Utilizing Actor Network Theory to Analyze the Deployment of Mass Surveillance Technology in Xinjiang, China

STS Research Paper

Presented to the Faculty of the

School of Engineering and Applied Science

University of Virginia

By

Tahmid Kazi

April 28, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____

Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

Among the countries that permeate the collective psyche and lives of the international community today, few are as prominent and pervasive as China. Once labeled as an impoverished country, their meteoric rise as an economic and technological superpower in the last 3 decades is nothing short of miraculous. With a GDP of $14.34 trillion USD (2019) and containing one of the largest populations on Earth, despite its Communist roots and current beliefs (which historically has not been a demonstrably successful arrangement), China continues to prove its competency as a economic world power, by balancing its political agenda while also successfully leveraging and reaping all the benefits of international trade and capitalist markets. One of the key reasons behind this meteoric rise is China's proficiency in manufacturing and exporting electronics and other high-technology products to cater to our increasingly technologically-dependent global economies. As their socio-economic influence grew, in line with their Communist policies, the Chinese Communist Party (CCP) derived a newer, data-driven approach to wide-scale population monitoring and control through the use of mass surveillance technologies and a system called the social credit system. Through the advent of ubiquitous computing, low -cost scalable surveillance technology such as drones, CCTV cameras, facial recognition algorithms and exabyte-scale data collection (dubbed “Big Data”), China has been successfully undertaking one of the most comprehensive citizen-monitoring programs ever conceived. The benefits reaped from these systems enable an unparalleled level of social cohesion and order to the CCP. However, it does warrant cause for concern when such powerful technologies are leveraged for the suppression of minority groups such as the Uyghurs in Xinjiang Province, China.

The goal of this paper is to view this feat of technology and policy through the lens of Actor Network Theory to identify and analyze all the actors involved in the Network, with a special emphasis placed on network building and network translation, to identify the commercial enterprises and government entities that worked hand in hand to bring this system into a reality, and their contributions to the current state of surveillance in Xinjiang, China. The intent behind this analysis is to shed some light on how our modern information technology products and infrastructure are being used successfully by an economic superpower in the service of suppressing a populace, and committing humans rights abuses on the scale of millions, and how the ubiquity of such powerful technology has enabled such atrocities to be carried out at such an efficient and rapid manner. Within the context of this network, I will show how the collaboration between the various vendors to the profitable surveillance industry in China, the electronics manufacturing industry in Shenzhen, China, the policies enacted by the CCP (such as the social credit system and Internet of Things) that enabled for the deployment of hundreds of millions of CCTV cameras, and the algorithms and data architecture that has been put in place to monitor and collect real-time data on more than 1.2 billion people, all created a socio-technical network that has been successfully leveraged for the suppression of the Uyghur Muslim minority population in Xinjiang, China.

Literature Review

Digital Social Management in China (VELGHE et al.)

To better understand the factors that led to the success of China in using its technological prowess to better manage the Chinese populace, I will be examining socio-technical systems and policies in place, that have pushed the lever in the direction of mass surveillance. Understanding

China's ascent into a technological superpower, would not be possible without taking into account China's expertise in the field of electronics and high tech manufacturing. In the early 2000s, as a result of the push for industrialization, and the growing market for smartphones, China slowly emerged as the leader in low cost high-tech manufacturing, to cater to the world's need for electronic devices (Review et al.). A large young population, coupled with high literacy rate and low wages, coupled with certain key policy decisions by the CCP to allow for the establishment of privately-owned businesses, and the establishment of specialized economic zones (such as Shenzhen, China, which is dubbed as the "Silicon Valley of Hardware" (Mina and Chipchase et al.)) ensured that the technological competence of China continued growing. As a result of economies of scale and Moore's Law, low cost computing became more widely available, enabling the creation of a whole host of technology companies that produced a wide range of electronic goods such as cameras, networking gear, cell phones (and more recently smartphones) (VELGHE et al.). Coupled with the advent of the internet, this gave birth to the Internet of Things industry, which meant that China had all the ingredients in place to ensure that the bulk of their activities moved into the digital domain, aided by the advent of these cyber-physical systems (VELGHE et al.). As shown in numerous polls, China has one of the highest number of internet monthly active users (Thomala et al.), and its homegrown software services such as WeChat provide comprehensive services, from making online payments to making an appointment at a doctor (Zheng et al.), and services such as Alipay, which is the largest financial technology company (due to its ubiquity in the field of digital payments) (Ryan, Pascoe, Hoffman, Garnaut, Izenman, Johnson & Thomas et al.) ensures that a non-insignificant amount of a person's data stays in the digital domain. And due to the strict censorship laws and open-door policies with technology companies (Lin and Chin et al.), all of this data historically

has been available and actively used by the government to survey its citizens (VELGHE et al.). Also, the (recent) pervasiveness of facial recognition software and the widespread use of security cameras in all public spaces, currently enables the government to create a comprehensive digital dossier on every Chinese citizen within (and sometimes outside) its borders (Andersen et al.). The way in which this system of surveillance technology is used particularly against the Uyghurs in Xinjiang China, will be investigated in detail in the sections to come.

The Social Credit System (LOUBERE & BREHM et al.)

In early 2014, the Chinese government outlined a controversial policy of scoring its citizens using a digital system called the social credit system, with the aim of having it fully deployed by 2020. At a high level, the objective of this system is to leverage the Internet of Things to actively track and reward those who are deemed as trustworthy and loyal to the Chinese Communist Party (CCP) or are in line with their policies, ideals and beliefs. The level of integration into the daily lives of Chinese citizens is what makes this system so pervasive and controversial. Because of China's wide-scale embracing of surveillance technology, hundreds of millions of surveillance cameras, drones, persistent tracking across all the citizen's digital devices (all of which are part of the cyber-physical domain called the Internet of Things) through open-door data policies with technology vendors (LOUBERE & BREHM et al.) are all used in service of this social credit system. Coupled with a heavily censored internet, the CCP gathers and analyzes all the data, on all the online and offline behaviours and habits of all the Chinese citizens that fall under the purview of this program to assign a numerical score (Kobie et al.). This score is comprehensive and all-encompassing in its implications. A good score means special privileges such as first class plane tickets, better rates on mortgage and insurance, better

job opportunities, and even the chance to travel outside the country. A bad score entails higher scrutiny by authorities, more restrictive travel and financial privileges, lack of employment and even the potential of civil or criminal charges if your score is allowed to get too low (Ye & Chor et al.).

The way the scores are measured and updated in real-time is even more eerie. Actions such as donating to charity, only buying essential items, always following road signs, not using foul language, or saying bad things about the government all improve your score. Actions such as jaywalking (which are caught on the always-prevalent security cameras), buying too much alcohol, creating problems in the workplace or in your residential neighborhood all lower your score. Even searching up controversial news articles and installing banned apps (such as Facebook, Google, and some other American software) has the potential to lower your score (Ye & Chor et al.). On the technology and software side, any company (including any telecom and technology company) that is registered as a business in China is legally obligated to hand over any and all consumer data to the CCP. Furthermore, the severe restrictions imposed on foreign technology companies coupled with the creation of sovereign software and applications such as WeChat, Baidu Search engine, Alibaba, QQ.com, JD.com ensures that all of the Chinese consumer's internet needs are catered to within its borders.

Currently in the beta phase of the deployment, one of the regions that have been most adversely affected by the deployment of this system is the region of Xinjiang China, in particular due to its large population of ethnic Uyghur Muslims. As they have a different culture and value system than the majority of mainland China (and therefore are not always aligned with the ideology), after 2014 (following a string of uprisings and civil unrest (Tiezzi et al.)) the CCP began using their surveillance technology and the social credit system to rigorously monitor the

region and systematically root out any actors that strived to be contrarian to the narrative dictated by the CCP (Samuel et al.). Leveraging the technology and pairing it with policy, it is estimated that more than a million Uyghurs are currently situated in reeducation camps, as a result of these actions (Maizland et al.).

The way in which social credit scores are used particularly against the Uyghurs in Xinjiang China, will also be investigated in detail in the sections to come. In this paper, I will use the advent of digital social management and the social credit scoring system to demonstrate how these policy and technology decisions are actively being used to successfully suppress the Uyghur minority population. By using actor network theory (ANT) I will provide a more thorough and systematic analysis of how the sophistication, ubiquity and scale of these systems have enabled such large scale atrocities to be successfully carried out.

Conceptual Framework: Actor Network Theory

Actor Network Theory (ANT) is a Science Technology and Society (STS) concept that provides us with a powerful framework for systematically analyzing all the heterogeneous components and connections in the area of mass surveillance, as it pertains to the region of Xinjiang, China. In this paper, I will be using ANT to follow the form laid out by the French sociologist, Michel Callon. At its core, Actor Network Theory is a framework for analyzing and evaluating the formation and functioning of complex sociotechnical systems. The goal of ANT is to simplify heterogeneous elements with heterogeneous relationships into a cohesive network of human and non-human actors defined by their relative positions within the network (Callon 1987). To better understand and analyze the buildup and progress of the network we can use Callon's concept of translation (Callon, 1986), which is the process where functioning actor-networks are formed by and around a primary actor (or a few key actors). Callon lays out

four phases of translation: problematization, interessement, enrollment, and mobilization (Callon, 1986).

In the problematization phase, primary actor(s) appear and define the problem at hand to be addressed by the network, identify the necessary joint actors that need to be recruited, and charts itself down the path of the "obligatory passage point" (OPP) through which the other actors must pass to form a stable and mutually beneficial network. In the interessement phase, the primary actor then attempts to actively recruit the other actors into the network and to align their interests with the problem and OPP originally defined by the primary actor. During the enrollment phase, the other actors that have aligned with the problem definition are assigned roles and positions within the network by the primary actor(s). Importantly for this paper, enrollment dictates that the other actors in the network actually accept and faithfully carry out their assigned roles as intended. Finally, in mobilization, the primary actor(s) take up their role as the director and spokesperson for the actor-network, which begins to function as a cohesive whole.

I intend to use ANT to track the successful construction of this sociotechnical actor-network of mass surveillance. Using Callon's concept of translation, I intend to identify how key officials in the CCP, alongside the contributions of businesses and engineers, were instrumental in building and stabilizing the surveillance state actor-network in Xinjiang and how key technological commodities and policy decisions were leveraged for the wide-scale surveillance and detainment of the Uyghur Muslim population.

Analysis of the Actor Network surrounding surveillance in Xinjiang

Section 1: Network Components

The first step to understanding the socio-technical system of mass surveillance that is deployed in Xinjiang is to reconstruct the surveillance actor-network. This will provide us with key insights behind the network's success, and a critical framework to use for our analysis down the line. The first step would be to identify and define all the heterogeneous actors in the network. I have identified the central human or organizational actors by synthesizing them into relevant social groups. These actors are defined as follows: (1) the Chinese Communist Party (which includes the leader Xi Xingping, state officials, local government representatives, among other government-affiliated actors), who are the ones charged with creating the policies that are pivotal in the construction of the network, as well as ensuring that power is concentrated in the hands of key decision makers whose ideologies align with the long-term goals of the political party as a whole (VELGHE et al.); (2) law enforcement (which encompasses numerous actors ranging from local police officers to the national military) who are charged with enforcing policy and ensuring the buildup and stabilization of the network (they essentially act as an extension of the government actor-network)(VELGHE et al.); (3) businesses and other commercial actors (which includes executives, suppliers, engineers and other technologists, marketers and distributors) those who employ the resources, capital, entrepreneurial and technical skills at their disposal to construct the network in accordance to the policy and commercial directives (Li et al.) (Lin & Chin et al.); and finally (4) the Uyghur Muslims and other residents of the Xinjiang province of China, the ones who are subject to marginalization, within the scope of this analysis (Maizland et al.). In identifying key non-human actors we can classify the following groups: the electronic hardware devices (including but not limited to) CCTV cameras, networking equipment and drones, and the software systems such as facial recognition algorithms and (big) database systems (VELGHE et al.), whose existence and active application facilitated the building of the

socio-technical system, and aided the human actors in their objective of suppression the Uyghur populace.

Section 2: The Government Actors

The overarching role played by the government actors due to the totalitarian control exercised by the CCP in the surveillance of the Uyghur people of Xinjiang, China, entails that these government actors be assigned the role of network builder. They are the primary actors to follow and through whose eyes we can try to interpret the process of network construction (Cressman). If we follow these actors through the stages of translation, we can map the actions taken that have resulted in the surveillance actor-network that we have today. In the stage of problematization, given the hierarchical structure of the CCP, the primary actor that began the network would be Xi Xingping in the 2010s, after a series of attacks by Uyghur separatists and radicals over the years. In particular the 2014 Kunming station massacre in the region of Kunming, Yunnan (Tiezzi et al.) was pivotal to the start of the network (Leibold et al.). Since the problem of radical Islam still permeated the collective global consciousness at the time, and given the differences in cultures and values of the Uyghurs from the Communist ideologies, the problem statement for the CCP then became the indoctrination of the Uyghurs. In addition, the introduction of the Belt and Road Initiative in 2013, coupled with the economic significance of the region of Xinjiang, with its abundance of natural resources, served as key catalysts for the network builder (CCP) to enforce tighter controls on the region of Xinjiang region (Overton et al.). During the phase of interessement, when the politicians were formulating all the details of the system, businesses that cater to the surveillance industry were brought into the fold, in a mutually beneficial arrangement (more contracts meant more revenue). Furthermore, given the autocratic nature of the rule of law in China, individuals and even businesses have little leverage

to protest the ethical implications of such a program, so once the policy and business contracts were set, the phase of enrollment soon followed (Leibold et al.). To date, more than 20 million security cameras have been installed in the region of Xinjiang, and detainment camps housing more than a million Uyghur Muslims (for reeducation) have been constructed (Leibold et al.).

Section 3: The Commercial Actors

The role played by businesses and caterers of technology products contributed to the stabilization of the network. The political directive requiring the need of millions of cameras, networking technology and software products was of great benefit to businesses as multi-year contracts ensured stable jobs and consistent revenue for many of the companies in this space. Companies such as Huawei, Tencent, Alibaba are a few of the conglomerates (in addition to countless smaller companies) who are interwoven into the complex supply chain of surveillance technology and its distribution. In particular, Huawei, a prominent vendor of consumer electronics, telecom equipment and networking infrastructure, is one of the largest providers of all the hardware required to connect the vast network of surveillance cameras together (Maizland & Chatzky et al.). Tencent with its all-encompassing app WeChat (as it is known in the West) leverages the size of its user base and comprehensive list of features to ensure that any need of the consumer (including the Uyghurs) are catered to from the digital product, whether it be communicating with others, making payments, booking a doctor's appointment, looking for information, or any other societal function that a person could need. As a byproduct of its ubiquity, it ensures that WeChat has a comprehensive collection of all the digital (which in this case could very well mean all) interactions between citizens is permanently stored and available for analysis, providing the companies with a rare trove of insights into the collective psyche of

populations, including regional population (Li et al.). This insight is important as it provides the CCP (who by law require all commercial user data to be shared with them) to monitor in real time, the sentiment and psyche of the region of Xinjiang. As a result of these insights generated from digital technology, the CCP were able systematically root out any forms of dissent against the government and utilized the surveillance technology and user data to target specific individuals who are then subjected to re-education camps (Maizland et al.). By creating a robust and sophisticated technology pipeline, technology companies have ensured the stabilization of the actor-network and provided speed and efficiency to the efforts of the CCP to suppress its minority population.

An argument can be made whether companies can stop to do business with the government. Major technology companies such as Tencent and Alibaba are multinational companies, incorporated in the Cayman Islands and traded publicly in the Hong Kong and New York Stock Exchanges (Fried & Schoenfeld et al.), and their massive valuations ensure that they have enough economic power to live without the government contracts for building surveillance technology. However, given that the primary source of revenue for these companies are within China, and the nature of doing business in China involves companies complying with its strict laws on human governance, we come to understand the incentives for these profit-seeking companies do not align with the humanitarian goal of preventing misuse of these technologies. Similar to how IBM and Intel continued to do business with South Africa during the apartheid and provided key technology used in the suppression of the populace (NARMIC et al.), when incentives do not align with the public good, profit-seeking enterprises often choose what's best for the company over what is best for the people.

Furthermore, we can also make the argument that the suppliers of electronic components (the ones who provide the components that tech conglomerates then use to create the final products) could choose to refuse to do business with government and corporate vendors that use their technology for such purposes. However, the same argument of incentives applies here as well.

Section 4: The Scientists and Engineers (Technical Actors)

While policy and business decisions were the primary contributing factors in the establishment of the mass-surveillance actor-network, an argument can be made about the contributions of scientists and engineers that utilized their technical proficiency and time to collectively come together and construct all the key technological components that led to the success of this socio-technical system in the suppression of the Uyghurs. Key technological components such as: circuit boards, microchips and camera sensors that were assembled to create surveillance cameras, the firmware that networked millions of these cameras together, and allowed a central operator to monitor and archive the daily movings of millions of people, the development and deployment of deep learning facial recognition algorithms (Mina and Chipchase et al.). These algorithms utilized the archived footage as training data to singularly identify every individual person from a pool of millions, often in real time, to give the government and business operators even more granular and efficient data, to enable the creation of comprehensive digital dossiers (Lin & Chin et al.). All of these components greatly increased the efficiency and speed at which individual action could be surveilled, which enabled the government and corporate actors to take action, especially when a person's actions fell out of alignment with the government policy or ideology. From this perspective, it is evident that the collective actions of these countless technical actors played a key role in the building and

stabilizing of the mass-surveillance actor network. There are several ways that preventative action could have been taken by these technologically competent actors to prevent the widespread abuse of these technologies to the suppression of the Uyghur minority. Data obfuscation and siloing, where a programmer could ensure that data is not personally identifiable, is a technique that they can employ to prevent targeting and discrimination by the facial recognition algorithms of the minority population. Scientists and engineers could also choose to go on strike as a possible means of protesting the use of their work in such negative ways. However, due to the incentive structure and the harsh penalties (including but not limited to, unemployment, societal harassment and even prison time) involved with individuals who opposed the CCP's agenda (Kobie et al.), the cost of protesting or refusing to contribute to the building of this network is much higher in China than it is in contemporary Western nations (Mina and Chipchase et al.). For example, American software engineers can protest the use of their work in military applications (such as the walkout staged by Google employees (Shane & Wakabayashi et al.)) without suffering the same sort of repercussions as their Chinese counterparts. Therefore, while considering this line of argument, due to the overwhelming higher power held by the government actors, and the prevalence of the collective mindset over the individual mindset, engineers and scientists have little leverage to act against the building of the network, and consequently, the responsibility of the misuse of this socio-technical system falls under the purview of the CCP.

Conclusion

The objective of this paper is to demonstrate how the state of mass surveillance and the advent of the social credit scoring system (enabled by the surveillance) have led to widespread ethnic discrimination (some would say ethnic cleansing) in the region of Xinjiang China (in particular

of the Uyghur people of that region). By analyzing the actors and network builders involved in the construction and maintenance of this comprehensive socio-technical system, and the numerous driving factors involved in the system, such as policy decisions, economic incentives, technological proficiency and ubiquitous deployment of artificial intelligence, and by using the tools provided to us by Actor Network Theory, such as the concept of network translation, we are better able to identify the all the human and non-human actors and their unique contributions to the success of the network, whether it be the deployment of hardware or software products, policy enacted to provide greater leeway for government authority to acquire and utilize personal data (in the form of payment, location, online behaviour, public behaviour and numerous other data points), and the actions taken as a result of the data-driven decision-making. With these analyses in mind, the average reader will be more cognizant of how human decisions regarding the use of cutting-edge technology, especially when it serves an opportunistic purpose, can have negative consequences on the lives of those who fall out of favor with the successful party's goals.

Total Word Count = 4149 words

Works Cited

- Andersen, R. (2020, July 30). The panopticon is already here. Retrieved March 16, 2021, from https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/
- Callon, M. (1986). Some elements of a sociology of translation: The domestication of the scallops and the fishermen of St.Brieuc Bay. In J. Law (Ed.), Power, action & belief: A new sociology of knowledge? (pp. unknown). London: Routledge & Kegan Paul
- Callon, M. (1987). Society in the making: the study of technology as a tool for sociological analysis. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), The social construction of technological systems: new directions in the sociology and history of technology (pp. 83–103). Cambridge, MA: MIT Press.
- Cressman, D. (2009, April). *A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation* [PDF]. ACT Lab/Centre for Policy Research on Science & Technology (CPROST) School of Communication, Simon Fraser University.
- Fried, J., & Schoenfeld, M. (2019, February 4). The risky business of investing in Chinese tech firms. Retrieved April 27, 2021, from https://corpgov.law.harvard.edu/2019/02/04/the-risky-business-of-investing-in-chinese-tech-firms/
- Kobie, N. (2019, June 07). The complicated truth about China's social credit system. Retrieved March 16, 2021, from https://www.wired.co.uk/article/china-social-credit-system-explained

- Latour, B. (1986). The powers of association. In J. Law (Ed.), Power, action and belief: A new sociology of knowledge? (pp. 264–280). London: Routledge & Kegan Paul.
- Leibold, J. (2019). Surveillance in China's Xinjiang REGION: Ethnic Sorting, coercion, and inducement. Journal of Contemporary China, 29(121), 46-60. doi:10.1080/10670564.2019.1621529
- Li, J. (2019, September 13). A US official says tech Giants Alibaba and TENCENT present similar risks as Huawei. Retrieved April 27, 2021, from https://qz.com/1708662/chinese-tech-giants-tools-of-the-communist-party-us-official/
- Lin, L., & Chin, J. (2017, November 30). China's tech giants have a second Job: HELPING BEIJING spy on its people. Retrieved March 18, 2021, from https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284
- LOUBERE, N., & BREHM, S. (2019). The Global Age of Algorithm: Social Credit and the Financialisation of Governance in China. In Franceschini I., Loubere N., Lin K., Nesossi E., Pia A., & Sorace C. (Eds.), *Dog Days: Made in China Yearbook 2018* (pp. 142-147). Acton ACT, Australia: ANU Press. Retrieved April 27, 2021, from http://www.jstor.org/stable/j.ctvfrxqcz.29
- Maizland, L. (2021, March 1). China's repression of Uyghurs in Xinjiang. Retrieved March 18, 2021, from https://www.cfr.org/backgrounder/chinas-repression-uyghurs-xinjiang
- Maizland, L., & Chatzky, A. (2020, August 6). Huawei: China's controversial tech giant. Retrieved April 27, 2021, from https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant

- Mina, A., Chipchase, J. (2020, April 02). Inside Shenzhen's race to outdo Silicon Valley. Retrieved March 16, 2021, from https://www.technologyreview.com/2018/12/18/1661/inside-shenzhens-race-to-outdo-silicon-valley/
- NARMIC, & American Friends Service Committee. (1982). *Automating apartheid, U.S. computer exports to South Africa and the arms embargo*. NARMIC; American Friends Service Committee. Retrieved April 27, 2021, from https://jstor.org/stable/10.2307/al.sff.document.bmdv3
- Overton, T. (2016, January 01). The energy industry in Xinjiang, china: Potential, problems, and solutions. Retrieved March 16, 2021, from https://www.powermag.com/energy-industry-xinjiang-china-potential-problems-solutions-web/
- Review, S. (2019, December 07). How far has China's electronics industry come? - Part 1. Retrieved April 28, 2021, from https://medium.com/@ecruiser/how-far-has-chinas-electronics-industry-come-part-1-c3ff7523cf4
- Rupp, M. (2020, June 5). Data obfuscation. Retrieved April 28, 2021, from https://www.cryptomathic.com/news-events/blog/secure-hardening-for-mobile-banking-apps-data-obfuscation
- Ryan, F., Pascoe, A., Hoffman, S., Garnaut, J., Izenman, K., Johnson, M., & Thomas, E. (2020). *The flipside of China's central bank digital currency* (pp. 19-22, Rep.). Australian Strategic Policy Institute. Retrieved April 27, 2021, from http://www.jstor.org/stable/resrep26895.10

- Samuel, S. (2018, August 17). China is going to Outrageous lengths to surveil its own citizens. Retrieved March 16, 2021, from https://www.theatlantic.com/international/archive/2018/08/china-surveillance-technology-muslims/567443/
- Shane, S., & Wakabayashi, D. (2018, April 04). 'The business of WAR': Google employees Protest work for the Pentagon. Retrieved April 27, 2021, from https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html
- Thompson, D. (2019, May 30). A tale of two surveillance states. Retrieved March 16, 2021, from https://www.theatlantic.com/technology/archive/2019/05/the-us-and-china-a-tale-of-two-surveillance-states/590542/
- Thomala, L. (2021, February 09). China: Number of internet users 2020. Retrieved April 27, 2021, from https://www.statista.com/statistics/265140/number-of-internet-users-in-china/
- Tiezzi, S. (2014, March 04). Is the KUNMING knife ATTACK CHINA'S 9-11? Retrieved March 18, 2021, from https://thediplomat.com/2014/03/is-the-kunming-knife-attack-chinas-9-11/
- VELGHE, P. (2019). "Reading China": The Internet of Things, Surveillance, and Social Management in the PRC. *China Perspectives,* (1 (116)), 85-89. Retrieved April 27, 2021, from https://www.jstor.org/stable/26663907
- Ye, K., & Chor, L. (2018, December 12). China's citizen tracking system can wreck people's lives. Retrieved April 27, 2021, from

https://www.vice.com/en/article/gy7kpb/chinas-citizen-tracking-system-can-wreck-peoples-lives

- Zheng, W. (2020, August 09). What is WeChat and what can it do? Retrieved April 27, 2021, from https://newseu.cgtn.com/news/2020-08-09/What-is-WeChat-and-what-can-it-do--SNepY1rgNG/index.html