversation.com/the-history-of-chinas-muslims-and-whats-behind-their-persecution-117365.
[12] Richardson, Sophie. 2017. "China: Minority Region Collects DNA from Millions." Human Rights Watch.
https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.
[13] Leung, Jocelyn. 2010. "The Chinese Communist Party's Treatment of Ethnic Minorities." E-International Relations. https://www.e-ir.info/2010/01/10/the-chinese-communist-partys-treatment-of-ethnic-minorities/.
[14] Lindsay, et al 2015.
[15] *Ibid.,*

article published in 2019 claimed the Chinese government sponsored hackers to place monitoring implants into cellular phones to specifically spy on the Uyghur minority group. The article supported this idea by examining a report conducted by cybersecurity company Volexity whose specialized span to track the direct ways the Chinese government monitors Uyghurs. The report was released September 2nd, 2019 and it revealed that specific websites were tailored for a Uyghur audience and upon a user's visit to the website, their phones would be hacked without their knowledge. Adam Segal, the director of the Digital and Cyberspace Policy program on the Council of Foreign Relations, referred to this phenomena as "watering hole" attack, the tactic that allows a hacker to compromise sites their targets are likely to go to rather than seek them out directly.[16] The significance of this is that it illustrates how the development of crescively intrusive technology combined with a lack of clear safeguards or guidelines control the level of freedoms for citizens in China seem to vary amongst different groups of people.

A belief amid scholars regarding the future impacts of new technologies in China tend to focus on the ability of the state to maintain civil society and the capabilities technology holds to execute state censorship and execute these efforts.[17] The question of how China's application of cyber espionage is part of the government's vision of social, political, and economic power continues to grow as technology advances. Through my findings I will be able to show how internal surveillance and monitoring is playing out in comparison of the favored Chinese majority (Han ethnic group) vs the most marginalized group (Uyghurs).

The core of current research surrounding China's use of AI and what specific new forms of technology the government is using has been recorded within the last 40 years. The most primary of which have been models of academic journals, Western and Chinese news articles,

---

[16] Collier, Kevin. 2019. "China hacked iPhones and Android devices to target Uyghur Muslims." CNN. https://www.cnn.com/2019/09/04/politics/china-uyghur-hack/index.html.
[17] Lindsay, et al 2015.

books that draw the line relating China's overall history with the rates of development in the present day, and so on. A belief held by predominantly Western scholars is that a greater knowledge of the complex system of China's centralized one-party government, can show the trajectory for the future role of technology in China.[18] Groups such as the Eighteenth National Party Congress run by current Chinese President Xi Jingping, the Central Military Commission, and People's Liberation Army, have been recorded as key actors in maintaining Chinese cyber policies, domestic politics, and governmental protocols. Journalist Owen Churchill, a specialist in technology and culture in China, goes into depth about why the Chinese State Council made the decision to implement the New Generation Artificial Intelligence Development Plan.[19] Comparably, a recent translation of a journal based in China writes about the goal of the New Development Plan, a five- year plan for resource rich areas in China to see great social and economic development that will also strengthen the general population of China's knowledge of AI and improve the level of precision in public services through technology to increase the quality of life for Chinese citizens.[20]

The existing research and literature surrounding the topic of Chinese cyber-technology are common in the fact that Western entities or any country outside of China will never truly know the extent of how deep China is going in cyber-surveillance. An example of this ideal of stated in a Harvard University research article written by Jeff Jones who is one of the school's National Security Fellows, argues the extent of Chinese cyber espionage activities is likely significantly more serious than what news organizations and industry representatives are

---

[18] Mitter, Rana. 2019. "How the one-party state may shape our future." The World Economic Forum. https://www.weforum.org/agenda/2019/08/how-the-one-party-state-may-shape-our-future/.
[19] Churchill, Owen. 2018. "China's AI Dreams." ProQuest 553, no. 7688 (January): S10-S12. DOI:10.1038/d41586-018-00539-y.
[20] Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania. 2017. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)." New America. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

reporting due to the clandestine nature of cyber espionage, monitoring intrusions within China simply go undetected.[21] My analysis will combine sources and data from both Chinese based research as well as sources outside of China to ensure the information I obtain will not come from a primarily Western lens. The goal of my thesis is to build upon the already existing narrative of China being an unignorable tech superpower, and then go even further to illustrate what desired society they want to achieve through technology.

The bulk of my research will be an analysis on Chinese surveillance and monitoring of its citizens by the use of technology aiding as a form of punishment towards political dissidents and ethnic minorities, while pushing for a completely secular belief system. There is still no central machinery or set of rules that is public knowledge in China that states an agreed upon governmental position of what they can or cannot have access to from the population. In an academic report published in 2014, research analyst for news outlet CNBC Amy Cheng highlights the implications of the multifaceted regime of cyber control in the capital city of Beijing. Her findings are relevant to this research because they show the direct ways the PRC utilizes outlets outside of their primary government to execute data mining, social media censorship, and the implementation of invasive nation-wide security systems.[22]

Despite the efforts made by the Chinese Government to spy on its citizens, it is important to acknowledge that social media and internet based censorship that is funded and sponsored by the PRC includes independent entities as well. In their efforts to highlight how the technological espionage in China reaches outside the will of the government, authors Taiyi Sun and Quansheng Zhao lead a discourse about the culture surrounding media in China. They write that Chinese culture and the overarching role that history plays in the concept of domestic espionage is one of

---

[21] Jones, Jeff. 2020. "Jeff Jones." Belfer Center. https://www.belfercenter.org/person/jeff-jones.
[22] Cheng, 2014.

the many driving factors of the monitoring efforts in China today. Specifically, the shift towards non-traditional media practices and away from governmental reliance in China can be credited to both the pluralization of internet content and the wave of new-media.[23]

Relating back to Chinese Intelligence operations internally, there is a trend of common underlying aspects that vary in influence, but remain similar in their goals. Written in the Journal of Chinese Political Science, author Jonathan Hassid writes about how the sudden increase of growth in China's internet users directly correlates to the ability for the government and the "higher ups" in the state to exercise and maintain control over its citizens. By combining newspaper articles, blog posts, and secondary sources, Hassid and researchers alike argue Chinese media coverage is 'distorted by censorship and corruption to the benefit of China's entrenched interests'.[24] Another common theme throughout modern literature is that there is a clear disparity between favoring the ethnic majority of the ' Han' group vs any other ethnic group who are seen as out groups within China.

As more research surrounding the PRC's use of technology is revealed through human rights reports, the idea that monitoring and surveying citizens in China is not unique to one group of people has become increasingly evident. Through my analysis of the connections between China's technological presence in Beijing and the Uyghur minority group in the Northwest, I will build on the existing studies of why China's data collection abilities are a reason for further study. The issue of the PRC's efforts to exercise influence in diaspora and minority groups sparks an important, and for some dormant, question of how China perceives such communities as their own property.[25] This supports my research's claim that the PRC is using high-tech surveillance to

[23] Sun, Taiyi, and Quansheng Zhao. 2021. "Delegated Censorship: The Dynamic, Layered, and Multistage Information Control Regime in China." *SAGE Journals*, no. 1 (May), 1-31. 10.1177/00323292211013181.
[24] Hassid, Jonathan. 2020. "Censorship, the Media, and the Market in China." *Journal of Chinese Political Science* 25, no. 2 (March, 2020): 285-309.
[25] Lindsay, et al 2015.

subdue minorities in not only metropolitan cities, but also in resource rich areas in the country. The combination of two case studies to connect back to the bigger picture of China's motives pertaining to their continued espionage towards its citizens internally through a highly-crafted digital domain will show my audience that there is not one group China is trying to monitor, rather it is a widespread phenomenon.

Methodology

Comparative and Qualitative Analysis

The primary bulk of my research will be obtained through media outlets such as the Human Rights Watch, CNN, BBC News and other forms of public press from both Western and Chinese entities. Despite the Uyghurs being one of the 55 officially recognized ethnic groups in China, advocacy groups alike are bringing more attention to the Northwest Region of Xinjiang and the potential for the state to be held accountable for crimes against humanities. I will analyze the information I find regarding the events happening in Beijing to those of the Uyghurs and will use it as the foundation for the third comparative chapter.

Studies continue to place importance on highlighting the rates that technological influence from the Chinese government is structured around ensuring the beliefs they align with are not being rejected by minority groups or those outside of the ethnic majority group[26]. The informatization of China is focused on acquiring data which can then be used for political advancements, preventing civil unrest, and maintaining order, but it is also a fallback to use in case there were to ever be an upheaval of any scale in these areas. The notion that China has a '

---

[26] Buckley, Chris, and Paul Mozur. 2019. "How China Uses High-Tech Surveillance to Subdue Minorities." The New York Times, May 22, 2019. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

precise, all-seeing, and infallible pair of policing systems and surveillance methods'[27], is the driving scare tactic the government uses on its citizens- whether in the capital or one of the 55 recognized ethnic minorities.[28] While there are many minority groups that are being subjected to unfair treatments, the Uyghurs are the most spoken about in current studies and news which is why they are one of my case studies. The method of comparative analysis will highlight the tangible ways in which the PRC is not only violating human rights but simultaneously targeting the Uyghur ethnic group because they are the largest minority group which poses a threat to the Han majority.

---

[27] Buckley, Chris, and Paul Mozur. 2019. "How China Uses High-Tech Surveillance to Subdue Minorities." The New York Times, May 22, 2019. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.
[28] "Uighurs: Western countries sanction China over rights abuses." 2021. BBC News. https://www.bbc.com/news/world-europe-56487162.

Chapter Two

Beijing Case Study Analysis

The current state of the technological surveillance network in Beijing once began as an unattainable cyber dream is now an all-seeing, invasive, and constantly updating plethora of grid-style surveillance nexus. With a population of 21.7 million citizens in 2021, Beijing is China's technological experimentation ground and is a goldmine of data collection efforts as well. The Chinese government has long relied on Artificial Intelligence and CCTV to catch potential criminals or spot regime resistance before it occurs, yet, because of the rapid modernization and development of technology the government has begun using it in ways that used to seem unimaginable. The potential of economic prosperity and increased geopolitical control in Beijing has driven China's government to obtain mass amounts of quantitative and biometric data. The installation of 626 million surveillance cameras equipped with modern day facial recognition software in 2020 in Beijing has allowed China's government to procure personal information without regulation.[29]

The CEO and founder of Digital Barriers, a company that specializes in global surveillance, describes China's push for increased cyber-espionage has enabled a segregated surveillance system in Beijing.[30] The invasive technology that reinforces the current state in China is part in parcel of a government system that will not decrease rule or control. In addition to all basic security infrastructures being put into effect by Beijing, it is also the hub of increased

---

[29] Maranto, Lauren. 2020. "Who Benefits from China's Cybersecurity Laws? | Center for Strategic and International Studies." Center for Strategic and International Studies |.
https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.
[30] Maranto, Lauren. 2020. "Who Benefits from China's Cybersecurity Laws?

private networks, intrusion detection and prevention systems, and network access control

systems that serve as the framework for the entire country.[31] In this chapter, I will examine the

case of Beijing, China's capital and third largest city, to reveal how the PRC is using surveillance

technology to monitor and control its citizens. The case of Beijing is significant because it

illustrates how the PRC uses such technology to regulate the dominant Han, urban and middle

class portions of its population, and reaches to almost every corner of the city. This chapter is

divided into two subsections. First, I will discuss the timeline of the development of modern

surveillance technologies and its connection to Beijing. I will then turn to how the social unrest

in both Beijing as well as neighboring cities has greatly contributed to the increase of espionage

endeavors by the Chinese government. Finally, I examine how all of these factors contribute to

the larger picture of China's surveillance network. I conclude my chapter with how the PRC is

not only enforcing these technologies in major cities, but also in provinces where minority

groups are the dominant ethnic groups and the significance of that.

The Development and Current State of the Beijing Surveillance Network

Facial recognition software is not limited to government officials and does not require

cooperation from institutions that do not want to partake in the use of the technology.[32] The

surveillance networks, cameras, and motion sensors are directly controlled by both local and

state level authorities. Beijing police use the information they received from the surveillance

grids to generate lists of citizens, virtual alarms for who a certain individual meets with, or

---

[31] Lindsay, Jon R., Tai M. Cheung, and Derek S. Reveron, eds. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. N.p.: Oxford University Press.
[32] Buckley, Chris. 2019. "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims (Published 2019)." The New York Times. https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html.

updates of people at any hour of the day.[33] Although the Chinese government and President Xi

Jingping have made their surveillance policies and internet monitoring efforts very clear,

pushback amongst Beijing's citizens has become increasingly popular. In an article published by

Quartz Research Media Group, author Jane Li reflects on the opinions of the surveillance state

from Beijing citizens. Following an interview with a Chinese Journalist, Muyi Xiao claims that

in response to the PRC's emphasis on digital security, more citizens will start to maintain their

individual protection against surveillance efforts. Xiao follows this claim by asserting that if the

economy of China continues to develop at its current rate, the PRC will tolerate little personal

rights but the process will be very gradual and slow.[34] In the same article, Li examines MF

Socket, a cell phone app whose use base is primarily in the XUAR region and has been found on

users phones following visits to police stations or one of the security checkpoints throughout

Beijing. A user by the handle "*FuckMFSocket*", in a bid to push back against the app, leaked a

code online that assists in hiding users personal information (contacts, messages, location) from

the government.[35] It is worthy to note that Li was unable to reach users with the MFSocket

installed on their phones outside of Xinjiang region to discover if they downloaded the app

willingly or not.

While surveillance networks can be downloaded without the knowledge of users, there

are more apparent and clear methods of technological surveillance entities within Beijing as well.

Following the installation of four cameras and several phone scanners referred to as IMSI

catchers in the Shijiachi housing complex, one of the residents' Agnes Ouyang stated, " *Each*

[33] Buckley, Chris. 2019. "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims."

[34] Li, Jane. 2019. "Chinese people are pushing back on Beijing's digital surveillance." Quartz. https://qz.com/1659328/chinese-people-are-pushing-back-on-beijings-digital-surveillance/.

[35] Li, Jane. 2019. "Chinese people are pushing back on Beijing's digital surveillance." Quartz. https://qz.com/1659328/chinese-people-are-pushing-back-on-beijings-digital-surveillance/.

person's data forms a trail. It can be used by the government and it can be used by bosses at the big companies to track us. Our lives are worth about as much as dirt."[36] Although the system was implemented by local police, over the first four days of the software establishment 482 residents' names, marital and family status, and records of their loyalty to the PRC were acquired by unprotected servers.[37] The primary function of the system is to connect all of the data received together and then identify any irregularities of a citizen. The government also has the authority to add people to an official blacklist document that makes it easier to share the information local police collect up the chain of command to the Central Ministry of Public Security in Beijing.[38]

An essential aspect of the complexity of the current civilian surveillance apparatus in Beijing is the relationship between surveillance systems administered by the PRC, those operated by local authorities and created by big data tech corporations. There is a growing hesitancy from state-run companies in Beijing to share lucrative data with local authorities because of the value the data has to the ' higher-ups' in the government. The disconnect between the two entities has resulted in local police purchasing their own personal trackers instead of adhering to the regulations of the Central Ministry.[39] The fight for power in maintaining Beijing's authoritarian regime is supported by the completely unregulated, citywide surveillance infrastructures. Baidu, one of China's leading tech companies, has long exploited and gathered information in Northern Beijing yet it does not report directly to the PRC. Any information the company gains from scanning their employees faces when they walk into work is collected for their use. [40]

---

[36] Buckley, Chris. 2019. "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims."
[37] Ibid.,
[38] Ibid.,
[39] Ibid.,
[40] Larson, Christina. 2018. "China's AI Imperative." *Science Mag* (Beijing), February 9, 2018, 628-630.

Companies in Beijing are also starting to develop the Cambricon-1A chip that is inserted into cellular devices that will enable the government to use facial recognition, location services, and audio monitoring. Christina Larson writes the Cambricon-1A chip shows that China's technological advantages go further than internal government efforts because of the sheer size, scant privacy protections, and amounts of data within China.[41] Chris Bukley and Austin Ramzy reflect on the perspective of larger corporations and tech companies in China stating that although they supply the technology to the government they are not responsible for how it is used.[42] The fact that both the government and separate companies being able to use any method of espionage with uncurbed freedom blurs the line between ensuring safety and eliminating personal freedoms entirely.

The Personal Information Security Specification that took effect in May 2018 extended the PRC's control over surveillance data to promote the "secure development of technology in China."[43] The law solidified that any data stored within China was able to be subjected to any government driven security checks at any time. Yet, the intentional obscurity of data protection laws from the PRC has left Chinese citizens vulnerable to their personal data being sold, leaked, or taken without their knowledge.[44] Although the narrative of cyber-espionage becoming progressively eminent in Beijing, every aspect of life will continue to be watched and recorded at accelerated rates. When comparing the reasons of *why* the government is using invasive technology methods, it is crucial to acknowledge it is not only for security measures. For example, a professor at a university in Beijing used a facial recognition scanner to ensure the

---

[41] Larson, Christina. 2018. "China's AI Imperative." *Science Mag* (Beijing), February 9, 2018, 628-630.
[42] Buckley, Chris. 2019. "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims."
[43] Maranto, Lauren. 2020. "Who Benefits from China's Cybersecurity Laws? | Center for Strategic and International Studies."
[44] Maranto, Lauren. 2020. "Who Benefits from China's Cybersecurity Laws? | Center for Strategic and International Studies."

attention and interest of his students in a bid to punish students who were not attentive.[45]

Similarly, a toilet paper dispenser neighboring the public Temple of Heaven in Beijing is

reported to scan faces to prohibit civilians from using what the government deems to be too

much paper.[46] By Chinese authorities enforcing the PRC's guidelines of a surveillance state they

are able to gain access to the personal security information of any citizens in seconds. A Wuhan

policeman explained in A New York Times article that the surveillance systems they are

implementing must be able to comprehensively collect the identity of all internet users in public

spaces, their internet behavior, location, movement, and identifying information about their

phones.[47] Similarly, Ma Ce, a lawyer specializing in facial recognition issues in Hangzhou

revealed that Chinese citizens are worried that because facial recognition is often obligatory for

accessing a service, with no alternative, the technology isn't foolproof.[48] The methods used to

obtain data from the general public in Beijing reflect the government's inclination to further

idealistic and authoritarian views.

Following 2003, a five-year projection plan aiming to create a network that covered

100% of China was introduced and investments towards physical surveillance capabilities

increased dramatically. Named Project Sharp Eyes, the plan's goal was to record and gather data

from all public spaces- streets, transportation centers, schools- eventually reporting it back to

government officials. In 2012, Beijing and the Chinese government introduced Skynet (天网,

Tianwang) a nation-wide mass surveillance system. Skynet focuses primarily on installing

---

[45] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash." Fortune. https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/.

[46] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash."

[47] Krolik, Aaron, and Paul Mozur. 2019. "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers (Published 2019)." The New York Times. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.

[48] Crossman, Rozena, and Frédéric Schaeffer. 2021. "In China, How People Are Pushing Back On Surveillance State." Worldcrunch. https://worldcrunch.com/tech-science/in-china-how-people-are-pushing-back-on-surveillance-state.

cameras and video surveillance that would connect to facial recognition algorithms throughout the nation.[49] According to Chinese state- run reports, Skynet is able to scan and analyze the data it receives in less than one second with up to 99.8 percent accuracy and has no technical limitations. Yet, this statistic is greatly criticized as the level of definitive up-to-date information on the PRC's surveillance objectives are not entirely accurate, Dahlia Peterson, a Center for Security and Emerging Technology Research Data Analyst reports.[50] As of 2022, the Skynet directive continues to evolve as a New York Times article affirms that it is being used in building complexes and housing developments where facial recognition controls the ability for people to enter and leave the buildings.[51] The data received from the photos and videos are sent to local security networks and stored in databases whose main job is to connect the information gathered to community grid style security.

Although the PRC publicly stated the project was for " improving public safety and security", a 2019 survey done by the Nandu Personal Information Protection Research Center in Beijing recorded that 57% of participants claimed to be concerned about their movements and private information being tracked.[52] According to the same survey 74% of participants said if they had the choice they would rather have analog identification methods rather than facial recognition or AI.[53]In stark contrast with the involuntary and intrusive methods of facial recognition currently in place in Beijing, the Analog Identification method is a downloadable software that places the user in charge of the amount they share with the government. This

---

[49] Gershgorn, Dave, and Dahlia Peterson. 2021. "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space." Center for Security and Emerging Technology.
https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/.
[50] Gershgorn, Dave, and Dahlia Peterson. 2021. "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space." Center for Security and Emerging Technology.
https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/.
[51] *Ibid.,*
[52] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash."
[53] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash."

statistic demonstrates that regardless of what the majority wants, the Chinese government will not waiver from their methods. Although the results of the survey are not uncommon amongst Beijing citizens, the PRC has already built the most exhaustive web of surveillance methods in the world.[54]

Social Unrest Leading to Surge of Security

As briefly noted earlier, a key factor fueling the PRC's focus on surveillance in Beijing, and similar cities, is growing anti-government sentiment, including occasional social unrest in the capital. Beijing's role in the development and enforcement of invasive, cyber monitoring programs is that a majority of the technical companies that create the software are based out of the capital. The nationwide riots and protests are incited by the general population's determination to foster a greater global awareness about how the PRC is controlling their lives through cyber-espionage. Beijing's cyber espionage and digital monitoring capabilities are conditional upon the degree of state and government sponsored technology production and generation. Equivalently, the vast infrastructure of closed-circuit television (CCTV) surveillance throughout China is pertinent to illustrating China's strategic surveillance control regime. As of 2021 AI firm Watrix, created by Huang Yongzhen, designed a software that is able to identify individuals up to 50 meters away based upon slight movements of their walk in large groups.[55] The significance of this is that Watrix's software is identifying the civilians who are taking part in the Beijing protests, reporting them to the government and eventually accusing them of anti-party charges.

---

[54] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash."
[55] Campbell, Charlie. 2019. "The Entire System Is Designed to Suppress Us': What the Chinese Surveillance State Means for the Rest of the World." TIME. https://time.com/5735411/china-surveillance-privacy-issues/.

By labeling Beijing as the backbone of technological development efforts and policies, the Chinese Communist Party is working against the civil, political, and social rights of their citizens by acts like erasing personal or social freedoms.[56] In this section, I argue that the PRC uses protests as a means to capitze off of increasing surveillance networks and digital authoritarianism. While Beijing is at the forefront of expanding the PRC'S technological and espionage capabilities, the bilateral relationship between the government and the city reaches every corner of the country. Therefore, the coordinated steps the PRC is taking in Beijing are previews of what the nation will look like in the future.

Journalist Paul Mozur reveals that cities such as Hong Kong are beginning to take to non-traditional methods of protest against Beijing's increasing security state. In 2019, protestors began a citywide charge against Beijing in fear that the city would disappear and become a 'shadow world of surveillance, censorship and digital control led by the capital.[57] The significance of the Hong Kong riots illustrated that despite the PRC's efforts to accelerate its desired society, it is not maintaining control over the people. The riots reached unprecedented levels of traction in Hong Kong as protestors covered cameras in the streets with a reflective rubber coating to prevent themselves from being identified and possibly obtained by the police.[58] Following the enforcement of the new National Security Law of China in 2020, the pro-democracy movement in Hong Kong sparked outrage from Beijing and its leaders took immediate action. In a bid to combat the movement, Hong Kong's primary newspaper, *The Apple Daily,* was eradicated by Beijing in June of 2021 directly mirroring the intensity of the riots.[59]

[56]Human Rights Watch. 2021. "Hong Kong: Beijing Dismantles a Free Society." Human Rights Watch. https://www.hrw.org/news/2021/06/25/hong-kong-beijing-dismantles-free-society#.
[57] Qiqing, Lin, and Paul Mozur. 2019. "Hong Kong Takes Symbolic Stand Against China's High-Tech Controls (Published 2019)." The New York Times. https://www.nytimes.com/2019/10/03/technology/hong-kong-china-tech-surveillance.html.
[58]Qiqing, Lin, and Paul Mozur. 2019. "Hong Kong Takes Symbolic Stand Against China's High-Tech Controls
[59] Human Rights Watch. 2021. "Hong Kong: Beijing Dismantles a Free Society." Human Rights Watch.

Escalating government opprobriums are calculated and meticulously monitored by Beijing's surveillance systems that continue to justify one-party rule and communist thought with no resistance.

State actors and government officials must ensure regime power while maintaining absolute cyber-monitoring capabilities. Best said by authors Taiyi Sun and Quansheng, China's government implementation of invasive technological networks is defined as interactive authoritarianism. Interactive authoritarianism is a discriminative approach that targets individuals under certain conditions through frequent interactions, heightened state power and ensuring mutual cooperation[60]. The escalation of security measures in response to the protests in Hong Kong are parallel to the dismantling and inability for individuals to form independent thought throughout China. By using the vast network of surveillance, the PRC is able to identify protestors and silence them by jailing them, threatening them or their family, or label them enemies of the state. In response to the ongoing protests the government responded by monopolizing media outlets, mobile platforms (cellphones), and the internet.[61]

By connecting an individual's every technological interaction to physical movements such as going to work, the PRC gains quantitative data that is used to maintain absolute control over a desired area. The phenomenon of interactive authoritarianism supports the notion that a regime is successfully maintained by increased political control through methods that have no limitations. The population in Beijing and other Chinese cities is being controlled through an invasive apparatus that spans delegated censorship in social media outlets, independent networks, and non-governmental entities to suppress any anti-government thought.

[60] Sun, Taiyi, and Quansheng Zhao. 2021. "Delegated Censorship: The Dynamic, Layered, and Multistage Information Control Regime in China." SAGE Journals, no. 1 (May), 1-31. 10.1177/00323292211013181.
[61] Sun, Taiyi, and Quansheng Zhao. 2021. "Delegated Censorship: The Dynamic, Layered, and Multistage Information Control Regime in China." *SAGE Journals*, no. 1 (May), 1-31. 10.1177/00323292211013181.

Beijing has long fought for a secular-citizens that embody each facet of the Communist Party's agenda with little to no pushback from the people. Although there have not been direct attacks on the government there has been an increase of public stabbings, bombings, and protests beginning in 2009. In 2014 the PRC identified what they saw as the three feared components of separatism, extremeism, and terrorism, and used this narative to combat anti-government and anti-Chinese thought.[62] This depicts that the non-Han citizens who are viewed as others are believed to need constant surveillance and monitoring because of the overarching goal of preventing terrorism. Additionally, it also justifies increased surveillance methods and networks in prominent cities such as Beijing.While existing technology in China is not focused on monitoring a singular type of individual, it is designed to procure specific data whether or not it is deemed useful at the current time.

The methods of maintaining power of the PRC are not limited to technological surveillance. By instilling fear that the government can observe every action and part of a person's life, the PRC is eliminating the possibility of citizens even thinking about going against the government out of fear. An example of the use of fear mongering to gain information can be observed in 2018 when a railway station deputy police Chief, Shan Jun, caught a heroin smuggler in the street without questioning, torturing, or interrogating him. The author of the New York Times article, Paul Mozur, defines this method as *panopticon,* the concept that civilians will obey law and order if they subconsciously always believe they are being watched and do not think otherwise.[63] The Communist regime in China makes compromise and internal stability conducive to the government's inability to appear weak to outside entities.

---

[62] Buckley, Chris. 2019. "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims."

[63] Mozur, Paul. 2018. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras (Published 2018)." The New York Times. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

When faced with public acts of defiance the regime will default to eliminating or punishing the subject instead of reasoning. In the *Journal of East Asian Studies* Li Shao connects the determinants of political criticism in China to the government's desire to maximize popular support among the population. Shao claims that when the regime is placed under fire or scrutiny by local protesting officials of any level will not offer compromises due to the regime then losing control of public affairs. Additionally, they will avoid communicating with protestors at all levels because it weakens the one-party rule and poses a direct threat to the framework of the regime.[64] The degree of which the PRC maintains majority support of the public is explicitly reliant on their ability to respond immediately to both political and social unrest. As the surveillance state continues to grow in China, citizens have begun pushing back on the policies in ways outside of protesting such as non-violent public art installations. Frédéric Schaeffer, an author for the online news-site WorldCrunch, outlines a performance in February 2021 on Xingfu Street in the heart of Beijing. A dozen citizens dressed in reflective vests formed a single file line where they were either hunched to the ground or hesitantly walking sideways almost as if they were being held hostage or dodging a bullet, Shaeffer recalls.[65] The protestors were participating in a performance directed by Chinese artist Deng Yufeng to try and adequately portray how challenging it is for citizens to avoid the video cameras and CCTV throughout the capital.

The presence of surveillance systems in Beijing have become the blueprint for a nation-wide implementation of espionage softwares and networks. President Xi Jingping has made the development of modern surveillance technologies a primary focus of the PRC's government and security efforts which has made the technology almost unavoidable in all

---

[64] Shao, Li. 2018. "The Dilemma of Criticism: Disentangling the Determinants of Media Censorship in China." *Journal of East Asian Studies* 1 (18): 279-297. 10.1017/jea.2018.19.
[65] Crossman, Rozena, and Frédéric Schaeffer. 2021. "In China, How People Are Pushing Back On Surveillance State." Worldcrunch.
https://worldcrunch.com/tech-science/in-china-how-people-are-pushing-back-on-surveillance-state.

aspects of life. Xi's justification for the increased surveillance has been to combat the threat of terrorism in not only Beijing and major cities but also in areas where the ethnic majority is not the Han. Despite civilians in Beijing knowing they are being monitored, there has still been pushback from the population in forms like peaceful protests, public art installations, and large rallys. This consequently results in more security measures coming from the government, resulting in a growing intolerance towards political and social freedoms such as the freedom of expression. Yet, the security measures are not only enforced in-response to an action, they are targeting peaceful minority groups who have done nothing but simply exist. My next chapter will examine how the PRC uses surveillance networks not only to its favored majority group but also the largest minority group, the Muslim Uyghurs, in an attempt to surpress their beliefs and values.

Chapter Three

Uyghur Minority Case Study Analysis

The Northwest Region of Xinjiang where the Uyghurs primarily reside is on the receiving end of an intense, biometric data collection effort and an oppressive cultural execution that began in 2001.[66] The city of Xinjiang which is often referred to as a virtual cage is now home to a complex web of invasive technology networks that surveilles every citizen's movements such as their electricity usage, internet activity, travel activities, or when they leave and enter their homes. President Xi Jinping has stuck by the belief of Han superiority and the ways that identifying within the Han majority encapsulates the definition of what it means to be a true Chinese citizen. Writing in *The Atlantic,* journalist Ross Andersen notes that the "re-education" centers where Uyghurs were detained and forced into by the thousands is now the largest internment of an ethnic-religious minority since the fall of the Third Reich in 1945.[67] The combination of high tech surveillance networks and detention centers has led to Xinjiang becoming the model of a dystopian and highly controlled city. Supported by a modern technological system that enforces the concentration-camp like environment the surveillance technology in Xinjiang is geared towards suppressing, controlling, and monitoring the Uyghur Muslim minority.

Although any citizen the PRC sees as a threat to the state is subject to questioning and other security measures, the Uyghurs are also forced to denounce their belief system, religion, and culture. In his book *The Perfect Police State,* Geoffrey Cain argues that the goal of the PRC in Xinjiang is to completely erase the identity and history of the Uyghur people in hopes of

---

[66] Richardson, Sophie. 2017. "China: Minority Region Collects DNA from Millions." Human Rights Watch. https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions#.
[67] Andersen, Ross. 2020. "China's Artificial Intelligence Surveillance State Goes Global." The Atlantic. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

China achieving total assimilations of millions.[68] For example, a Uyghur citizen was forced to paint her living room red to support Communism after a CCTV camera that runs 24/7 reported her walls were painted light blue, the color that symbolizes Uyghur independence.[69] For President Xi Jingping there is an evident people's war on terrorism that yielded " walls made of copper and steel and nets spread from the Earth to the sky" to capture said terrorists.[70] However, this rhetoric surrounding the Uyghur population as being a violent terrorist support group is based on false narratives that dehumanizes the Uyghur's and strips them of everything they believe in. The debate on whether or not the events in the XUAR should be labeled as genocide or crimes against humanity is still widely discussed by the international community. If the Uyghurs are stripped of everything they believe in and the PRC successfully does so through force and technological mediums, an entire ethnicity will be erased under the guise of ensuring singular ideological thought in China. This chapter will go further to provide an explanation on what the Chinese government is doing to the Uyghur minority population and will illustrate my findings through analyses, reports, and statistics from the last two decades.

The discourse surrounding terrorist organizations and anti-party thought in XUAR have prompted the PRC to create and enforce multi-tiered security measures which have been the base of new technologies and espionage practices. Official Chinese government documents and reports outline the gradual increase of grid-style policing networks such as the Skynet as well as the amount of security related jobs and policing. By analyzing government documents it is evident that the PRC is using technology to target the Uyghur Muslim minority group in ways that expand the government's claim of preserving safety within the country.

---

[68] Salmon, Andrew, and Geoffrey Cain. 2021. "Deep inside China's perfect surveillance state." Asia Times. https://asiatimes.com/2021/06/deep-inside-chinas-perfect-police-state/.
[69] Salmon, Andrew, and Geoffrey Cain. 2021. "Deep inside China's perfect surveillance state." Asia Times. https://asiatimes.com/2021/06/deep-inside-chinas-perfect-police-state/.
[70] Zenz, et al 2017.

Assuring Social Stability Through Increased Surveillance

As of June 2021 there were 12 million Uyghurs recorded in the Xinjiang region and of those 12

million over two million have been detained, forced from their homes, and 'relocated to

re-education centers' by the Chinese Government. Sean Roberts presents an analysis of how the

current treatment of the Uyghurs has been a gradual event where a whole group of people are

labeled as a threat to society.[71] He writes that in November of 2001, a published document by the

PRC titled, " Terrorist Activities Perpetrated by Eastern Turkistan Organizations and their Ties

with Osama Bin Laden and the Taliban" stated there was a vast network of Uyghur terrorists who

enjoyed international support and posed an immediate threat to both China and the world.[72] By

publically labeling an entire group of people to be involved with a terrorist organization directly

following the attacks on 9/11, the government created widespread panic and justification for

further mistreatment. Detention centers were created that ranged from low-level prisons to

"transformation through education" camps that mirror forced-labor facilities that forbid the use

of the Uyghur official language and all religious practices.

 In addition to this initial document the government continued to issue official documents

that eventually gained enough recognition globally to where the United Nations and United

States officially recognized the Uyghur group to be an imminent terrorist threat.[73] Moreover, In

2001 the People's Republic of China published an official document titled "Terrorist Activities

Perpetrated by 'Eastern Turkistan' Organizations and their ties with Osama bin Laden and the

Taliban" affiliating the Xinjiang Region with terrorist groups such as Al-Qaida and the Taliban.

In accordance with paragraph 13 of resolution 1822 (2008) in the document, the Eastern

---

[71] Roberts, Sean R. 2018. "The biopolitics of China's "war on terror" and the exclusion of the Uyghurs." *Taylor & Francis Online* 50, no. 2 (March): 232-258. 10.1080/14672715.2018.1454111.
[72] Roberts, Sean R. 2018. "The biopolitics of China's "war on terror" and the exclusion of the Uyghurs." *Taylor & Francis Online* 50, no. 2 (March): 232-258. 10.1080/14672715.2018.1454111.
[73] *Ibid.,*

Turkistan Islamic Movement (ETIM) is active in South Asia, Central Asia, and the Xinjiang

Uyghur Autonomous Region of China.[74] By linking together a terrorist organization to an entire

region and group of people, the PRC was able to set the tone for future endeavors of

technological espionage and surveillance efforts that directly target Uyghurs.

The use of technology as a means of surveillance within the PRC has adapted to

primarily focusing on the Han majority to minority groups across the nation. The Chinese

government is increasing security and surveillance measures in Xinjiang to achieve social

stability and create a secular citizen who will never threaten regime or state stability. An engineer

for the China Electronics Technology Corporation (C.E.T.C), Wang Pengda, illustrates the region

of Xinjiang being a battlefield of a precise, all-seeing, and infallible platform of military inspired

cyber security systems. The panoptic surveillance system includes sound systems, facial

recognition software, cellular apps, digital forensic tools, and handheld devices called

"counterterrorism swords." The files, pictures, audios, and information received from the

systems, regardless if they are flagged or marked, are then stored in government databases that

contain up to 68 billion records.

A previous Chinese police contractor, Baimurat, reflected on his time working on the

Integrated Joint Operations Platform (IJOP) system in Xinjiang where he was responsible for

monitoring face-scanning machines, surveillance cameras, and other digital enclosures targeting

the Uyghurs. Baimurat stated that as the physical technology supplied government systems with

information, the datasets modernized to a point where they could identify when someone was

wearing an Islamic veil, if they had installed banned apps like WhatsApp, or if they had refueled

---

[74] United Nations. 2018. "EASTERN TURKISTAN ISLAMIC MOVEMENT | United Nations Security Council."
The United Nations Security Council.
https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/eastern-turkistan-islamic-mo
vement.

their car with gas.[75] Furthermore, there is no way around AI- surveillance for the Uyghurs since downloading a private VPN or any other banned cellular software would immediately alert authorities.[76] This pervasive network of technology, implemented to increase espionage efforts against the Uyghurs supports state-led incentives that explicitly target Muslims.

The policing and security recruitment in Xinjiang have increased tenfold in past years, foreshadowing the implementation of more severe and totalitarian inspired security measures throughout the region.[77] In conjunction with the technology that is meant to track physical movements, obtain video and photographic figures, and execute the digital checkpoints throughout Xinjiang, the PRC is supplementarily using technology to collect biometric data in the guise of a free health care program. Human Rights Watch published a report highlighting the Physicals for All initiative Chinese Authorities introduced in 2017. In accordance with the initiative, police and authorities are supplied with varying security devices to ensure efficient collection of information. President Xi Jingping has named the mobile internet technologies and CCTV analytics combined that are currently joined with over 30,000 policemen in XUAR as the fists and daggers of counter-terrorism efforts in China.[78] Through the ability of offical government documentation to report the collection of information as a means of self defense against an entire ethnic minority believed to be connected to terrorist organizations they are able to increase state security surveillance efforts and continue to displace, mistreat, and abuse Uyghurs. The intensification of digital espionage in Xinjiang masked under the guise of a free

[75] Byler, Darren. 2020. "The Xinjiang Data Police - NOEMA." Noema Magazine. https://www.noemamag.com/the-xinjiang-data-police/.
[76] Andersen, Ross. 2020. "China's Artificial Intelligence Surveillance State Goes Global." The Atlantic. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.
[77] Salmon, Andrew, and Geoffrey Cain. 2021. "Deep inside China's perfect surveillance state." Asia Times. https://asiatimes.com/2021/06/deep-inside-chinas-perfect-police-state/.
[78] *Ibid.,*

medical exam is one of the many ways the government is adopting new technology and cyber-security systems to achieve total social stability.

High-tech surveillance systems throughout the PRC have also played a key role in the re-education camps. President Xi Jinping introduced the concept of creating re-education camp systems and new government mandates in May of 2014 following several attacks in the Xinjiang capital of Ürümqi. Chen Quanguo was appointed to be the new head secretary of the Communist Party located in XUAR in 2016, and in 2017 Xinjiang authorities implemented over 7,500 new technological police-monitoring stations. The police stations ensured that the 24-hour surveillance system is only to be used for quick responses in times of emergency despite the XUAR Department of Justice issuing a clear mandate of creating the "transformation re-education centers" in Xinjiang.[79] Under Xi Jinping XUAR has become an incubator for crimes against humanity and the mass incarceration of the Uyghur minority as they are being forced into concentration-like camps in the name of fighting-terrorism.

The prison-like centers in Xinjiang are the result of an abrupt but not shocking claim made by President Jingping stating, "The Chinese people's fear of instability and quest for social harmony is most intensely felt in China's strategic Western borderlands. Here the party-state is penetrating deeper into the lives of its citizens, seeking to forcefully transform their cultures, thoughts, and behavior in hopes of manufacturing what it calls "enduring peace" (长治久安)".[80] The re-education centers made the control and espionage of an entire ethnic and religious group more feasible because it is monitored in its totality by the Skynet tool. Comparing Skynet to the holy grail of surveillance technology, author Andrew Salmon compares Skynet to a human where

---

[79] The University of British Columbia. 2019. "Major Events Preceding the Construction of Re-Education Camps - Xinjiang Documentation Project." Xinjiang Documentation Project. https://xinjiang.sppga.ubc.ca/timelines/reeducation-camps/.

[80] Leibold, James. 2019. "Leibold | China Leadership." China Leadership Monitor. https://www.prcleader.org/leibold?fbclid=IwAR38OsGVP3ZYJwSUXy80gct52ywNid3RZjl0Q3BhOfSDx_OruGW-2K7L3mA.

the program uses eyes, CCTV cameras and AI facial recognition software, it's brain, the deep

neural network that connects images, videos, and data points to other patterns, ears that come

from voice recognition software, and the blood and flesh from the DNA samples and biometric

data. [81] The significance of this comparison is that because Skynet adapts to the data it receives

and learns from it, there is no aspect of life for the Uyghurs that was not under draconian

surveillance measures.

Since the creation of the re-education centers in 2017, security measures within the

camps have grown significantly. In an article written by Darren Byler in December of 2021, the

Uyghurs were first held in detention facilities with lights on them nonstop day and night and

civilians were held to extreme measures such as sitting completely straight without movement or

not being able to cover their faces.[82] If a detainee was caught breaking a rule the motion sensor

cameras were triggered and the guards were immediately notified. President Jinping employed

over 60,000 police workers and military members to be grid workers who scanned the Uyghurs

cellular devices and digital activity to label them as trustworthy or untrustworthy.

Byler advocates for the claim that the creation of the surveillance network in XUAR

precludes domestic human rights violations due to the technologies that are in place do not

explicitly state their evaluative processes. What this means is the Skynet system or any "smart

technology" that is in the XUAR area cannot trace an individual's thought process and is unable

to check someone's moral code. But, the PRC supports anti-Uyhur sentiments and punishments

through "micro-clues," when the system flags a person, from the surveillance infrastructures

which prompts immediate reactions from authorities. The establishment of espionage technology

---

[81] Salmon, Andrew, and Geoffrey Cain. 2021. "Deep inside China's perfect surveillance state." Asia Times. https://asiatimes.com/2021/06/deep-inside-chinas-perfect-police-state/.
[82] Byler, Darren. 2020. "The Xinjiang Data Police - NOEMA." Noema Magazine. https://www.noemamag.com/the-xinjiang-data-police/.

in XUAR resulted in a campaign led by PRC authorities with the clear motive to limit religious observation and expressions.[83]

By restricting the religiosity and way of life of the Uyghurs, the PRC has allowed the Chinese government to foster a more antagonistic approach to monitoring and controlling them. The differences between the technology and methods used to surveille the ethnic Han majority and one of the ethnic minority groups, the Uyghurs, is both flagrant and glaringly obvious when it comes to extremist policies. The preemptive measures that were taken to increase safety within the Xinjiang region were defended by police as being "illegal", such as arresting Uyghurs for illegal religious activities, illegal preaching, naming their children traditional Muslim names, or attending religious services and centers (Mosques).[84] The 24/7 cameras and CCTV networks in the XUAR camps equivantly aided in suppressing the lives of Uyghurs by monitoring weddings, funerals, preventing the participation of the Ramadan fast, and forbidding expressions of their culture through writings or reciting of poems and literary works throughout the region.[85] The technologies that regulate and control the Uyghur's way of life, movements, and thoughts are being used to justify the existence of detainment camps that mirror genocidal acts. Surveillance technology is integral to the PRC's goals in relation to controlling the Uyghur minority and ensuring the future of the state's regime.

In 2014, the Chinese government launched the document and initative "Strike Hard Campaign against Violent Terrorism" (严厉打击暴力恐怖活动专项行动) which Human Rights Watch claims is the reason why Xinjiang turned into one of China's primary locations for using new technologies for social control. The document also highlights the PRC's belief that ethnic

---

[83] Roberts, Sean R. 2018. "The biopolitics of China's "war on terror" and the exclusion of the Uyghurs." *Taylor & Francis Online* 50, no. 2 (March): 232-258. 10.1080/14672715.2018.1454111.
[84] Roberts, Sean R. 2018. "The biopolitics of China's "war on terror" and the exclusion of the Uyghurs." *Taylor & Francis Online* 50, no. 2 (March): 232-258. 10.1080/14672715.2018.1454111.
[85] *Ibid.,*

unrest and civil disobedience in Xinjiang is why the Strike Hard campaign is necessary in continuing surveillance and control of the area. The reason this initiative is significant is because it outlines an in-depth analysis of how government officials in XUAR communicate with and report to Chinese authorities through the Integrated Joint Operations Platform (IJOP-体化联合作战平台).[86] IJOP, a regional data system that combines AI and surveillance technology to monitor the government checkpoints throughout XUAR as well as public institutions such as hospitals, banks, parks, theaters, etc.[87] According to an interview conducted by Darren Byler of the Guardian, a Uyghur man by the name of Alim returned to China following a study abroad trip and was immediately taken into police custody seconds after walking off of the plane. Subsequent to mandatory questioning, Alim was deported to one of the several re-education camps where he states he was devoid of sleep and food as well as subjected to verbal abuse, hours of interrogation, and was tortured with electric shocks.[88] While minority groups are subjected to government mandates void of any pretense of injustices, digital footprints and assumed anti-party political and social offenses is how the government uses technology to maintain absolute power.

In 2017, an official, state-publish document titled *"The [Xinjiang Uyghur Autonomous] Region Working Guidelines on the Accurate Registration and Verification of Population" (*全区人口精准登记核实工作指南*, "The Population Registration Program*" was issued by Xinjiang's Office of Population Service and Real Name Registration Work Leadership Committee (自治区

---

[86] Human Rights Watch. 2019. "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App | HRW." Human Rights Watch News Release.
https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.
[87] Byler, Darren. 2019. "China's hi-tech war on its Muslim minority." The Guardian.
https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition.
[88] Byler, Darren. 2019. "China's hi-tech war on its Muslim minority." The Guardian.
https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition.

人口服务管理和实名制工作领导小组办公室).[89] As per the document, Xinjiang government officials and police will carry out the Population Registration Program in stages under the guise of social stability and a benefit to a region that is economically poor. The initial framework of the program is to verify the true number of the Uyghur population in the region through collection of DNA biometrics and constant photographic and video surveillance for anyone aged 12-65 with no exceptions.[90] The use of mobile apps, designed for *hukou* (household status registration) or other new technologies is the way police and officials are able to carry out government mandates. The technology that is being made readily available to the PRC is how they are able to place millions of Uyghurs into concentration like camps which are being referred to as re-education centers.

The Population Registration Program officially states that the collection of biometric data from the Uyghurs will be comprehensive and will not include consent from participants. A translation of the document done in 2021 states the guidelines of the program say officials must ensure that [information from] every household in every village, every person in every household, every item for every person will be collected.[91] In essence, by culminating this amount of information on each individual in the Xinjiang region, the Chinese government is allowed to use cloud computing, big data, and modern technologies to continue targeting basic human rights of the Uyghurs.

In section four of the program document authorities vernacular states workers use handheld devices and technologies supplied by the government to verify and collect all data received. Through a smartphone app introduced and implemented by the China Electronics

[89] Richardson, Sophie. 2017. "China: Minority Region Collects DNA from Millions." Human Rights Watch. https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.
[90] Richardson, Sophie. 2017. "China: Minority Region Collects DNA from Millions." Human Rights Watch. https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.
[91] *Ibid.,*

Technology Corporation (C.E.T.C), specialized policemen in Xinjiang receive data and reports directly to their phones.[92] The police then target individual Uygurs with support from a grid-style surveillance application that stores any and all data that is deemed as valuable. The smartphone app has the ability to flag certain behaviors that have been deemed valuable by the government: growing a beard too long, leaving out of the backdoor of your home, worshiping at a mosque. The notifications from the app are then compiled into an online database where it is entirely up to the local security forces discretion on if they think the civilian in question should be detained, arrested or brought to a governmental worker with a higher rank.[93]

By flagging behaviors that are individual to Uyghurs like attending their place of worship, it shows the government's push for a totalitarian state and singular thought citizens that mirror the Han majority group. To fully grasp the severity of the events occurring in Xinjiang it is essential to acknowledge that although other minorities in China are facing injustices, the disproportionate discrimination explicitly against the Uyghur Muslims is why this issue is relevant and worthy of further analysis.

Beginning with an immediate result of the assertions about the Uyghur terrorist threat in the early 2000s led to the passing of amendments to China's criminal legal code in December of 2001. In section 7, article 54 of Chapter 2 (第七节　剥夺政治权利) it states, "*Anyone who is sentenced to public surveillance is deprived of political rights as a supplementary punishment, the term of deprivation of political rights shall be the same as the term of public surveillance,*

---

[92] Mozur, Paul, and Chris Buckley. 2019. "How China Uses High-Tech Surveillance to Subdue Minorities (Published 2019)." The New York Times.
https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.
[93] Mozur, Paul, and Chris Buckley. 2019. "How China Uses High-Tech Surveillance to Subdue Minorities (Published 2019)." The New York Times.
https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

and the punishments shall be executed simultaneously."[94] Implied in this statement is that the rights of the Uyghurs are conditional upon if they are being surveilled. Since all Uyghurs are being monitored, authorities in XUAR are supported by Chinese law to precipitate any measures against Uyghurs they deem sufficient. While these amendments in the legal code primarily address terrorist crimes or acts against the state, the crimes outlined under the category of "Endangering Public Security," are absent of new sufficient definition to be fairly punished.[95] The lack of clear reason for punishment throughout the legal code resulted in a legal gray area that is entirely subjective and gives Uyghurs little to no freedoms in their lives.

The Old Versus the New in China's Treatment of Minorities

China, supported by a history of authoritarian policies, prioritizes the preservation of power and the existence of the Han majority leaving no room for the definition of what it truly means to be Chinese up for debate. The People's Republic of China, founded in 1949, officially acknowledging the 56 ethnic groups in the state with 10 recognized as Muslim minorities. Despite the recognition of the 56 groups there continues to be an ostensive Han hegemony based upon century-long ideals of how being a part of the Han majority equates to the national vision of China.[96] It is the ideology of supremacy that isolates minority groups in China and sets the framework for new technologies that could not have been imagined before.

Harvard Law School Professor, Shoshana Zuboff, argues that because of China's history of security-industrial establishment the control and surveillance over the Uyghurs has become a

---

[94] Merkley, Jeff, and James P. McGovern. 2016. "Criminal Law of the People's Republic of China." Congressional-Executive Commission on China. https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china#Chapter%20III.7.

[95] Roberts, Sean R. 2018. "The biopolitics of China's "war on terror" and the exclusion of the Uyghurs." *Taylor & Francis Online* 50, no. 2 (March): 232-258. 10.1080/14672715.2018.1454111.

[96] Campbell, Charlie. 2021. "How Beijing Is Redefining What It Means to Be Chinese, from Xinjiang to Inner Mongolia." TIME. https://time.com/6078961/china-ccp-anniversary-identity/.

test case for big data companies and tech giants to achieve unfathomable records of growth. What this implies is that while Chinese tech companies continue to create further methods of surveillance, potential for market growth also increases. This phenomenon is expressed clearly in the importance placed on the Belt and Road Initiative as well as the Digital Silk Road policy vision. When a state places the concepts of "getting ahead" and economic prosperity over the individual freedoms of its civilians there is no reason to stop if they remain unchallenged. This being said, the Chinese government began to shift away from relying on the physical reports of its citizens and more towards means of high-tech surveillance when tensions between the Uyghurs and Han began to escalate in the early 2000s.

Revealing itself in the forms of ethnic riots in Xinjiang and the Urumqi riots both in 2009, the PRC began moving sizable amounts of Han Chinese into Xinjiang as " big brothers and sisters". These people had the sole responsibility of surveillance and monitoring every motion of the Uyghurs while they ate with them, slept with them, and ensured their assimilation into the desired Chinese culture.[97] The difference between relying on the reports of other citizens in comparison to technological surveillance records is that the ability of real time mobile monitoring that has no limitations, such as rest or bias, could dig even further into the lives of the Uyghurs. The recent advancements of technology in the PRC have taken previous methods of surveillance to an entirely new level as the Chinese government continues to use it against ethnic minorities to exert control.

Stated directly in Article 2 of Order 435 of the Law of the People's Republic of China on Regional Ethnic Autonomy(国务院实施〈中华人民共和国民族区域自治法〉若干规定):

---

[97] Andersen, Ross. 2020. "China's Artificial Intelligence Surveillance State Goes Global." The Atlantic. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

Governments at all levels shall intensify the publicity and education of Law of the People's Republic of China on Regional Ethnic Autonomy and related laws, regulations and policies towards minorities, formulate implementation measure by law to protect the legitimate rights and interests of ethnic minorities and properly dispose issues concerning national unity, uphold and improve the system of regional ethnic autonomy, consolidate and enhance socialist ethnic relations of equality, solidarity and mutual assistance and any act which undermines the unity of the nationalities or instigates division is prohibited.[98]

However, by shifting from a preventative to a preemptive approach to monitoring and controlling the Uyghurs the PRC now relies on technology to fight against the very protections and freedoms they outline and present in their own laws. As technology works alongside with police, there is no interaction between Uyghurs that is not seen as suspicious or worthy of questioning. Specifically, IJOP algorithms notify authorities if an Islamic prayer rug is purchased online or if someone is using more or less electricity than normal.[99]

Working in tandem with old methods of surveillance and control, the PRC found a way to decrease the potential of the Uyghur population increasing. The security and CCTV checkpoints that surround every corner of XUAR also set off alerts in the networks when a pregnant woman passes through them. The automated surveillance system tracks the pregnant woman, and according to a piece written in the Atlantic, Uyghur women are often forced to have abortions, get an IUD inserted, or women with existing children are streilized by the state against their

---

[98] Merkley, Jeff, and James P. McGovern. 2016. "Criminal Law of the People's Republic of China." Congressional-Executive Commission on China. https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of-china#Chapter%20III.7.

[99] Andersen, Ross. 2020. "China's Artificial Intelligence Surveillance State Goes Global." The Atlantic. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

will.[100] This treatment resulted in a 60% decrease of birth rates for Uyghurs in certain regions of China, as stated in the same article. Instead of using outdated methods of espionage like the big brother- sister spying system, the PRC is using modern technologies to fashion more pre-meditated and calculated ways of surveillance.

The ability to mine, store, and then process this level of data with no safeguards in place for civilians was unimaginable even as recently as a decade ago. The PRC's initiatives to implement more surveillance networks and capabilities, primarily towards minorities, is part of a larger human rights issue. Through the use of biometric data in the guise of free health exams, maintaining the preservation of Han-majority by concentration like "re-education centers' ', and other violent measures have shown that the surveillance goals of the PRC goes beyond maintaining domestic security. While it is unknown what extent the PRC will go to relative to developing increasingly invasive methods of surveillance, by observing the timeline of the treatment of minorities in China the policies already in place foreshadow the future of technological surveillance in the state. The final, empirical chapter of this research will summarize the two previous case studies while also illustrating the involvement of the West and if the international community sees the events in China and the XUAR as human rights violations.

---

[100] Andersen, Ross. 2020. "China's Artificial Intelligence Surveillance State Goes Global." The Atlantic. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

Chapter Four

Comparison of Case Studies

The People's Republic of China has pursued a surveillance state that is centered around preventing premeditated domestic terrorism, threats to both social and political stability, and guaranteeing the future of the state. The domestic surveillance networks within China track civilians' every movement, such as monitoring visitors at tourist sites or conducting security checks at airports as well as more significant actions like visiting a place of worship or how many times you leave your home.[101] By emphasizing the importance of a safe society for the citizens of China, the PRC has been able to advance the manufacturing of networks and systems, such as Skynets which are high-tech surveillance grids that monitor 24/7. The growing popularity of using technology as a method of surveillance and control in China has been presented by President Xi Jingping as a way to more effectively prevent crime and increase safety throughout the nation. Yet, the systems in place have been believed to be one of the many ways the government is targeting minorities and suppressing the freedoms of Chinese citizens. Throughout this chapter I will summarize the findings of my two case studies by comparing the ways they are similar, as well as arguing how despite their differences they both are a part of a larger picture of the PRC's overall internal surveillance dreams.

However, the evolution of surveillance technologies in China has evoked global concerns as well as international recognition. While Western entities alike criticize the PRC's surveillance

---

[101] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash." Fortune. https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/.

state, both democratic and authoritarian governments from predominantly the global south have embraced the policing machinery and survyenace methods from China. At the same time, leaders of countries such as the United States have publicly claimed that what the PRC is doing in the XUAR is a genocide and a human rights violation, there has been at least 80 countries who China has sent surveillance technologies to. Granted, several of the surveillance methods used in the PRC are being used in democratic entities across the globe such as France and the United States as well, a New York Times article states.[102] Regardless, the implications of the PRC's goals of expanding its technological surveillance methods insinuates that the PRC does not only want to enforce increased technological espionage methods domestically, but also globally. This section argues that the rise in the PRC exporting its espionage technologies has resulted in a global response and potentially labeling the events in China as crimes against humanity.

Differences and Similarities

Technological surveillance measures in China are not distinctive to one group of people. The People's Republic of China has developed new forms of technology to monitor its civilians in totality but the ways in which they are using the technology is disparate from the Han majority versus ethnic minorities. Regionally, both the Xinjiang Uygur Autonomous Region (XUAR) and the city of Beijing have both become some of the most surveilled cities as eight of the ten most surveilled cities in the world are in China.[103] Fortune Magazine writer Grady McGregor writes that China's efforts to track its citizens on a mass scale through technology-enabled practices

---

[102] Krolik, Aaron, and Paul Mozur. 2019. "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers (Published 2019)." The New York Times. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.
[103] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash." Fortune. https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/.

have blanketed all regions in the country regardless of population.[104] On the one hand, it is

argued that Beijing is the blueprint of modern surveillance technologies because it is a

higher-profile territory being the nation's capital. Still, because the methods of surveillance and

security in the XUAR is continuing to become increasingly violent and has precipitated a global

response, it is clear the goal of surveillance in the two areas is vastly different.

  The parallels between the XUAR and Beijing is seen in the methods of tracking every

day life and data mining such as facial recognition- CCTV at every street corner, security

checkpoints, and increased policing to maintain party obedience and loyalty. In Beijing, a

city-wide Skynet that tracks the movement of almost 1.4 billion people now has the ability to

monitor and report on how many times a day a citizen leaves their home.[105] President Xi Jingping

has identified the three main reasons of increasing surveillance methods throughout the nation as

fighting seperatism, extremism and terrorism.[106] In the past decade Beijing has seen growing

levels of social unrest and means of protest in response to the citizens becoming more

dissatisfied with the Chinese government. National Public Radio (NPR) reporter Emily Feng

attributes the demolition of wealthy suburbs in Beijing to a growing popularity of anti-party

thought.[107] Feng clearly states that citizens in the area had begun to hang copies of the Chinese

Constitution on their doors to prevent complete destruction of their homes to show that what Xi

Jinping is enforcing coincides with his socalist thoughts on a rule-of-law society. Any seperatist

thought in Beijing is reported to regional authorities, flagged, and dealt with immediately. This is

---

[104] McGregor, Grady. 2020. "China's surveillance system—the world's largest—is growing. So is the backlash." Fortune. https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/.

[105] Mozur, Paul. 2018. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras (Published 2018)." The New York Times. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[106] Salmon, Andrew. 2021. "Deep inside China's perfect surveillance state." Asia Times. https://asiatimes.com/2021/06/deep-inside-chinas-perfect-police-state/.

[107] Feng, Emily. 2021. "Residents Protest As China Demolishes Some Of Beijing's Wealthy Suburbs." NPR. https://www.npr.org/2021/01/26/960855956/residents-protest-as-china-demolishes-some-of-beijings-wealthy-suburbs.

similar to what is occurring in Xinjiang because President Xi and the PRC sees all minorities and religious groups outside of the Han as enemies of the state which is why the XUAR is being as closely monitored and controlled as it is.

The surveillance methods in Beijing are additionally present in the XUAR region, but in Xinjiang it has taken a far more invasive and hostile approach. Since the creation of the People's Republic of China in 1949, minorities have been separated from the Han ethnic majority and have been divided into 10 separate factions dispersed across the country.[108] The separation between the ethnic minority and majority is one of the primary reasons why the Chinese state has continued to restrict, monitor, and control certain groups more than others. Authors Adrian Zenz and James Leibold argue the continued surveillance efforts of the PRC on both the Han and the Uyghurs is not solely a matter that impacts one group more than the other. They write, "since the July 5, 2009 riots in the regional capital of Urumqi, thousands have died in violent clashes between the Muslim Uyghur minority and the Han-dominated Party-state."[109] This claim supports the idea that while surveillance technology is meant to enforce one group's beliefs over another, the increased policing state and monitoring of Chinese citizens is not central to only one group. Through commonalities such as mass surveillance apparatus' or facial recognition softwares, the ways in which technology is used in cities such as Beijing and the XUAR reveal the PRC's overall domestic agenda of technological surveillance.

The Western and Global Response

---

[108] Hammond, Kelly A. 2019. "The history of China's Muslims and what's behind their persecution." The Conversation. https://theconversation.com/the-history-of-chinas-muslims-and-whats-behind-their-persecution-117365.
[109] Zenz, Adrian, and James Leibold. 2017. "Xinjiang's Rapidly Evolving Security State." *China Brief* 17, no. 4 (March). https://jamestown.org/program/xinjiangs-rapidly-evolving-security-state/.

For the past decade the PRC's surveillance state has yielded a global response, primarily from Western countries and international organizations alike. In 2017, the Chinese State Council publicly stated that by 2030 they plan to become the world leader of artificial intelligence with technology at the center of all domestic efforts.[110] The long-term goals from President Xi Jingping for China's surveillance state have raised criticisms and warnings from global actors because the technology has surpassed only domestic goals. Journalist Ross Andersen for *The Atlantic* argues that it is not only repression within China that is alarming but also its exporting of surveillance technology. In doing so, Andersen states that if unchecked, these technologies could prevent billions of people across the world from ever securing any measure of political or social freedoms.[111] When discussing the possibility of an international response towards the PRC regarding the Uyghurs, American reporters and journalist Anna Mitchell and Larry Diamond of *The Atlantic* place the utmost importance of the West not perceiving China's desire for long-term internal stability with a grain of salt. They claim the PRC uses the network of technological surveillance and information to safeguard its regime which supports the theory that it is not just the repression taking place within China that must be acknowledged, it is also the global reach of it.[112]

Monica Wang, a senior analyst at the IHS Markit in Shanghai, states that the United States, with around 62 million surveillance cameras in 2016, had a higher per capita penetration rate than China, with around 172 million[113]. Yet, what sets Democratic entities apart from China is its reasoning for why they are monitoring citizens to an unavoidable degree. Additionally,

[110] Kharpal, Arjun. 2019. "US takes aim at Chinese surveillance as the trade war becomes a tech war." CNBC. https://www.cnbc.com/2019/05/27/china-mass-surveillance-state-technology-at-center.html.
[111] Diamond, Larry, and Anna Mitchell. 2018. "China's Surveillance State Should Scare Everyone." The Atlantic. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.
[112] Diamond, Larry, and Anna Mitchell. 2018. "China's Surveillance State Should Scare Everyone." The Atlantic. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.
[113] Denyer, 2018.

because there are clear safeguards put in place that outline a clear frame of rights, human rights activists, protestors, and citizens who want to exercise their freedom of expression will not be severely punished or oftentimes killed. By framing the current events in China as human rights violations, like the invasive methods of collecting biometric data from Uyghurs or preventing Uyghur women from bearing children, the response of international entities should be proportional to the acts of the PRC. Sophie Richardson, the China Director at Human Rights Watch, supports this claim in her online article as she writes, " The mandatory databanking of a whole population's biodata, is a gross violation of international human rights norms, and it's even more disturbing if it is done surreptitiously, under the guise of a free health care program."[114] The international response towards the PRC is not limited solely to the policies enforced by the government, but also the tech companies and startups that are making the espionage and monitoring feasible to begin with. Frances Eve, a researcher for the Hong Kong Human Rights Defense group, argues China's tech companies are objectively complicit in human rights violations and also that it is a crime in itself to fight against these companies. Eve follows that claim by noting, "The government treats human rights activists, lawyers and ethnic Uyghurs and Tibetans as criminals, and these people are being caught, jailed and possibly tortured as a result of this technology."[115] As more information becomes available to the public about the Uyghurs and the goals the PRC has for minorities, it is crucial to acknowledge the impacts it has on global order such as human rights, global finance, and the environment, Richardson additionally notes.

---

[114] Richardson, 2017.
[115] Denyer, Simon. 2018. "China bets on facial recognition in a big drive for total surveillance." The Washington Post. https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.

According to the Uyghur Human Rights Project Foundation (UHRP), as of 2021 there have been global responses from over 17 countries and several national-multilateral organizations that have publicly released their views on the Uyghur crisis. On October 21, 2021 at the United Nations Third Committee meeting, 43 countries released a joint statement expressing their concerns and declaring the condemned atrocities relating to human rights violations occurring in China.[116] The first official record of coordinated human-rights sanctions against China was in March of 2021 where BBC news writes the European Union, U.K., the U.S., and Canada placed visa bans and financial asset freezes on four PRC officials and the Xinjiang Police department. Prior to these economic and governmental responses, countries like Germany took a more social approach. Written in the same UHRP article, in August of 2018, Germany announced that it would halt all deportations but only of Uyghurs back to China. In 2021 the Lithuanian parliament called on the U.N. to immediately begin a legal inquiry into the Uyghur genocide in China and voted to "strongly condemn China's massive, systematic and grave human rights violations and crimes against humanity."[117] The bilateral relationship and support from both nations and independent groups imposing sanctions, releasing determinations of future policy changes towards the PRC, or issuing Atrocity Crimes Statements and support towards the Uyghurs shows that what is happening towards the Uyghurs does much deeper than what the PRC is claiming.

The Digital Silk Road and the Investment to the Global South

---

[116] UHRP. 2021. "International Responses to the Uyghur Crisis." Uyghur Human Rights Project. https://uhrp.org/responses/.
[117] UHRP. 2021. "International Responses to the Uyghur Crisis." Uyghur Human Rights Project. https://uhrp.org/responses/.

Introduced and implemented in 2013 by President Xi Jinping, the Belt and Road Initiative (BRI) has taken monumental leaps in becoming one of China's primary foreign policy objectives. In efforts to bridge the gaps in China's trade route, the Belt and Road Initiative has become the largest infrastructure commitment to date and become increasingly diverse in its assistance to the PRC.[118] Two years after the Belt and Road Initiative began in 2013, the Digital Silk Road (DSR) was launched with much fanfare. The primary goal of the initiative was to create an expansive global data foundation of wireless networks, surveillance cameras, subsea cables, and satellites.[119] The secondary goal of the DSR was to bring attention to China's involvement in providing aid for countries or trading partners of the initiative. By China investing into members of the initiative, there was a guarantee of return or a greater potential for the state to make money. Exhausting the bounds of security, the Digital Silk Road became a multifaceted expansion plan for China to further immerse themselves in the global economy and increase digital infrastructure externally.

Despite the initial proclamations of the BRI being to expand China's economic reach to global levels, it has now also became another way for the CCP to enforce technology enabled authoritarianism into other countries as well. [120] I argue that the DSR is not a means of increasing economic prosperity but is an additional medium for the CCP to justify the use of new forms of technology for internal surveillance and control. According to an analysis done by Open Source Intelligence expert group, Insikt, if China continues to develop the DSR initiative the focus of the CCP will be to eliminate all pro-democracy movements throughout the state and affiliates of

---

[118] Kurlantzick, Joshua, and James West. 2021. "China's Digital Silk Road Initiative | The Tech Arm of the Belt and Road Initiative." Council on Foreign Relations. https://www.cfr.org/china-digital-silk-road/.
[119] Reconnecting Asia. 2021. "Mapping China's Digital Silk Road - Reconnecting Asia." Reconnecting Asia. https://reconasia.csis.org/mapping-chinas-digital-silk-road/.
[120] Kurlantzick, Joshua, and James West. 2021. "China's Digital Silk Road Initiative | The Tech Arm of the Belt and Road Initiative." Council on Foreign Relations.

the initiative. The potential to have a global presence, most prominently in countries within the

Global South, provides China the ability to continue exporting AI- enabled technologies,

invasive surveillance networks, and the beliefs that come with them to both non-democratic and

democratic countries alike.[121] Consequently, I argue that while one of the pillars of the DSR is to

provide financing and assistance for development, such assistance comes at a price. By allowing

Beijing to use data they receive from Chinese firms located in partnering countries, there is a

greater risk of those recipient countries to adopt and implement the content filtering, surveillance

networks, and espionage controls in their states.[122]

It is important to note that there is a link between the PRC international objectives with

the DSR and their domestic surveillance programs. The Digital Silk Road maintains the CCP

thought of domestic control by using Beijing as the standard of state-ran security. As Richard

Ghiasy and Rajeshwari Krishnamurthy argue, the CCP's vision for the DSR can be seen from

both macro and micro levels because it is not limited to domestic endeavors.[123] They highlight its

goals such as " Made in China 2025" and " China Standards of 2035" as example initiatives to

enhance domestic technology innovations, decrease government vulnerabilities, and strengthen

the foundation of global digital order.[124] By stating that the Chinese government's view on digital

control and governance has a " state-paternalistic nature" the DSR will aid in closely monitoring

and controlling its population through enlarging the overall network. For example, a new DSR

[121] INSIKT GROUP. 2021. "China's Digital Colonialism: Espionage and Repression Along Digital Silk Road." Recorded Future. https://www.recordedfuture.com/china-digital-colonialism-espionage-silk-road/.
[122] Kurlantzick, Joshua, and James West. 2021. "China's Digital Silk Road Initiative | The Tech Arm of the Belt and Road Initiative." Council on Foreign Relations.
[123] Ghiasy, Richard, Rajeshwari Krishnamurthy, and Sebastian Strangio. 2021. "China's Digital Silk Road and the Global Digital Order." The Diplomat. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.
[124] Ghiasy, Richard, Rajeshwari Krishnamurthy, and Sebastian Strangio. 2021. "China's Digital Silk Road and the Global Digital Order." The Diplomat. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

project initiated in June of 2020 by the name *BeiDou,* is a global satellite system that connects

subsea data cables, 5G networks, and CCTV to state-ran digital infrastructures.

The establishment of the DSR highlights the evident steps in which the CCP will take for

developing new technologies that can then be used to surveil their citizens and enforce a digital

authoritarian regime. The academic journal " *The Beijing Effect: China's Digital Silk Road' as*

Transnational Data Governance" written by Matthew Erie and Thomas Stretinz argue, the DSR

furthers internal surveillance methods because of the CCP's pursuit of domestic control through

data espionage. They explain that the explanation for this phenomenon is called digital

authoritarianism. This term is supported by the fact that when China exports new technology

globally, it also exports its values and governance systems. In arguing this belief, the authors

claim, " data sovereignty in China is illusory as the Chinese party-state retains varying degrees of

control over all Chinese enterprises".[125] The article continues to argue that the CCP's technology

control model is enforced by the ambitions of the state to create new technologies that spread

digital authoritarianism and surveillance networks they enforce within their country. As the

Chinese government continues to export digital surveillance technologies to foreign countries,

the DSR will remain a testing ground for new technologies that will also be used domestically.

As of October 2021, Chinese surveillance technologies and policing blueprints have

taken effect in over 80 countries with the exclusion of Australia and Antarctica.[126] By expanding

its surveillance state and regime policies externally to outside global states the Chinese

government increases its capacity to maintain their desired social and political agenda while also

expanding the amount of data they have access to. While a recorded 16 countries have signed

---

[125] Erie, Matthew S., and Thomas Streinz. 2021. "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance." *Journal of International Law and Politics* 54, no. 1 (February): 92. SSRN.
[126] Reconnecting Asia. 2021. "Mapping China's Digital Silk Road - Reconnecting Asia." Center for Strategic & International Studies. https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

official agreements with China to receive DSR-related benefits, the Council on Foreign Relations

argues that one- third of the 138 countries involved in the DSR are receiving unreported

investments from China.[127] Internally, China is using their technological capabilities to maintain

a dystopian surveillance state that mirrors the beliefs of the ethnic Han majority. Externally,

China is preserving their global presence while also exporting their technologies to countries that

are falling behind in either digitization or are lacking a solid government infrastructure. For

example, countries in Africa or Latin America that are less-developed than China need

inexpensive and readily-available technology to expand their capacity to trade with other global

actors, access to the internet for things such as education, and funding in hopes to create a digital

backbone within their country. The DSR also enacts a safeguard for China in that it reduces the

state's vulnerable dependence on outside tech giants such as the United States or Japan.[128] The

promise of increased technology and greater financial opportunities leads to China's desire for

complete digital dominance and the authoritative and oppressive practices easily maintained

outside of China.

China currently provides more financing and technological investments to Africa than

any other leading democracy or multilateral organizations do combined.[129] The potential to

receive investments from China is appealing because not only are they promised high-quality

technology, there are also a plethora of other aspects that supply countries with physical benefits

from China. Matthew Erie and Thomas Streinz argue that outside of technology, jumpstarting

traditional infrastructure projects like highways, railroads, power plants, and smart cities are

[127] Reconnecting Asia. 2021. "Mapping China's Digital Silk Road - Reconnecting Asia." Center for Strategic & International Studies. https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

[128] Ghiasy, Richard, Rajeshwari Krishnamurthy, and Sebastian Strangio. 2021. "China's Digital Silk Road and the Global Digital Order." The Diplomat. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

[129] Reconnecting Asia. 2021. "Mapping China's Digital Silk Road - Reconnecting Asia." Center for Strategic & International Studies. https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

promised.[130] This phenomenon is known as digital authoritarianism and it is how China is able to maintain power control outside of its borders and provide the illusion of power sharing to countries that need it. This threatens the sovereignty of developing countries because China sets the standards of which it operates, making receiving countries unable to sustain technological development without them. Similarly, China will use the AI-technologies and surveillance practices within the countries they are located in to magnify Chinese supply chains, its economy, and its data localization abilities.[131]

China's security and surveillance methods have been adopted by countries because of factors such as the appeal to the receiving country and China's goals of geopolitical power and the expansion of its market. In a 2020 report conducted by Brookings Institute, author Sheena Greitend states that both push and pull factors add to the growing use the PRC's surveillance technology: countries that are strategically important to the PRC are comparatively more likely to adopt it, but so are countries that need immediate solutions to issues like high crime rates or violence.[132] The implications of this is that while there might be little correlation if a more economically developed country that is more developed would invest in the technologies, it still supports the idea that the PRC is going global with its surveillance systems and security policies.

President Xi Jingping has made ensuring domestic security the forefront of his presidency and the strategies that it includes are directly targeting minority groups throughout the nation. By comparing this research's two case studies of the Beijing and the Uyghur minority groups it provides a comprehensive outlook on the bigger picture of what is happening in China. The use

---

[130] Erie, Matthew S., and Thomas Streinz. 2021. "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance." *Journal of International Law and Politics* 54, no. 1 (February): 92. SSRN.
[131] Ghiasy, Richard, Rajeshwari Krishnamurthy, and Sebastian Strangio. 2021. "China's Digital Silk Road and the Global Digital Order." The Diplomat.
https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.
[132] Greitens, Sheena C. 2020. "Dealing with demand for China's global surveillance exports." Brookings.
https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/.

of technology to go beyond the prevention of domestic terrorism is paramount to acknowledging the directives that are in place in China such as the forced relocation of hundreds and thousands of Uyghurs into concentration like camps, the forced sterlization of Uyghur women, and the grid-style surveillence efforts that include tracking every aspect of the life of the Uyghurs. While both Beijing and the XUAR are being closely monitored, the differences of surveillance methods are exceedling different in terms of violence, magnitude of human rights violations, and the reasons behind why the PRC is enforcing the surveillance to begin with.

Conclusions

The government of the People's Republic of China has used technology as a medium to not only surveil their citizens but to control their beliefs and ensure regime stability. In answering my research question of *How China is using technology to surveil and monitor their citizens,* the motives of the PRC become evident through its current policies, government mandates, and future goals of developing these technologies. The state-of-the-art technologies that make up the vast surveillance systems throughout China support President Xi Jinping's efforts of an "all-seeing" network that has gone beyond the nation's borders. China has a long history of surveillance but the modern technologies that span to every corner of the country is what makes the topic of digital espionage more than purely a domestic concern.

The results of this research proves my hypothesis that not only is the PRC using technology to uphold its desired society of a totalitarian state, but it is going even further and weaponizing technology against minorities. Rooting the technologies at a local level and granting regional authorities and police full responsibility of upholding PRC rules has allowed the state to target vulnerable groups through CCTV networks, constant video and photograph surveillance, and access to cellular apps that obtain biometric data as well. Not only do these

systems obtain the data, they also connect it and send it to online databases that have become the driving factor for the RPC attaining qualitative and quantitative data from its population. Official government documents and reports support the notion that China's police and authorities are not hiding what they are doing, yet state-ran companies have bought trackers and softwares to use on their own completely unregulated by the government. The implications of this is that Chinese citizens have become increasingly unaware of the true extent they are being monitored which has resulted in public protests and other acts of defiance. Beginning withthe 1989 Tiananmen Square revolts, the amount of surveillance in China has increased and the desire to prevent any future acts of terrorism is the justification of more violent and invasive methods of espionage and control.

The conclusions of this research's findings has led me to believe that future studies and research should focus on whether or not concrete intervention methods should be used. Whether or not those come from Western entities such as the United States or Europe, the PRC has begun to export its technologies to outside countries. This is significant because as the physical technologies are supplied by the PRC, it is unavoidable that the values and beliefs of the PRC and surveillance networks will follow as well. I propose that there must be comprehensive strategies moving forward such as China providing a clear outline of what their goals are for surveillance data and what they are doing domestically. One might argue that the PRC has already done this, but the standards and safeguards put in place for Chinese citizens, including minority groups, are close to zero. This being said, as China continues to develop invasive methods of surveillance technologies, the international community must act accordingly to ensure the rights of all Chinese citizens are maintained.

Bibliography (Chicago Author-Date 17th ed.)

Ablet, Adile, Alim Seytoff, and Joshua Lipes. 2017. "China Collecting DNA From All Uyghurs
  in Xinjiang Under Guise of Free Physicals." Radio Free Asia.
  https://www.rfa.org/english/news/uyghur/dna-12132017172938.html.

Andersen, Ross. 2020. "China's Artificial Intelligence Surveillance State Goes Global." The
  Atlantic.
  https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

Buckley, Chris. 2019. "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass
  Detentions of Muslims (Published 2019)." The New York Times.
  https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.ht
  ml.

Byler, Darren. 2019. "China's hi-tech war on its Muslim minority." The Guardian.
  https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-x
  injiang-uighurs-surveillance-face-recognition.

Byler, Darren. 2020. "The Xinjiang Data Police - NOEMA." Noema Magazine.
  https://www.noemamag.com/the-xinjiang-data-police/.

Campbell, Charlie. 2021. "How Beijing Is Redefining What It Means to Be Chinese, from
  Xinjiang to Inner Mongolia." TIME.
  https://time.com/6078961/china-ccp-anniversary-identity/.

Campbell, Charlie. 2019. "The Entire System Is Designed to Suppress Us': What the Chinese
        Surveillance State Means for the Rest of the World." TIME.
        https://time.com/5735411/china-surveillance-privacy-issues/.

Collier, Kevin. 2019. "China hacked iPhones and Android devices to target Uyghur Muslims."
        CNN. https://www.cnn.com/2019/09/04/politics/china-uyghur-hack/index.html.

Crossman, Rozena, and Frédéric Schaeffer. 2021. "In China, How People Are Pushing Back On
        the Surveillance State." Worldcrunch.
        https://worldcrunch.com/tech-science/in-china-how-people-are-pushing-back-on-surveill
        ance-state.

Diamond, Larry, and Anna Mitchell. 2018. "China's Surveillance State Should Scare Everyone."
        The Atlantic.
        https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.

Erie, Matthew S., and Thomas Streinz. 2021. "The Beijing Effect: China's 'Digital Silk Road' as
        Transnational Data Governance." *Journal of International Law and Politics* 54, no. 1
        (February): 92. SSRN.

Feng, Emily. 2021. "Residents Protest As China Demolishes Some Of Beijing's Wealthy
        Suburbs." NPR.
        https://www.npr.org/2021/01/26/960855956/residents-protest-as-china-demolishes-some-
        of-beijings-wealthy-suburbs.

Hammond, Kelly A. 2019. "The history of China's Muslims and what's behind their
        persecution." The Conversation.
        https://theconversation.com/the-history-of-chinas-muslims-and-whats-behind-their-persec
        ution-117365.

Human Rights Watch. 2019. "China's Algorithms of Repression: Reverse Engineering a Xinjiang
        Police Mass Surveillance App | HRW." Human Rights Watch News Release.
        https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering
        -xinjiang-police-mass.

Jones, Jeff. 2020. "Jeff Jones." Belfer Center. https://www.belfercenter.org/person/jeff-jones.

Leibold, James. 2019. "Leibold | China Leadership." China Leadership Monitor.
        https://www.prcleader.org/leibold?fbclid=IwAR38OsGVP3ZYJwSUXy80gct52ywNid3R
        Zjl0Q3BhOfSDx_OruGW-2K7L3mA.

Merkley, Jeff, and James P. McGovern. 2016. "Criminal Law of the People's Republic of China."

    Congressional-Executive Commission on China.

    https://www.cecc.gov/resources/legal-provisions/criminal-law-of-the-peoples-republic-of

    -china#Chapter%20III.7.

Mitter, Rana. 2019. "How the one-party state may shape our future." The World Economic

    Forum.

    https://www.weforum.org/agenda/2019/08/how-the-one-party-state-may-shape-our-future

    /.

Mozur, Paul, and Chris Buckley. 2019. "How China Uses High-Tech Surveillance to Subdue

Minorities (Published 2019)." The New York Times.

https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

Richardson, Sophie. 2017. "China: Minority Region Collects DNA from Millions." Human

    Rights Watch.

    https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.

Roberts, Sean R. 2018. "The biopolitics of China's "war on terror" and the exclusion of the

    Uyghurs." *Taylor & Francis Online* 50, no. 2 (March): 232-258.

    10.1080/14672715.2018.1454111.

Salmon, Andrew, and Geoffrey Cain. 2021. "Deep inside China's perfect surveillance state."

    Asia Times. https://asiatimes.com/2021/06/deep-inside-chinas-perfect-police-state/.

United Nations. 2018. "EASTERN TURKISTAN ISLAMIC MOVEMENT | United Nations

    Security Council." The United Nations Security Council.

    https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/ea

    stern-turkistan-islamic-movement.

The University of British Columbia. 2019. "Major Events Preceding the Construction of

    Re-Education Camps - Xinjiang Documentation Project." Xinjiang Documentation

    Project. https://xinjiang.sppga.ubc.ca/timelines/reeducation-camps/.

Ghiasy, Richard, Rajeshwari Krishnamurthy, and Sebastian Strangio. 2021. "China's Digital Silk

    Road and the Global Digital Order." The Diplomat.

    https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

Greitens, Sheena C. 2020. "Dealing with demand for China's global surveillance exports."

    Brookings.

https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/.

Ivanescu, Isabel, Robert Carlson, and Sebastian Strangio. 2021. "China's Paper Tiger Surveillance State – The Diplomat." The Diplomat. https://thediplomat.com/2021/04/chinas-paper-tiger-surveillance-state/.

Kharpal, Arjun. 2019. "US takes aim at Chinese surveillance as the trade war becomes a tech war." CNBC. https://www.cnbc.com/2019/05/27/china-mass-surveillance-state-technology-at-center.html.

Krolik, Aaron, and Paul Mozur. 2019. "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers (Published 2019)." The New York Times. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.

McGregor, Grady. 2020. "China surveillance system—the world's largest—is growing. So is the backlash." Fortune. https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/.

Mozur, Paul. 2018. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras (Published 2018)." The New York Times. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

Reconnecting Asia. 2021. "Mapping China's Digital Silk Road - Reconnecting Asia." Center for Strategic & International Studies. https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

Salmon, Andrew. 2021. "Deep inside China's perfect surveillance state." Asia Times. https://asiatimes.com/2021/06/deep-inside-chinas-perfect-police-state/.

Zenz, Adrian, and James Leibold. 2017. "Xinjiang's Rapidly Evolving Security State." *China Brief* 17, no. 4 (March). https://jamestown.org/program/xinjiangs-rapidly-evolving-security-state/.

Gershgorn, Dave. 2021. "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space." Center for Security and Emerging Technology. https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/.

Gershgorn, Dave, and Dahlia Peterson. 2021. "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space." Center for Security and Emerging Technology. https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/.

Ghiasy, Richard, Rajeshwari Krishnamurthy, and Shannon Tiezzi. 2021. "China's Digital Silk Road and the Global Digital Order." The Diplomat. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

Human Rights Watch. 2021. "Hong Kong: Beijing Dismantles a Free Society." Human Rights Watch. https://www.hrw.org/news/2021/06/25/hong-kong-beijing-dismantles-free-society#.

INSIKT GROUP. 2021. "China's Digital Colonialism: Espionage and Repression Along Digital Silk Road." Recorded Future. https://www.recordedfuture.com/china-digital-colonialism-espionage-silk-road/.

Krolik, Aaron, and Paul Mozur. 2019. "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers (Published 2019)." The New York Times. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.

Kurlantzick, Joshua, and James West. 2021. "China's Digital Silk Road Initiative | The Tech Arm of the Belt and Road Initiative." Council on Foreign Relations. https://www.cfr.org/china-digital-silk-road/.

Larson, Christina. 2018. "China's AI Imperative." *Science Mag* (Beijing), February 9, 2018, 628-630.

Li, Jane. 2019. "Chinese people are pushing back on Beijing's digital surveillance." Quartz. https://qz.com/1659328/chinese-people-are-pushing-back-on-beijings-digital-surveillance/.

Lindsay, Jon R., Tai M. Cheung, and Derek S. Reveron, eds. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. N.p.: Oxford University Press.

Maranto, Lauren. 2020. "Who Benefits from China's Cybersecurity Laws? | Center for Strategic and International Studies." Center for Strategic and International Studies |. https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

McGregor, Grady. 2020. "China surveillance system—the world's largest—is growing. So is the backlash." Fortune. https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/.

Mozur, Paul. 2018. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras (Published 2018)." The New York Times. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

Nan, Hai. 2015. "Beijing '100 Percent Covered' by Web of Surveillance Cameras." Radio Free Asia. https://www.rfa.org/english/news/china/cameras-10052015120935.html.

Qiqing, Lin, and Paul Mozur. 2019. "Hong Kong Takes Symbolic Stand Against China's High-Tech Controls (Published 2019)." The New York Times. https://www.nytimes.com/2019/10/03/technology/hong-kong-china-tech-surveillance.html.

Reconnecting Asia. 2021. "Mapping China's Digital Silk Road - Reconnecting Asia." Reconnecting Asia. https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

Shao, Li. 2018. "The Dilemma of Criticism: Disentangling the Determinants of Media Censorship in China." *Journal of East Asian Studies* 1 (18): 279-297. 10.1017/jea.2018.19.

UHRP. 2021. "International Responses to the Uyghur Crisis." Uyghur Human Rights Project. https://uhrp.org/responses/.