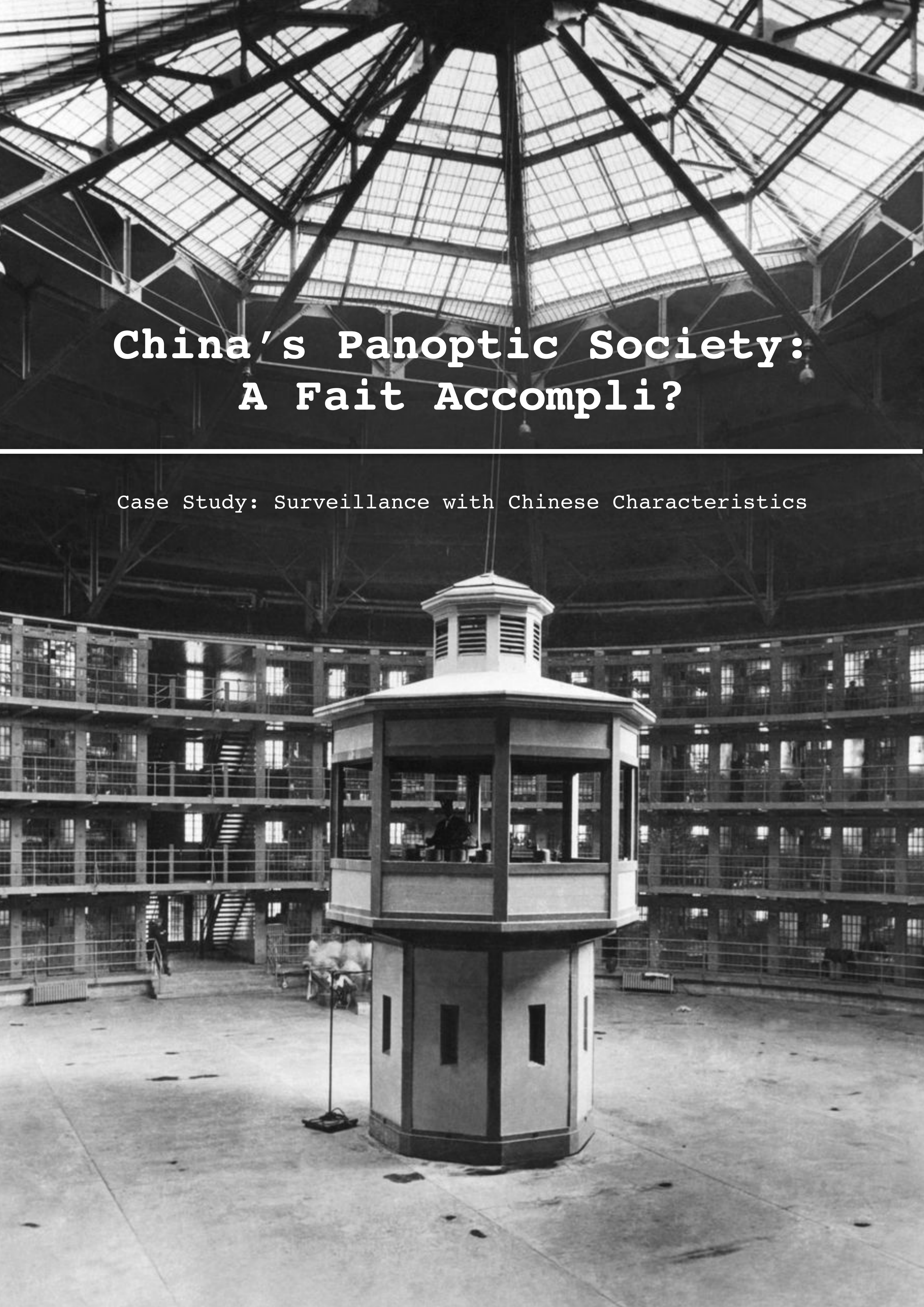

# China's Panoptic Society: A Fait Accompli?

Case Study: Surveillance with Chinese Characteristics

Master Thesis
MSc. Crisis and Security Management
Researcher: Martijn Bomas
Word Count: 19.053
2020

## Preface

Before you lies the dissertation *'China's Panoptic Society: A Fait Accompli ?'*, a case study of surveillance with Chinese characteristics. The research has been done to fulfil the graduation requirements of the MSc Crisis and Security Management at Leiden University.

The project was born from an interest in China's surveillance capabilities that is frequently getting mischaracterized by Western media. Foreign media have depicted the "all-seeing eye" and the Panoptic state as a dystopian reality; this research examines if the Panoptic state is already realized and presumably irreversible, hence a fait accompli.

The author would like to thank supervisor and assistant professor James Shires for his guidance and feedback throughout the writing process.

**Martijn Bomas**

## Table of Content

## 1. Introduction

We are living in the golden age of surveillance, and the technological advancements of our time will only enhance the endless capabilities within the domain of surveillance (Schneier, 2015). Security and surveillance are matters that are addressed daily by scholars, media and politicians, but what trade-off is the Chinese society paying for safety? Political scientist Theodore Lowi warned in the 1990s that a George Orwell type of scenario would be plausible with the rapid development of technology (Lyon, 1994, p. 57). Fast forward thirty years and the question emerges if the technology has brought us closer than ever to the realization of a Panoptic society or is it already a fait accompli?

Nation-states have extensively expanded and intensified their surveillance programs to improve and safeguard their national security, illustrated by the revelations of Edward Snowden (Snowden, 2019). China is now the global market leader in the field of surveillance, regularly obtaining global headlines with the Social Credit System (shehui xinyong tixi - SCS) and its unparalleled methods of surveillance. Beijing furthermore holds the titles of the most surveilled nation-state and the *'world's worst abuser of internet freedom'* for the 4th consecutive year (Zhang, 2019a; Freedom House, 2019). Illustrating the desire of the Chinese Communist Party (CCP) to monitor and control society, both online and offline.

The characterization by the Western media, however, fails to portray the fractured state of the surveillance apparatus. There is a vast amount of programs such as Skynet (Tiangwang), and Sharp Eyes (Xue Liang) that showcase that there is no evenly-distributed main surveillance system (Ahmed, 2019). Foreign media have painted a dystopian portrait of a Panoptic society with social credit ratings while in reality, it is nowhere close to Black Mirror fantasies (Horsley, 2018). This research wants to correct the narrative by giving insight into the surveillance apparatus and its underlying motives.

Surveillance has a wide range of governmental purposes and is frequently co-occurred by authoritarianism and totalitarianism. It enables the micromanaging enforcement of non-dissents in part by the help of -technological - surveillance, leading to what Paul Mason (2017) describes as the death of democracy, outlining the universal significance for the growing amount of nation-states adopting surveillance with Chinese characteristics. Surveillance and technology are thus interconnected to the development and bolstering of a Panoptic society. The Panopticon from Foucault carries over the old forms of power from Nineteen Eighty-Four touching upon two essential points; the accumulation of power and the direct supervision of subordinates (Lyon, 1994). Both elements can be traced back to the motives of the Party and its social governance style.

Surveillance is thus on the rise, and more nation-states around the globe are adopting Chinese-style surveillance techniques (Mozul, Kessel, Chan, 2019), there is, despite, an academic gap between connecting the enhanced technological capabilities to the construction of a potential Panoptic society. There is a far-reaching theoretical basis for understanding contemporary surveillance, though it fails to portray a full picture of the influence and scale of modern-day technologies. Mainland China, identified as the pinnacle of technological surveillance, will be the departure point upon testing Foucault's Panoptic theory. China's leading role within the surveillance industry (Feldstein, 2019; Mozur, 2019) and its current state of affairs provides a threshold upon examining the theory of Foucault on a national level.

The aim is to give insight into the development of Facial Recognition Technology (FRT) and Artificial Intelligence (AI) and how they are affecting the Chinese surveillance industry combined with the aspect of social governance. It is the puzzle if the physical and digital technological advancements will create and bolster a Panoptic society. Will the citizens of mainland China be prisoners of the Panoptic system? Based on the elements, the following research question is formulated:

*“How well does Foucault’s Panoptic society theory explain the development of Facial Recognition and AI, in 21-century mainland China?”*

The centrepieces of technological innovation will be AI and FRT due to theoretical, political and economic considerations. China is the global leader of AI technology that is rapidly proliferating around the globe. FRT in combination with Closed-Circuit Television (CCTV) furthermore embodies the asymmetrical relationship and Orwell’s dystopian image depicted by Western media. Both elements of technology play a significant role in the increased amount of surveillance worldwide (Wood, 2017; Robbins & Henschke, 2017: Hou, 2017) and the capability upon constructing a Panopticon.

## 2. Theoretical Framework

There is an increasing amount of awareness regarding the topic of surveillance blended with an ever-widening number and types of surveillance technologies (Galic, Timan, Koops, 2015; Espoti, 2014). Scholars from a range of disciplines are analyzing surveillance and its modern-day implications, which gave rise to the discipline of surveillance studies (Galic et al., 2015). Surveillance is a multidisciplinary field focusing on topics as the current and near-future surveillance in societies on areas such as policy, governance, privacy and security. It is, nonetheless, not an entirely new phenomenon, and, according to Ian Hacking (1990), an integral part of society and the interpretation of the nation-state. Surveillance has become interconnected to the notion of security and entered our daily lives, both in a visible and invisible form, affecting citizens from Asia to Latin America. Edward Snowden revelations provided confirmation that states are involved in extensive surveillance programs and thus involved in tracking the movements of its citizens both in the online and offline world (Snowden, 2019; Greenwald, 2014; Harding, 2014). While it is known that governments are involved in surveillance programs, the revealed documents showcased the extensive scale that the NSA and Government Communications Headquarters (GCHQ) monitor their citizens. Liberal democracies are major users of AI surveillance technology (Feldstein, 2019) and hence its fueling and generating the fear that Western liberal democracies could descend into authoritarian nation-states, as described by Paul Mason (2017). The rise and evolution of surveillance is a topic of global importance and thus needs to be examined to study the current state of affairs to analyze what the foreseeable future conceivably holds for Western democracies.

### Orwell’s Vision as point of Departure

A returning metaphor within the arts of surveillance is the Panopticon, made famous by Michel Foucault in his novel *‘Discipline and Punish’* from 1975. It has become the preeminent model within the discipline of surveillance for the analysis of a nation-state (Caluya, 2010); the framework is further examined in chapter 2.2. The work of Foucault is closely related to the futuristic vision of Orwell (1949), that could not have foreseen what the marriage of technology and surveillance makes possible in terms of Big Brother capabilities. The novel of George Orwell has clear-cut points of departure that deviate from the current state of surveillance. In the novel, the upper and middle-class are subject to extensive monitoring, while the lower-class of society named the *proles* are left out of scope. Notably, the revelations of Snowden showcase that the apparatus of mechanical-surveillance is applied to everybody in society. Another essential distinction is the parties that are involved as an agent of surveillance; this is no longer bound to the state alone; non-state institutions are involved in the monitoring of society in the 21st century. Modern-day China is adopting the combination of state and non-state institutions that are monitoring the entirety of society, thus including the *proles* (Haggerty & Ericson, 2003).

There is a large body of literature associated with contemporary methods of surveillance, but the implications for society, its social consequences and the possible rise of the Panoptic society are found in a defined amount of work (Espoti, 2014). There is a literature gap regarding the analysis of the technological advancement made within the domain of surveillance that could lead to a realization of Orwell’s novel within mainland China. To have the right tools of analysis, the case study will make use of two theories of choice. The theory chapter will start with Copenhagen School’s Securitization theory followed up by the Panopticon of Foucault.

### 2.1 Copenhagen School's Securitization Theory

The concept of securitisation is widely used within the domain of security studies and is commonly associated with the scholars Waever and Buzan from the constructivist Copenhagen School. The notion of securitisation was first developed by Waever in 1995 with the chapter *"Securitisation and desecuritization"* in the book *"On Security"* by Professor Ronnie D. Lipschutz. Securitisation is defined as *"shifting an issue out of the realm of normal political debate into the realm of emergency politics by presenting it as an existential threat"* (Peoples & Vaughan-Williams, 2010, p. 76). It is a process of portraying a particular problem as an existential threat which, if accepted, allows for the suspension of normal politics and the use of so-called emergency measures (McDonald, 2008). The threats get outlined in the form of a speech act by an institutional voice. Defined by Waever as *"if a state-representative uses the language of security it moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it"* (Waever, 1995, p. 55).

The theory is envisioned towards the norms of the Western hemisphere with integrated terms such as the rule of law, and open political deliberation, consequently forming a Western-based inclination. Although the theory favours a state-society relation, it has begun expanding outside of the European borders to places such as Hong Kong (Curley & Wong, 2008; Emmers et al., 2008; Lo Yuk-ping & Thomas, 2010) and India (Upadhyaya, 2006). The divide between China's political system and the Western liberal democracies furthermore creates a split, shifting the gravity of the theory towards how Beijing is framing existing and new problems, both offline and online, to vindicate its actions towards Chinese society. It is predominantly a state-centred framework that allows political leaders to speak on behalf of national security; thus, it can be implemented to elements of the offline and online world. The expansion of the theory outside of the European borders provides a first glance at the future implications outside of the standard Eurocentric framework. This research is expanding the boundaries of the theory towards unexplored territory, testing its usage within a Chinese case study with a surveillance backdrop.

The facilitating conditions differ from China vis-à-vis a Western liberal democracy; the process of securitisation is therefore altered, which influences the securitisation act and sequentially the securitisation process. First off, China is a one-party state, effectively controlling all institutions and thus, the space of policymaking (Nathan, 2003, p. 13). Even though the Party is under full control, the acts of securitisation are still crucial for the Party's legitimacy and domestic image vis-à-vis the ruled. The theoretical framework thus provides an understanding of the Party's policy making and process upon building a possible Panoptic society, as described by Western media outlets (The Guardian, 2019). The theory is giving a critical security viewpoint that progressive ends can be achieved through security rather than without. The Copenhagen School addresses securitised topics as covered in secrecy and urgency with a limited amount of actors getting to contribute to a solution (McDonald, 2008). Secrecy and urgency are both intertwined with Chinese policymaking, thus making it applicable for further scrutinising of the research topic.

While the securitization theory is another Western approach outside the place of origin, it provides a framework on understanding the securitization moves of the Party (Bilgin, 2011). It is establishing a bridge between the realm of politics and security, hence questioning the threats that are at stake and whose safety is at stake. The Chinese security context, though, various from the Western conception of security, thus affecting the contextualization of the connection within the case study. Chinese commentators have noted that the necessity of using security language is not necessary, for instance, on the domain of climate change due to the central policymaking and implementation methods. Securitization nevertheless provides an insight into the vindication of a politically costly action (Trombetta, 2019). It extends the scope of the Chinese context on (non-) traditional threats and the logic and practices. For the Party to rule effectively, the state power must be seen as legitimate by not only the rulers but also the ruled (Yang & Zhao, 2015), outlining the importance of the theory in relation to the case study. Chinese commentators have differentiated between the handling of national security practices and non-traditional threats within mainland China, contrasting that the initial one gives the opportunity upon applying all means necessary (Trombetta, 2019). The emerge of non-traditional threats hence gave an insight into the mechanism of security outside of the traditional sphere, such as the research done by Yan Bo on Chinese climate change policy (2016). Ultimately, there is an overlap between the domain of national security affairs and the – performance – legitimacy of the Party to safeguard the nation-state.

### 2.2 Foucault’s Panopticon

Foucault model of surveillance occupies a *central* role in this research. The Panopticon, based on Bentham’s work, is an annular building that has a central guarding tower in the middle, providing the warden with full oversight of the events within the building. The prisoners, on the other hand, do not know if the guard is watching; thus, the prisoners have to assume they are always being observed. Foucault described that *“the major effect of the Panopticon is: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power”* (Foucault, 1977, p. 124). It represents an asymmetrical power relationship between the correctional officers on the one hand and the inmates, which can be applied to modern-day society.

Foucault provides a metaphor for understanding contemporary surveillance as a theory of power. Individuals do not know when the guards are observing them, thus leading to the disciplinary aspect of the panoptic that requires the prisoner to reflect on their behaviour, e.g. productive soul training, to ultimately transform the inner self (Haggerty & Ericson, 2003). The metaphor of the Panopticon was constructed as a theory of power to be extended beyond the scope of the prison, providing a framework on understanding the mechanism of power and surveillance within society. Foucault Panopticon furthermore shares the concept of Orwell’s novel that there is a central core of oversight, a single actor that is all-seeing. The central guarding tower in the Panopticon is Big Brother in the novel 1984, a singular state actor that induces a state of permanent visibility. The Panopticon is criticized due to the lack of possibilities on explaining modern surveillance technology within the framework of power (Haggerty & Ericson, 2003; Caluya, 2010). Consequently, variants of the Panopticon have been constructed such as the Electronic Panopticon by Diana Gordon (1987) or the Super Panopticon from Mark Poster (1990). While this research acknowledges the limitations of Foucault’s concept, it will not stretch the definition beyond its initial context but alternatively, draw from additional explorative tools.

There are numerous of studies that provide a linkage between surveillance and social control; there is, nevertheless, a gap determining the implications on society via self-surveillance and the construction of a Panopticon as depicted by Western sources. The vision of the Panopticon was to internalise discipline; you can always be monitored at any moment of the day, creating the urge for self-discipline. It is the principle of *‘seen-but-not-be-seen’* that is creating a relationship between the surveillance techniques and the outcome of social control. Scholars, as mentioned before, have also turned to new frameworks, so-called ‘post-panopticism’ to understand the contemporary social and technological developments that have their impact on surveillance and consequently society (Caluya, 2010). One of the primary surveillance studies at the theoretical turning point has been *‘the surveillant assemblage’* (2000) by Haggerty and Ericson. The assemblage consists of a *“multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they work together as a functional entity”* (Patton, 1994, p. 158). The surveillance assemblage operates by creating flows of information that separates members of society into groups, thus creating a virtual data double. The technological developments of our time, such as AI, FRT and Big Data, make it possible for the assemblage to operate, reassessing the idea of the Panopticon within a digitalised society.

Technologies that are closely intertwined with surveillance are AI and FRT, with at least 75 out of the 176 nation-states globally making use of AI-driven surveillance techniques (Feldstein, 2019). The effectiveness of the technology is up for debate, but the use of FRT and AI has become more pervasive and invasive in the 21st century. An increasing amount of nation-states are adopting advanced AI surveillance for monitoring, tracking and surveilling, both lawfully and unlawfully. AI surveillance technology intertwined with the Panoptic element of FRT with CCTV is thus the pinnacle of modern-day surveillance, requiring further scrutiny to understand the possible Panoptic effects on society. Analysing the Chinese domestic domain of AI and FRT is furthermore closely interconnected to political and economic policymaking (Feldstein, 2019). Requiring an understanding of the political system for explaining the nature of securitisation in contemporary China (Breslin, 2015).

Securitisation is ultimately used as a tool to understand the securitisation process of the Party, where security is intertwined with national policy and objectives (Trombetta, 2019). The Panopticon is the possible outcome of the relating policies, establishing a sense of being always monitored via cameras in the *offline* domain. To quantify the theory of the Panopticon, there is a break down into four separate points of analyses that are derived from the literature. First, there is the exploitation of modern-day technology by securitizing technical elements for the self-interest of the Party. Secondly, there is the element of self-surveillance. Third is the presence and acting of a unitary actor, a so-called ‘all-seeing eye’ of oversight, the Big Brother factor. The last point of analysis is the presence of blanket coverage of surveillance across mainland China. Points mentioned above provide vital indicators to verify the presence of a Panopticon society. The theories of Securitization and the Panopticon are thus used to analyse the Western assumption that there is a Panoptic society established within mainland China, creating the feeling in public spaces that citizens are under continuous surveillance.

## Definitions

Technological surveillance systems are used to measure the societal and political control of the Party within mainland China. With technical surveillance systems being interpreted as the whole of online and offline surveillance systems present on behalf of the Chinese state apparatus, including surveillance cameras in public spaces and the online monitoring of internet usage. Hence, it is the incorporating of the digital in the physical world to create an all-seeing system. While online monitoring is taking into consideration, it will not be explored in-depth due to the scope of the research. There is furthermore made no distinction between the Panoptic gaze operated by humans or AI-driven technology.

Surveillance is defined in various forms with either a neutral (Giddens, 1985) or negative perception (Foucault, 1977). This study will define surveillance using the definition from Gary Marx, as *"the use of technical means to extract or create personal data"* (Gary Marx, 2002, p. 12). Social behaviour is defined from the perspective of the Panopticon and the vision of Bentham, of constant monitoring and the urge for self-discipline. This research takes the approach of using Foucault's Panopticon, while it embraces the philosophy it will not fully embrace every aspect of the concept. It will use the theory of Foucault and Securitization as a tool kit to draw from selectively in light of the analytical task at hand (Deleuze & Foucault, 1977, p. 208).

The Chinese government, the Chinese Communist Party (CCP) and the Party are used interchangeably throughout the research paper due to the Chinese regime being a one party-state. The CCP penetrates all other institutions and hence also makes policy for all realms of action (Nathan, 2003, p. 13); thus, this research paper makes no distinction between the terms.

### Implication of the theories

Both theories provide a distinct perspective on the surveillance capabilities of the Chinese nation-state. The theory of securitization offers an alternative lens compared to the traditional approaches, thus giving new insights into the political acts of the CCP. While the Party, with the Politburo Standing Committee (PSC[1]), has a central decision-making body, the act of securitization can still be used to visualize the process and justification of the costly political action (Nathan, 2003; Trombetta, 2019). The securitization theory thus prioritizes the security issues, showcasing the process of the Party, with the Panopticon being the conceivable outcome of the policies. The Chinese system is furthermore incorporating private institutions to improve the system of surveillance, with the Panopticon being centred on the inner core of power: the state. The overall elements of the Chinese surveillance system could hence be fragmented, but later in the process combined to create a feeling that is relatable to the Panopticon (Ahmed, 2017; Creemers, 2018). While there is no possible distinct singular unit of Big Brother, as framed by Orwell, the actors could create a sense of surveillance that is done by a sole actor within society, hence creating a feeling that the all-seeing Big Brother Party controls the Panopticon. The research thus acknowledged the limitation regarding the fractured state of surveillance, it, however, uses the element of self-surveillance of the Panopticon as an end goal of the Party. The end goal is described as inducing a state of conscious and permanent visibility, making citizens believe that wherever they travel the surveillance will be continues in its effect, even it would be discontinuous in its action (Foucault, 1977).

[1] The Politburo Standing Committee (PSC) is the party's key decision-making body since the reform era in the 1970s. It is composed of five to eleven members that discuss and implement policy if the Politburo is not in session (Miller, 2016),

## 3. Setting the scope

The correlation between technological advancements within the domain of surveillance and the development of the Chinese Panopticon is at the core of this research. As aforementioned is China leading the dance on the field of surveillance (Feldstein, 2019), making it a suitable case-study for scrutinising the development of a Panoptic society. As the world leader of AI-based surveillance, it provides a threshold upon testing the claim, made by the Western media, that there is Panoptic society in place.

The research will be conducted by the use of analytical framework made off a tri-fold of elements, (1) policy and state-centred ambition, focused on AI and FRT (2) domestic implementation and (3) tools of mass surveillance. The model is built on the work of scholar Sara Espoti (2014) on dataveillance. The analytical framework is constructed to guide the information towards answering the research question. The subsection of policy and state-centred ambition will focus on the integrated use of newly developed technologies within the domain of surveillance, principally focusing on AI and facial recognition. Analysing the national policy set out by the Party for the domains of AI and FRT. Furthermore providing an informational background of the methods— leading to the first sub-question: *"How do technological advancements in surveillance change/affect the forms of control available to the government?"*

The second part of the analysis will focus on the domestic implementation of the policies mentioned above set out by the Party. Related questions are, which agencies and enterprises are involved with the domestic surveillance apparatus and *who* is effectively doing the monitoring. The second sub-question is: *"What is the Chinese strategy for implementing and usage of Artificial Intelligence and Facial Recognition?.*

The last element of the analysis, tools of mass surveillance, will combine the answers of both sub-questions to provide a framework for understanding the potential construction of a panoptic society. A selection of technological advancements will be examined within the shared domain of AI and FRT. What are the constructed innovations and the implication of the technologies on the construction of a Panoptic society? The SCS and other relevant methods of surveillance will be taken into account due to the Panopticon being a holistic construct of all elements. The Panopticon is a feeling created by all elements of surveillance that are deployed by state and non-state parties.

This study is a contribution to the field of critical surveillance studies by using a case study to explain the relationship and phenomenon of surveillance and social control. The use of a single case study gives the possibility to provide an in-depth insight into the phenomenon of surveillance in relation to the creation of a panoptic society. A singular case study will give the focus to understand contemporary surveillance in contradiction to a comparative analysis. China has manifested itself to be a unique case with the current 'information' policy of President Xi Jinping, using technology for upgrading societal and political processes (Velghe, 2019; Feldstein, 2019). It is providing a unique insight into what the media portrays as the *'surveillance state'* (WSJ, 2018), making it the case study of choice to understand the Panoptic theory within the 21st century.

The research will address the literature gap, as mentioned beforehand, via content analysis. Data will be collected by the use of secondary sources, such as but not limited to official government reports released by the CCP, academic literature, reports and books on surveillance such as *‘Data and Goliath: The Hidden Battles to Collect your Data’.* Reports such as the Informatization Development Strategy and the New Generation Artificial Intelligence Development Plan will be used to get insight into the strategy of China within the relevant domains. Governmental technological documents, in combination with academic literature, are essential to examine the pathway of Chinese development within the AI and FRT sectors.

Extensive reports such as the China AI Development Report 2018 by the China Institute for Science furthermore gives insight into the policy environment and market applications. Documents that are published in mandarin, such as the New Generation Artificial Intelligence Development Plan, are translated by independent and reliable organisations such as New America, which is done by leading and experienced linguists such as Rogier Creemers, of the Leiden Asia Centre and Graham Webster of Yale Law School China Centre. Non-governmental documents by – mostly Western – academia, think tanks and private institutions, such as the Journal of Contemporary China and the DigiChina Project by Stanford & New America connect the technological advancements into an overarching system which will be used to scrutinise the overall impact of the surveillance systems. Surveillance is a sensitive topic of interest, especially for the Chinese government. Policy documents will give insight into the ambition of the Party, but it will not provide full disclosure over the procedures that are practised. Hence this study will also rely on Western data to get a comprehensive, holistic perception of the surveillance system.

Reliability and validity both need to be taken into account on using a case study. Case studies are often criticised on being biased towards the interpretation of data and literature; this study seeks out to balance the scale of literature from both the West and the East, although the constraint of literature in mandarin might impose a Western bias on the outcome. The research is furthermore focused on technological surveillance within mainland China, constraining the generalising result due to it being a single case (Yin, 1984). The research scope is furthermore limited due to time constraints to the geographical area of mainland China, thus excluding Taiwan, Hong Kong and Macau. The aim is to provide a study on surveillance as a stepping stone for additional research within the domain of surveillance with a Panoptic research-scope.

## 4. Case Selection

Before diving into the surveillance apparatus in place, there will be an analysis of the current theories and policies that affect the case study. The current mechanism of surveillance deployed in mainland China is characterized by information asymmetries and unequal distributed power dynamics (McMullan, 2015). Consequently, there is a set of elements in place that grant the state the possibility to monitor citizens intensively — illustrated in the fact that eight out of the ten most-surveilled cities around the globe are located in mainland China (Bischoff, 2019a). On top of that, Beijing has the ambition of constructing a dazzling amount of CCTV cameras, leading to a potential ratio of one camera for every two citizens in 2022.

To adequately scrutinize the surveillance state, an overall set of elements needs to be addressed to construct a holistic approach. The state-centred policies will be addressed due to it forming the core of the Chinese political and economic pathway. Moreover introduced is the concept of performance-based legitimacy, that forms the foundation of the Party's power. As CGTV[2], a state-run news media claimed *"to understand China, one has to understand the Party"* (Hoffman & Mattis, 2016). It is followed up by an insight into Xinjiang province, frequently named the surveillance laboratory of China. Afterwards the state agencies are discussed and what their role is within the grand picture of surveillance. The case study selection sub-chapter will provide the necessary background for understanding the motives of the Party regarding the construction of the surveillance apparatus.

### State Centered Policies

China is continuously adjusting and improving its surveillance systems towards modern-day technology. Resulting in the fact that Beijing spends more on the monitoring of its people than guarding it against foreign threats (Anderlini, 2019), exemplifying the obsession of the Party to observe society. The obsession for domestic surveillance and security is a result of China's internal struggles and the evolved desire from the Party for complete authority.

Security is an accentuated discourse on vulnerability (Barnett, 2001, p. 2) that is more socially constructed by an actor instead of objectively determined. Hence the definition of – national – security can shift and change over time. The process of securitizing vulnerable objects and the defining of a particular risk, in this case for the Party, is hence a political one (Waever, 1995). The definition of national security determined by Beijing has shifted with time, presently including non-traditional threats such as climate change (Trombetta, 2019). The Party can thus adjust the definition of national security and what is perceived as a national threat.

China has come a long way, and after remarkable periods of growth, since the opening up of the economy by Deng Xiaoping, the nation-state is now defined as an upper-middle-income country that has lifted 850 million people out of poverty (World Bank, n.d.) There is a wide range of theories attempting to explain the successful development of the Chinese nation-state. Still, they tend to attribute the success to government policies and the institutional designs (Hongxing & Zhao, 2015). State-centrist theorist claim that the autonomy the state enjoys is allowing Chinese leaders to adopt policies that might not be in line with market principles but are positively rewarding in the long term. On the other side are the neoliberal scholars, arguing that the market-oriented policies have provided economic growth.

[2] China Global Television Network (CGTN) is a Chinese English-language news agency controlled by the Publicity Department of the Communist Party of China

The autonomy enjoyed by the Party to adjust policies and implement new ones is providing to be crucial upon setting new trajectories. Due to the government being a one party-state (Nathan, 2003), the Party can implement policies it deems necessary for political or economic progress. The same principle can hence be applied to the securitization and defining of particular risks. Effectively granting the CCP the ability to securitize anything it deems a possible threat to its reign or the safety of the nation.

The performance-based legitimacy is at the core of the power of the CCP; hence it is essential for both the theorist of neoliberalism and the state-centred argument. The CCP operates with a vast amount of autonomy and a strong capacity to penetrate society, freeing itself from powerful social groups. The ability of the Party of freeing itself from the constraints of other political groups has been pinpointed as one of the reasons for the successful development of the nation-state (Yang, 2008). The autonomy of the Party allows it to operate free from group politics and ideological restrictions, making it capable upon adjusting and adopting new policies if previous ones failed (Hongxing & Zhao, 2015). It brings a new dimension to the table regarding the discussion of securitization vis-à-vis the Western context. The Party can set out long-term strategies within all domains, including the intelligence and technology sector.

### Leadership and Social Control

Performance legitimacy is a key pillar the Party is structured upon. For the Party, strong leadership and societal control are primary elements for creating stability. The ideology of the Party fundamentally believes in the concept of social engineering and transformability of the individual (Creemers, 2018) also founded within the concept of the Panopticon. The mindset has led to the birth of the SCS and an unprecedented level of surveillance. Transformability of the individual is essential in relation to the Panoptic theory and the stage of self-surveillance. Individuals are thus seen in a construct where they can be influenced by social engineering to portray the behaviour wished by the Party. The policymaking regarding the subjects of safety and national interest is, however, surrounded by secrecy (Ramzy & Buckley, 2019), making it harder to grasp the direction and ideas of the Party.

Social engineering is represented in the domain of surveillance and the SCS with President Xi Jinping being the embodiment of strong leadership. China's *'Chairman of Everything'* (Hernandez, 2017) has risen to the top rank of power back in November 2012 and is not intending on stepping down anytime soon. Xi has deviated from former policies by becoming a hardliner on the topic of security and especially Xinjiang province. Being the son of an early Communist leader that supported relaxing policies on ethnic minority groups had the analyst guessing that the President would follow a similar style of leadership (Ramzy & Buckley, 2019). Xi Jinping, nonetheless, deviates from his father trajectory and can be considered to be a hardliner on the subject of security. The fear of President Xi is based upon the ideological laxity and spineless leadership that caused the collapse of the Soviet Union, according to the words of the leader (Ramzy & Buckley, 2019). Challenges that arise such as dissidents and human rights lawyers are pinpointed as reasons upon increasing the security measures. The continuation of the Party and the safeguarding of *'The Chinese Dream*[3]*'* is the number one priority, and every method of surveillance that can contribute will be considered.

[3] The Chinese Dream is a signature ideology run by the CCP, it resembles the rejuvenation of the modern Chinese nation-state. It's a rhetorical theme used to build a narrative of rapid modernization and economic triumph (Ohlheiser, 2013; Wang, 2014).

Development is regarded as the key pillar for achieving lasting security, according to Xi Jinping, but development is not the answer for every problem within the Middle Kingdom (Ramzy & Buckley, 2019). Hence, we can distinguish a relationship set by the President between development and national security. The development of the nation-state is thus intertwined to security and the securitization of technological elements. A lack of ideology and leadership could potentially lead to the downfall of the Party, and therefore, it requires a strong implementation across the nation. A potential uprising in Xinjiang province, or Hong Kong, could cause spill over effects that would affect other parts of China and eventually taunt the image of strength of the CCP. The image of strength is maintained within Xinjiang province via a campaign of surveillance and intelligence instigated by the President himself. (Ramzy & Buckley, 2019). Technology plays an essential role in finding solutions for the challenges that the Party faces. Big Data, FRT and 5G technology are regularly tested within Xinjiang and if deemed to be effective rolled-out across other provinces in mainland China. Added to the technological advancements are so-called old-fashioned methods that have been in place since the era of Mao Zedong such as neighbourhood informants. The mixture of old-fashioned methods with technological surveillance is providing the CCP with a toolbox upon surveilling society and implementing its social management policies.

Xi can be identified as a hardliner on the topic of security; he has broken with policies of his predecessors to build a strong securitized state. Hu Jintao[4], his predecessor, believed that economic development would be a cure for ethnic discontent, which is interconnected to the longstanding party policy. Xi Jinping has stated that *"Xinjiang has proliferated and that the standard of living has consistently risen, but even so ethnic separatism and terrorist violence has still been on the rise"*, he then declared that *''It shows that economic development does not automatically bring lasting order and security"* (Ramzy, 2019). The policy shift from Hu Jintao to Xi Jinping is henceforth essential, economic development is no longer seen as the cure for every security complex.

### Xinjiang Province: Window into the Future

One of the regions that is surrounded by surveillance and secrecy is Xinjiang province, a resource-rich territory located in the West of China. Xinjiang is classified as a massive surveillance operation where China is monitoring, controlling and internalizing citizens. There are estimates that two to three million people disappeared into so-called *re-education camps* which has spurred Western outrage. Xinjiang has dominated Western media outlets due to the cracking down on the Uyghur population and the unparalleled methods of surveillance (Buckley & Mozur, 2019; Cockerell, 2019; Zand, 2018). Half of the inhabitants of Xinjiang are part of predominantly Muslim ethnic minority groups with the largest being the Uighurs. The Uighurs have their own cultural and religious beliefs and speak a Turkic language, identifying themselves closer with the neighbouring Stan countries than China. Residents in Xinjiang have, according to the State Council, a *"relatively weak sense of the rule of law, lack understanding of the law, and are vulnerable to instigation and intimidation by terrorist and extremist forces, resulting in criminal behaviour"* (State Council, 2019, p. 16). The CCP has suppressed the Muslim minorities in Xinjiang for decades and has imposed a stricter rule and crackdown after a surge of anti-government and anti-Chinese violence erupted in the late 2000s. The West is depicting the actions of the State as a campaign of religious repression, while the Party is broadcasting an image of *'unprecedented effort of de-*

[4] Hu Jintao served as the leader of the Communist Party from 2002 to November 2012. Mr. Jintao is known for his ideal of building a 'harmonious society' that would bridge the gap between poor and rich.

*radicalization'* via its media channels such as CGTN and Xinhua[5] (Guan, 2019). The white paper '*The Fight Against Terrorism and Extremism and Human Rights Protection in Xinjiang'* released by the State Council of China (2019) is trying to justify the angle of the Party while at the same time proving the effectiveness of the methods. In December 2019 the Party, voiced by the region's chairman Shohrat Zakir, even published the story that all trainees have *graduated* from the vocational education and training centres, as what they are called by the State. Beijing is momentarily trying to counter-balance the Western depiction of 'concentration camps' and 'religious repression' into a message of de-radicalization that is welcomed with open arms by a '*global coalition of human rights violators'* such as Russia and Saudi-Arabia (Faiz, 2019).

In November 2019, 400 pages of internal Chinese documents had leaked that have provided an insight into the crackdown of the ethnic minorities that are living within Xinjiang province. The party boss of the region, Chen Quanguo, has expanded the surveillance and internment camps with the documents providing details upon the internal speeches given by Party members such as Xi Jinping. According to the so-called China Cables documents, Xi Jinping gave the order to *"round up everyone who should be rounded up*" (Ramzy, 2019). The crackdown on dissidents is a return to the period of Mao Zedong's political crusade, in which the top-down pressure on local officials encouraged overreach. Local officials that have doubted the methods of usage in Xinjiang, assuming that it would slow down the economic growth and enlarge the ethnic tensions, have been purged during recent years leaving no room for criticism on Party policy. It has been affirmed that the pressure on officials in Xinjiang to detain Uighurs and prevent any possible violence is relentless. Methods of surveillance that are used within Xinjiang province will be further scrutinized in chapter eight, tools of mass surveillance. The leak of the classified governmental documents gives a peek into the operations manual of what the media portrays as a 'Orwellian system of mass surveillance' (Allen-Ebrahimian, 2019).

## China's Security Agencies

While Western security agencies are under constant pressure to analyse the right method of data collection, the Chinese have a carte blanche on responding in any manner they find reasonable. AI technology grants the intelligence agencies with increased methods for the monitoring of society. The increase of powerful technology within the domain of intelligence, however, raises concerns. A question raised by Greg Allen and Taniel Chan in *"Artificial Intelligence and National Security"* (2019) is how the rise of AI in the cyber domain will affect the power position of individuals that are operating and supervising the systems. The Party fears the emergence of influential individuals within the security domain, showcased by the fate of former security chief Zhou Yongkang. Zhou was the head of the modernisation of China's intelligence and security system with the position as Minister of Public security (2002-2007) and as chairman of the Central Political-Legal Affairs Commission (2007-2012).

Zhou Yongkang was charged with corruption in 2014 and consequently expelled from the Party. Yongkang was at the foundation of constructing the social management policy in a catch-all clause to ensure social stability. The article *"Strengthen and improve social*

[5] Xinhua News Agency is a Chinese state-run media organization founded in 1931. It operates under governmental control and its news reflects state policy and promotes state programs. It was among the first news agencies to use a AI-driven news presenter (Baraniuk, 2018).

*management – promote social stability and harmony"* in the People's Daily[6] (2006) constructed a foundation for a public security platform for surveillance, early warning and emergency relief (Velghe, 2019). The idea of Yongkang was used by the CCP and developed into one of the key pillars of the 12th five-year plan. The plan was published in March 2011 with a *"social management system for greater social harmony and the use of volunteers"* (12th Five-year plan, 2011). The position of individuals working within the intelligence sector is hence affected by the use of technology such as AI. A position of power can also be counter-productive for a person's career path and effectively be used against them.

Two of the most pressing threats for an authoritarian regime are a coup attempt and a revolution. The 'threat from within' is seen as the most pressing with roughly 60-70% of the authoritarian regimes falling via a coup (Svolik, 2009) hence President Xi is weaponizing the government against an end of an era. Under the current leadership, the aim is to weaken the overall strength of the Ministry of Public Security and its sister agencies, by showcasing this with the public humiliation of the head during the Hu Jintao area (Schwarck, 2018). Zhou Yongkang initially came under fire for interfering with other areas of government that were outside his department. The Central Political-Legal Commission that was headed by Yongkang was interfering for the sake of *"maintaining stability'* and the Party's internal equilibrium. The reason for creating an intended fragmentation between the security agencies can be founded within a theory by Sheena Greitens. It is arguing that autocratic governments want to be "coup proof" by promoting fragmentation among the security agencies, consequently interfering with the internal coordination that would be necessary for a coup (Greitens, 2016). A consequence is that security agencies are less capable of fighting public disorder. Hence, Greitens argues that if autocratic governments such as China improve the cooperation between security services, this will increase the cohesion and ability for internal security while it strengthens the ability of the combined forces to launch a successful coup. China has a history of suspicion towards its security organs, and this resulted in the competing between the Ministry of Public Security and State Security in areas of shared jurisdiction. The Ministry of Public Security is now seen as the powerhouse behind computerised surveillance and thus AI-driven domestic surveillance.

In short, the definition of national security has shifted within mainland China, granting the Party the opportunity to further securitise technological elements for the sake of social engineering. The performance legitimacy of the Party is intertwined with the state-centrist and neoliberal policies; finding an equilibrium is vital upon sustaining economic growth and social control. Technology is seen in this process as a tool of creating a safe environment for the prolongment of the Party. Xinjiang area and the China Cables has pushed the Party into a position of international embarrassment that it is trying to fix with an international informational campaign. Interconnected to state surveillance are the Ministry of Public Security and State Security that the Party needs to coordinate and balance to stay effective without tipping the scale towards too powerful. Points mentioned above are a selection of key-indicators that affect the decision making-process for internal security and surveillance. It gives a foundation upon understanding the policy of the Party towards security in the public domain.

[6] The People's Daily is the official newspaper of the Party. It is the largest domestic newspaper and provides information on Party policy and viewpoints (Yi, 2017).

## 5. Case Study: Mainland China

The case study consists of three components; policy on AI and FRT, domestic players and finally the implementation process with examples of modern-day surveillance. The information is guided towards first analyzing the direction and aim of the Party with the specific technologies. It is followed up by an introduction of the private parties that cooperate with the government into constructing the technologies necessary for social engineering. The last chapter will give examples of present day surveillance practices and a sneak peek into the future with the SCS. The first two chapters will answer a sub-question upon guiding the stream of information towards answering the research question.

### 5.1 Policy and State-centered ambition

China has made digitalization the leading engine to strengthen the Chinese nation-state and economy since the 18th Party Congress (Velghe, 2019). Beijing is aiming at becoming a leader within the technology sector to transform its economy from ‘Made in China’ to ‘Innovated in China’. Its economic growth is slowing down, and the shrinking workforce is adding pressure to the wages. It is essential for the Chinese economy and the Party to move to a growth model of innovation and increased productivity (Wei, Xie, Zhang, 2017). To move towards an innovation-based growth model, the Party needs to invest in advanced technologies. The investments made within the surveillance sector resulted in a new generation of Chinese start-ups within the AI and FRT domain (Mozur, 2018). Pillars within the innovation-led model are Big Data, FRT, AI, cloud computing and the Internet of Things (IoT). Aforementioned technologies can furthermore be used to improve the governing capacity (Arsène, 2016) creating dual-purpose and a potential win-win situation. Beijing needs to shift to an innovative economy to realize its dream upon joining the high-income club (Wei, Xie, Zhang, 2017) and for staying ahead of any potential social unrest.

In the 13th Five-year plan the Party constructed a list of innovations to improve the population management and governance models. Points of interest are a national database of basic population information, real-name registration, credit rating systems and an early crisis warning and intervention system (13th Five year-plan, 2016, p. 199). AI is going to occupy a central role with the points mentioned earlier, making it an industry of priority. Ministries that are closely cooperating within the domain of security with interest in AI are the Ministry of Public Security, associated by Western media with domestic intelligence, and the Ministry of State Security, assigned to overseas intelligence and counter-intelligence (Schwarck, 2018). The rise of new companies within the domain of FRT and AI in combination with the public parties, is helping the government to realize its future goals on social management and governance.

AI has been identified as a strategic opportunity to tackle societal and economic challenges. Governmental strategic plans with AI include *‘Made in China’, ‘Guiding Opinions of the State Council on Internet+’* and the *‘Next Generation Artificial Intelligence Development plans’.* The targets set by the Party coupled with the initiatives by local governments has catapulted the development of the domestic AI market (AI Development Report, 2018). On the other side is FRT, which is part of “Xue Liang” (or Sharp Eyes program), a campaign to improve the domestic surveillance capabilities for the power of the state. “Xue Liang” is a reference to a famous Chinese idiom, linked to the former leader of the nation-state Mao Zedong, referring to the eyes of the masses being *“as bright as snow”.* It is a conception that society and the people see everything and are all-seeing.

The idea behind “Xue Liang” was to report wrongdoings to the CCP, effectively making society safer by social control. The Sharp eyes program is perceived as one of the major drivers behind the spending on urban and rural surveillance systems (Dai, 2019b). The system is constructed with the notion that people will feel that they are always being watched, as envisioned by the Panopticon of Foucault. The fear of shaming is the essence of Xue Liang (SCMP[7], 2018b), with it being tested out at 50 places scattered across mainland China before being rolled out on a national level.

AI and FRT are both industries of great interest for the Chinese leadership, and both receive considerable sums of investment money to become the world leader. The trajectory for FRT is going as intended, with China holding a 46% share of the US $17.3 billion global video surveillance market in 2018 (SCMP, 2018b). China’s largest FRT firm is SenseTime, with a third of its overall business being contributed to the Chinese police (Schmitz, 2018). The customer share of the police is showcasing the importance of the state as being a significant driver for innovation-led surveillance systems. Further information regarding domestic companies such as SenseTime can be found in chapter 5.2.

The AI and FRT companies within mainland China are achieving high growth rates, thus due to the high demand of the government. FRT technology in its current state within mainland China is mainly used for state-surveillance activity (Wright, 2018) although it is, of course, not exclusively used by state actors. FRT technology is continuously expanding into new territories such as security lock systems for doors, cab-hailing and commercial venues. AI and FRT are thus both dual-use technology, for governmental, civilian and military purposes.

The designated proving ground for China’s expanding surveillance system is Xinjiang, the Western province of China. Human informants, surveillance equipment and security checkpoints are an inevitable part of life for citizens in Xinjiang, especially for the Uighur. Xinjiang is becoming “*a real-life laboratory for surveillance”* with elements such as smartphone scanners, advanced FRT, voice analysis and GPS tracking devices for all vehicles (Wright, 2018, p. 1). Surveillance technologies are widely tested within Xinjiang province, and if deemed good enough, implemented in other parts of the nation-state, earning it the name of China’s surveillance proving ground (Phillips, 2018). It is providing the Party with its exclusive proving ground for new technology.

Chinese firms that are leaders within the domain of technology such as SenseTime and Megvii are in part growing in high rates due to the governmental demand, but in the future, the same tools could easily be exported to other nation-states with similar intentions. Liberal democracies are already large-scale users of AI surveillance technology (Feldstein, 2019), although this not directly mean these democracies are abusing the systems in place. The quality of governance is the determining factor if the available surveillance systems will be abused. Autocratic governments, such as China, Russia and Saudi Arabia, exploit the use of surveillance technology for mass surveillance purposes, showcasing that governments in autocratic and semi-autocratic nation-states are more prone upon abusing the technologies at hand compared to liberal democracies. Chinese firms are , nonetheless, seeking to expand their market as William Nee explained, *“Chinese enterprises want to grow their business and sell their technology to other authoritarian nation-states, or even democracies, if they are*

[7] The South China Morning Post (SCMP) is a Hong Kong based English-language newspaper owned by Alibaba Group. Alibaba Group has close ties with the State, chairman Jack Ma is furthermore a member of the Communist Party.

*looking for the same tools"* (Phillips, 2018). The possible construction of a Panoptic could hence be implemented in other nation-states if they wished to do so. Chinese firms are a significant driver behind AI and FRT surveillance worldwide with no code of conduct for not dealing with other nation-states based on principles known to the Western hemisphere. The fast-growing and expanding market of surveillance is hence a warning sign that futuristic surveillance is far from exclusive to the Chinese nation-state. The policies in place are set to make China the world market leader on AI and FRT systems which it then could utilize on the international market.

### Artificial Intelligence

AI technology enables computers to recognize patterns of for instance faces and voices and to make sense of large quantities of data so that it can be processed effectively (Schermer, 2009, p. 65). The technology can be applied to a wide arrange of fields such as public security, predictive policing and social governance activities, as China likes to frame it (CAICT, 2019). AI is a domain within the security market that is still under massive development. Its identified by the government as a key pillar for challenges such as sustainable economic development, economic transformation, social management and the pressure of an ageing population (AI Development Report, 2018). The push for AI has resulted in the fact that China is now the global leader on scientific AI papers and patents.

The current policy regarding AI is focused on six categories selected by the Party, namely: 'Made in China", innovation-driven development, IoT, Internet+, Big Data, and technological R&D (AI Development Report, 2018; Robles, 2018). We can distinguish at the core of the policy *'Made in China 2025'*, serving as the guideline for local governments. Currently, the machine learning algorithms are providing the next step within the domain of face recognition, speech recognition and other security-focused capabilities. It can furthermore replace the human factor within particular domains of the surveillance branch, effectively automating the process. This will result in the fact that computers will ultimately be the judge in the process, determining the punishment and consequences.

Most equipment currently in use is ,however, defined as 'non-intelligent". Shen Xinyang, chief technology officer of Eyecool, states that *"AI for public security is still a very insignificant portion of the whole market"* (Mozur, 2018). The company of Mr Xinyang has surveillance systems set up at more than 20 domestic airports and train stations, uploading a total of two million facial images every day to the big-data police system Skynet. The Chinese national database, interconnected to Skynet, holds an amount of 20 to 30 million suspects, including drug traffickers, potential terrorist and political activist. The technology executive, working closely with the Chinese government released this information with the disclaimer that today's FRT is not complex enough yet to work real-time with a database of that scale (Mozur, 2018). The idea is to create an overarching technological network powered by AI technology, while it is currently run by teams that go through the vast quantities of data and photos manually. One of the examples that shows the implementation capability for AI technology is the crosswalk-shaming in, for instance, Xiangyang. People that have jaywalked at the crossroad would be displayed upon large digital screens set-up at the intersection. The current process is that Chinese police officers go through the images captured by the FRT and find a match with a person's identity. As a result, pictures displayed are far from recent with a delay up to 5-6 days. Using AI with future capabilities would be able to determine the identity of the jaywalker and display his information on the screen within minutes.
The switch from Chinese police officers to AI will shift the notion from ex-post to real-time, changing the surveillance game.

The scenario mentioned above showcases that the person operating the system has direct power of the subject being surveilled, facilitating an idea of direct discipline (Schermer, 2009). The introduction of capable AI would ultimately cut out the human factor so that the system could operate autonomously. The systems will eventually be the judge, deciding upon the fine and consequences. It would also shift the usage and notion from surveillance from ex-post to real-time. Information currently collected and used by the surveillance system is ex-post. Since the digital and physical world will be more intertwined within the near future, surveillance operators – and algorithms – will have the ability to trigger events in real-time. It will change surveillance from an *‘architecture of observation’* to an *‘architecture of control’* (Schermer, 2009, p. 68). The shift to an architecture of control will enlarge the feeling of being in a Panoptic society due to direct punishment. Citizens are directly corrected, giving the impression that citizens are more the subject of centralized discipline (Lyon, 1994).

### FRT: New weapon of choice

Surveillance cameras (also known by CCTV, Closed-Circuit Television) and facial recognition technology are increasingly used around the globe for the monitoring of public and private spaces with advanced face-detection equipment. The widespread use is ranging from traffic control to oversight of urban environments, making it an inescapable part of modern-day China. Facial recognition systems are effectively used with CCTV to make use of computerized pattern-matching technology to identify the faces of people automatically. The FRT can then be followed up by AI-controlled databases that monitor and track citizens. As a Chinese citizen, especially of a tier-one or tier-two city[8] , you are under constant surveillance by CCTV’s, highlighted by the capital Beijing. Media outlets reported in 2015 that the capital is *‘one hundred per cent covered’* by surveillance cameras, with the city’s police department stating that *‘every corner’* is covered by the municipal surveillance system (The Guardian, 2019; Radio Free Asia, 2015). There is, however, a debate regarding the effectiveness of CCTV in the prevention of crime, and the results are inconclusive at best according to Privacy International.

The technology does raise questions regarding the privacy of citizens in public due to their identity being exposed at every moment. Citizens are hence visible at every moment, mirroring the feeling of walking within a Panopticon. Beijing especially, with its one hundred per cent CCTV coverage, creates a sense of being watched by unseen eyes constructing a tool of control for the Party. The feeling of being seen while the officials are invisible can be exploited upon creating a Panoptic feeling. There is nowhere to hide for the citizens *“obedience is the prisoner’s only rational option”* (Lyon, 1994, p. 59). CCTV cameras with FRT technology are hence the embodiment of physical proof that citizens are being watched.

The use of FRT is in line with the fading anonymity in mainland China. In the *offline* world, citizens are getting tracked by CCTV cameras while in the online world they are bounded by comprehensive real-name registration rules, adequately disclosing the identity of any citizen online (Lee & Liu, 2016). It is exposing the efforts of the Party upon eliminating cyberspace anonymity. At the core of the policies is social stability, which, via the free flow of information, enabled by digital platforms, could affect the process. The state wants to control

[8] Chinese cities are categorized according to tiers, with the most common system being into four respective tiers. Most factors to determine the tier fall within three macroeconomic categories: GDP, population and politics (SCMP, 2016).

the flows of information digitally by imposing rules on internet service providers (ISP) under the twin-principle of a harmonious society and social responsibility (Lee & Liu, 2016).

There has been extensive coverage over the use of facial recognition technology within the media over the last couple of years. The increased media coverage is in part due to the enhanced capabilities of algorithms, a large number of applications that use it and lower barriers for development within the algorithm domain (NIST, 2019). The use of FRT is thus intertwined with the developments made within the algorithms domain. AI and FRT are hence two components that work hand-in-hand for the surveillance sector. The face of the public is used in the process for the Party to increase its control and its social engineering capabilities (Mollman, 2019). China's new weapon of choice is thus the face of its citizen.

### Privacy

The take-off of FRT technology has raised concerns about the privacy of citizens. The technological advancements give the security state a greater playing area; hence the privacy and civil rights of Chinese citizens are coming under additional pressure. Data collection on individuals and groups is more restricted within the Western hemisphere with rules regarding what kind of data can be stored, for how long and by who. There isn't the same set of rules in place within the Middle Kingdom. The endless amount of personal data that is collected in combination with machine learning surveillance platforms is creating an environment where the Party can effectively monitor every public space with minimal need for a human touch. It is a free pass for massive data collection that can be translated into knowledge. Knowledge and power are dynamics that reinforce each other in a circular process (Foucault, 1977) benefiting the position of the Party vis-à-vis the ruled.

Beijing is deeming technological advancements necessary to safeguard the community and fight eruptions of violence. Still, the line between overusing the system for other means of control is thin. With the right set of elements in place, the government has the possibility of setting up a large scale police state that could be exported to other nation-states if China wishes to do so. Lao Dongyan, a law professor at Tsinghua University, noted that *"there needs to be consent before obtaining people's data"* according to Chinese law and regulation. However, in reality, facial recognition technologies are used without the public rarely knowing about it (Xie, 2019). The collection and storage by the state hence doesn't follow the legal requirements, added by the fact that there is no individual law regulating the use of facial recognition technologies. The state is furthermore not the only player within the system that collects facial data; a gross amount of Chinese apps also collects facial data without the consent of the user via an agreement. Even if there was a set of legislation in place for the restriction of unauthorized collection of facial data, the government would still find ways to evade the legislation for obtaining personal information, according to legal experts. The implementation of FRT and AI has a high impact on the privacy of Chinese citizens that was already under pressure. *"Once these technologies are used on a large scale, we have nowhere to hide"* according to Chinese based lawyer Wang Xinrui (Xie, 2019), making Beijing just the starting point of full oversight. The use of FRT on a large scale will rapidly eradicate the feeling of being unknown in public spaces, setting the scene for a feeling of permanent surveillance.

## Big Intelligence System

Closely connected with surveillance is the system of intelligence-led policing, what is at the core of the big intelligence system of China. Zhang Xinfeng, former Public Security Vice Minister, announced the big intelligence system at the 2008 Meeting of the National Public Security Bureau Chiefs in Nanjing (Schwarck, 2018). Informatization - computerization - was indicated as one of the three key priorities for the Ministry. The aim is to establish a big intelligence system that is going to promote the sharing of intelligence among the security forces. The slogan that captures the idea is *“all police collect, all police use, all police share”* (Schwarck, 2018). A multidimensional IT-based system is thus constructed for crime prevention and control, allowing the introduction of more technology-based appliances in community-level police work (13th Five year-plan, 2016, p. 204). The construction of a public security platform is furthermore found within information policy reports, such as the National Plan for the Distribution of IoT Development (2013). The aforementioned paper constructs a linkage between the surveillance platforms and social management as imagined by the Party. President Xi Jinping highlighted the concept in September 2017 when he called for *“a more systematic and innovative method of social governance, stressing the need to improve the capability to predict and prevent security risks”* (Zhang, 2017). Intelligence-led policing is at the forefront of fighting domestic crime and visible in, for instance, Xinjiang province.

The most significant change, however, will be for the foreseeable future. The construction of a big intelligence system makes way for ‘data-hungry AI platforms’ that would allow the police force to automate a significant amount of work. Systems of public security are increasingly more capable of analysing data without the need for a human touch. Bulk-Data collection such as video footage, photos and voice recordings can eventually be fully automated, cutting off the human factor what eventually streamlines and speeds up the process (Schwarck, 2018). In the study *“Artificial Intelligence and National Security”* (2019) by Greg Allen and Taniel Chan the authors state that there is a *“plausible winner-takes-all”* aspect to the combined future of AI and Surveillance. It will be tougher for potential criminals and dissidents to organize themselves and spread their ideas without leaving (digital) footprints that would be traceable for the Party. The eradication of offline and online anonymity will increase the power position of the watchmen to surveil citizens, enlarging the feeling of living within a Panopticon. It is an illustrative example to showcase that citizens are on the receiving end of an asymmetrical surveillance relationship, being objectified to a symbol of information (McMullan, 2015).

### The winner takes it all

AI is allowing the state to shift the domain of surveillance, in time, from an architecture of observation to control. The switch from non-intelligent equipment to intelligent surveillance systems will allow the watchmen to react in real-time instead of ex-post, making citizens aware and responsible for their actions within minutes. The ability to apply direct punishment will result in a greater feeling of living within a Panoptic state. The *who* element enforcing the direct discipline will consequently switch from a human being to AI-based technology. CCTV, coupled with FRT, will eradicate the possibility of being anonymously at public places in the near future. In the process, the public is starting to lose its anonymity due to a lack of legislation for the protection of privacy and civil rights of Chinese citizens. FRT will be used within the process of social engineering to utilize the face of the public as the new weapon of choice.

The sub-question of *“How technological advancements in surveillance change/affect the forms of control available to the government?”* can thus be answered via the information mentioned above. The development in AI and FRT will, in time, grant the Party with enhanced possibilities to uphold the social unity in society. The process of surveillance can be partly-automated, bulk-data will be analysed and interpreted by AI driven-systems that can eventually autonomously act as a judge. There is a *“plausible winner-takes-all”* clause to the combined future of AI, FRT and surveillance for the Party. FRT, in combination with AI, will be used to remind citizens they are being watched, reminding them to practice self-discipline and uphold their social responsibilities (13th Five year-plan, 2016, p. 200). Consequently, we can distinguish the factor that the Party is exploiting the use of technological innovations to bolster the surveillance and social management process. That the public will lose its anonymity in the process is seen as collateral damage.

## 5.2 Domestic security market

China is an instigator and driver for the global AI surveillance market. Chinese enterprises such as Dahua, Hikvision, SenseTime and Huawei supply sixty-three other nation-states with AI-based surveillance technology (Feldstein, 2019). Huawei is the undisputed king within the global domain of AI surveillance with customers in at least fifty other nation-states, leaving the closest non-Chinese firm NEC Corporation far behind with only fourteen. Chinese companies furthermore greatly benefit from the Belt and Road Initiative (BRI[9]) that is supplying countries with soft loans so that they can buy Chinese surveillance equipment. The subsidized purchase of repressive technology is then distributed to nation-states such as Uganda, Laos and Kenya (Feldstein, 2019). AI surveillance is then regularly used as a tool of repression, which is mainly associated with foremost autocratic and semi-autocratic nation-states such as Russia and Saudi-Arabia. Due to the global impact of Chinese firms, there is a short analysis of their domestic-and global position. Is there a singular actor within society that is or will be all-seeing or is every aspect of the surveillance system fragmented?

### Don't be Evil

China has a set of world-leading enterprises that work within the domain of surveillance, one of these is SenseTime, China’s largest AI company. Surveillance makes up one-third of the business of SenseTime with local governmental clients spread across the Middle Kingdom. Other customers include financial institutions, mobile operators and the smartphone industry. The widespread use of AI technology and the amount of demands from customers, has made SenseTime China’s largest unicorn, with a valuation of upwards 3 billion US dollars (Schmitz, 2018). The second-largest Chinese AI company is Megvii, that is at the top of the innovation chain due to governmental demand, according to the vice president Xie Yinan. The vice president has stated that *“The Chinese government is pushing AI technology from the top of the governmental organ, if Chinese companies want to make it happen they won’t have big obstacles”* (Schmitz, 2018). It is highlighting the differences between the Chinese and, as he explains, the US market. AI has turned into a race between Beijing and Washington. The Pentagon is investing large sums of money into outpacing China on the military AI side. US Defense Secretary Mark Esper explained that *“Whichever nation harnesses AI first will have a decisive advantage on the battlefield for many, many years”* (Gertz, 2019; Alper, 2020) — outlining the importance and stakes upon becoming the world leader in AI. For the Chinese market, we can distinguish SenseTime as the predominant FRT and AI company, selling to both government and private corporations.

The three largest surveillance cameras manufacturers in China are Zhejiang Uniview, Hangzhou Hikvision Digital Technology and Dahua Technology. All of the enterprises are located in Hangzhou’s Binjiang district. It’s a Chinese phenomenon that the same manufactures can be found within the same city, also called one-industry towns. The companies, as mentioned above have a 30% share of the worldwide video surveillance camera market, with Dahua and Hikvision together having more than half of the Chinese video surveillance market (Dai, 2019b). The fundamental reason for the Chinese development, according to Hikvision spokeswomen, is *“the low police-civilian ratio based on the large population in China, and the challenging situation for public security management”* (Dai, 2019a). Pinpointing that the capacity of the Chinese police force is not up to par with the size of the population, hence requiring technological advancements to even the playing field.

[9] The Belt and Road Initiative is a global Chinese development strategy that was announced in 2013. The aim is to strengthen hard and soft infrastructure and cultural ties. The initiative touches upon 138 nation-states and 4.6 billion people (OECD, 2018; China Power, 2017).

China is witnessing a rise in the video surveillance market by 14.7%, compared to the world average of 5.5% according to HIS Markit. The increase in equipment correlates with the increased public and private demand, with domestic projects such as China's Smart-City concept. The implementation of AI furthermore pushes the sector and its possibilities forward, generating more demand. Public demand is seen as the main driver and cornerstone of the development, Ren Tianlei, an engineer at Dahua, reaffirmed that the police contracts are a significant driver for domestic demand (Dai, 2019a). What differentiates the public demand from the private is the job at hand. The public domain is identified as the most complex to provide solutions for; consequently, it requires the most time to deliver tailor-made solutions.

A rather new domain of interest is AI voice recognition. There is a massive 55 billion USD voice recognition industry with AI-based software dominating the field (Ali, 2019). The largest party within China is iFlytek, which is producing approximately 80% of the domestic speech recognition technology (Human Rights Watch, 2017b). iFlytek was founded in 1999 and is producing software to identify a target's voice in phone conversations along with the ability for the AI to digitalize it into a readable format. The national champion in voice recognition is collaborating with the Ministry of Public Security upon developing a national database of voice patterns what will be further scrutinized in the next chapter.

### Huawei

Huawei is a giant of the Chinese tech industry. It is the world's largest provider of telecommunications equipment, the leader within the domain of 5G technology and a worldwide distributor of surveillance technology (Almond, 2018). The enterprise is known within the Western hemisphere partly due to the generated fear that the technology has so-called backdoors that could impose a security threat. The United States has reasoned that Huawei is in no position to say no to request that comes from the government, making it susceptible to spying activity (Keane, 2019; Doffman, 2019b). Further accusations are pointed towards Xinjiang. Huawei has long denied its connection with the controversial surveillance in Xinjiang, claiming it was only present via third-parties (Doffman, 2019a). While the China Cables, published by the International Consortium of Investigative Journalist, revealed the ecosystems of the camps, the follow-up report by the Australian Strategic Policy Institute uncovered the main technological providers. Huawei is identified as the main actor, and *"Huawei's work in Xinjiang is extensive and includes working directly with the Chinese Government's public security bureaus in the region"* (Cave, Ryan, Xiuzhong Xu, 2019). Other companies that came under scrutiny are ByteDance, creator of the app TikTok. The enterprise has, according to the report, "*deployed a public security and internet social governance model"* under close cooperation with government ministries of Publicity and the Public Security's press (Cave, Ryan, Xiuzhong Xu, 2019).

The technology sold by SenseTime, Megvii and Huawei are used for the Chinese "Sharp eyes" program, a plan by the Chinese government to integrate existing security cameras into a nationwide surveillance and data-sharing program. Another usage is for China's Smart City program, it is combining personal data with AI so that cities can eventually *"run more efficiently"* according to a government official (Schmitz, 2018). The technology hence gives an incentive to the CCP to support start-ups and other technological companies that are working on the required technology. The technological advancements of this age gives the government of China more possibilities on fighting crime, keeping track of citizens and creating a safe environment. The backdrop, however, is the privacy concerns that are growing within mainland China. Vice President of Megvii conceded that a lot of the technology they provide to the government has severe limitations. *“We just provide the government with the technology, and they do their job with it”* according to Xie (Schmitz, 2018). Hence, the vice president of Megvii is not taking responsibility for what the Chinese state is intending to do with the technology in a later stage. The end goal of Megvii is however similar to that of Google *“Don’t be evil”*, insisting that the Chinese government is ultimately using AI and FRT for the greater good, keeping cities safe, stopping crime and protecting its citizens. The technology is constructed to empower humans, not to control them is the motivation of Megvii, and *“if a government is using it to control locals, we’d think twice about doing business with them”* (Schmitz, 2018). The words of the vice president of Megvii and other domestic enterprises such as Huawei need to be taken into account, but the role of the government within mainland China is a force of reckoning.

### Race for Supremacy

China is in a race with the US on becoming the global leader in the AI domain. The dual-use technology is embedded within the blueprint of ‘Made in China 2025’, and its destructive military capabilities make it a top priority for both Beijing and Washington. Chinese tech companies are already trying to shape the UN standards for innovative technology on facial recognition and video monitoring/surveillance, according to a leaked Financial Times report (Jing, 2019). Telecommunications equipment maker ZTE, Dahua Technology and China Telecom are all proposing international standards within the domain of vehicle surveillance, video monitoring and facial recognition standards. The aim of Beijing is that implemented standards are ratified as policies by African nation-states, that are supplied with Chinese technology for surveillance under the BRI. Beijing is searching to increase its grip on the global AI market while its already providing 63 nation-states with AI-based surveillance technology (Jing, 2019). It is exemplifying the international reach of Chinese tech companies and the influence of standards set by Beijing. Criteria’s and international standards that Beijing is aiming for include the storage and creation of a database for detected facial features such as skin colour, birthmarks, scars, race and other demographics features picked up by surveillance cameras. The storage and usage of captured – biometric – data is yet another privacy concern for citizens worldwide. The increased deployment of biometric systems is moving towards the construction of a biometric passport of citizens (Griffith, 2019b) effectively being a whole new level of privacy infringement. Beijing is far from being privacy-aware, especially compared to Western nation-states, but it is creating a unique position where it is not only failing to protect privacy but is also actively invading it.

### Fragmentation

The second sub-question focused on the domestic market of surveillance and the Chinese strategy for the implementation and usage of AI and FRT. Leaks of the China Cables and follow up reports have showcased the extensive build-up of surveillance programs with the close cooperation of Chinese firms. Dahua and surveillance enterprises SenseTime, Megvii and Yitu are all involved with the ’re-education’ camps and its connected technology. Huawei, due to the release of recent reports, can be added to this extensive list. There is no deniability towards the controversial cooperation between Chinese enterprises and the government on sensitive topics, Western suspicion towards Chinese enterprises is far from being groundless and pinpoints a sensitive point for future expansion into the Western hemisphere.

Due to the multitude of actors involved and the fragmentation along with the various programs the concept of one unitary actor that can be defined as the ‘’all-seeing eye’’ is flawed. Commercial and public actors all contribute with pieces towards the creation of a Panoptic feeling. The so-called Big Brother factor connected to the Panopticon of a singular all-seeing eye is therefore inaccurate. Instead, there is a multitude of commercial and public players within the surveillance domain that can create a sense of constant monitoring. There is close cooperation between the state and Chinese firms upon constructing modern AI-based surveillance equipment, necessary for the social control outlined by the Party. The absence of a central all-seeing eye is a deviation from George Orwell’s Ninety Eighty-Four and the central guarding tower found in the Panopticon. There is a nonetheless a point of discussion regarding the impact it has for mainland Chinese citizens. How does one create a distinction between the presence of an all-seeing eye or the feeling of one? A vast amount of contemporary surveillance is also shifting into the realm of invisibility, making it harder for citizens to sense the presence of Big Brother. The offline world with CCTV’s is, therefore still a physical reminder of the Panoptic gaze. Within the virtual domain of the internet, there is no looming eye starring down, citizens are, however, aware that their actions are being monitored. The ever-increasing amount of digitalization can hence provide a greater sense of uncertainty, forcing people to simply comply because you never know who is watching (Lyon, 1994).

## 5.3 Tools of Mass Surveillance

China is spending a considerable amount of funds on fuelling the research within the domains of surveillance technology. The essence of surveillance, according to Foucault, is to accumulate information and have supervision over the subordinates (Schermer, 2009), supporting the Party with its quest for social control and management. The capabilities are extended beyond the identification of the face of a person towards the clothing they wear, the way they walk and how their voice sounds. The expanding list of surveillance capabilities, in turn, grants the Party with more opportunities to identify and monitor people. Governmental funding eventually results in new experimental gadgets such as facial-recognition glasses and biometric databases of, for instance, voice patterns.

China's top economic planner, the National Development and Reform Commission, is seen as one of the instigators of the development in the surveillance industry. In 2015 the Commission stated that China needs to set up *"a national, omnipresent, fully networked, always working and fully controllable video surveillance network by 2020"* (Qiang, 2019). They are furthermore stipulating that there should be no *"blind spots"* at complicated and densely populated areas. This section of the paper will analyse the advancements made to realise abovementioned goals from an AI/FRT perspective.

### Biometric adoption

Biometrics technology is becoming a part of the daily life of many citizens around the globe. It is integrated within smartphones and eliminates the need to remember a password or Pin. Facial recognition and fingerprints readers are examples of biometric authentication for payments that the world is heading into. It is no surprise that China has been ranked as the world's number one abuser of invasive and extensive use of biometric data (Zhang, 2019b). The study by Comparitech also found out that there is no specific law that is protecting the biometric data of citizens, making them vulnerable for the exploitation of collected information. The connected Panoptic element is thus that the face and voice of the public is becoming weaponized, making day to day activities impossible without being recognized.

Besides establishing a national database with the faces of the public, the government is also collecting voice patterns of individuals. The idea is similar to Skynet and aimed towards building a national database of voice biometrics. There is a collaboration between the Ministry of Public Security and iFlytek, the leading Chinese company on speech recognition technology, to automatically recognize the voices in phone conversations (Human Rights Watch, 2017b). The domain of biometrics is of increased interest for the government to create a so-called 'multi-modal' biometric portrait of its citizens. It is interconnecting the voice and facial features to the police database, which has personal information such as the identification number and home address. The database of voices, however, contains an insignificant amount compared to the national facial police database. The government has gathered 70.000 voice patterns in the province of Anhui, that is indicated as one of the main pilot areas (Ali, 2019). In contrast, the national facial database contains over one billion registered faces. Voice patterns are also collected without consent, so citizens most likely will not even now the government has this type of a biometric collection.

Beijing is taking it even one step further with the construction of a DNA database. The Ministry of Public Security has started building a "Forensic Science DNA Database System" back in the early 2000s as part of the Golden Shield Project (Fan, Khan, Lin, 2017; Human Rights Watch, 2017a). Police officers are compelling ordinary citizens to have their blood drawn, especially in the Xinjiang area. There is no minimum threshold of being, for instance, the suspect of a crime to have your blood taken, Beijing does have specific target groups such as migrant workers, Uyghur Muslims and dissidents. In the current state, it is the largest DNA database in the world, with more than 54 million individuals registered (Fan, Khan, Lin, 2017). The gathering of biometrics is part of the broader ambition of the police to collect so-called 'basic-information'. China Director Sophie Richardson has stated that *"China is moving its Orwellian system to the genetic level"* (Human Rights Watch, 2017a) and without regulations regarding the collection of DNA outside of criminal investigations the public has no choice then to cooperate.

### Power of FRT

The power of FRT is displayed within the BBC video *"In Your Face: China's All-Seeing State"* (2018), it's an experiment that showcased how long it would take for the police to determine the whereabouts of BBC reporter John Sudworth in Guiyang. The city is located in Guizhou, which is one of China's least developed provinces. Via the use of a central database of images, the Guiyang police could identify and detain John Sudworth in the city centre at the 7-minute marker. The experiment entirely relied on FRT, with a central database with of images of every citizen that lives within Guiyang - 4.5 million residents - and facial recognition cameras placed across the city. Powerfully showcasing that citizens are no longer anonymous and that the face of the public is the new weapon of the Party. AI and FRT are hence enabling the police to directly hold citizens accountable for their actions. A faceless crowd is no longer possible with algorithms and FRT taking over the public domain. The technology is opening a box of opportunities for the Party to utilise the full potential of the technology for the process of social engineering.

FRT is furthermore increasingly used by schools and universities. Facial recognition is used to scan the faces of students upon analysing their behaviour and presence, as what is happening in a high school in Hangzhou (Wright, 2018). The faces of students are analysed every 30 seconds to be then classified on a scale of happy, angry, fearful, confused and tired. The so-called intelligent classroom behaviour management system is besides analysing the student's emotional state, also recording the writing, reading, or possibly sleeping at the desk. Hence, it also records if a student is present. ID cards are also replaced by FRT technology, allowing students to pay at the canteen and library with biometric payment methods (Chan, 2018). The simplification of payment will be at the cost of the privacy and anonymity of students. In fact, it is instilling a sense of permanent gaze by a *watchman* early on in the life of Chinese citizens. Even within the classroom, students are soon not able to escape the CCTV cameras.

Another insight into a Panoptic tool was given in Zhengzhou to a journalist with the facial recognition glasses, described as *"one of the more dystopian tools of China's burgeoning surveillance-industrial complex"* by the New York Times (Mozur, 2018). It's essentially a camera mounted to a pair of sunglasses that is connected via a wire to a minicomputer. The cam checks the images it records against a database of faces, essentially being a moving version of a CCTV camera with facial recognition capabilities. This form of hybrid reality was showcased in the novel Halting State by Charles Stross (2007), adding a layer of information projected on top of the physical world, which helps the police with their duty. Mixing the physical world with an added layer of information is named 'CopSpace', that could be intertwined with intelligence-led policing and eventually predictive-policing. It enforces the feeling for citizens that even beyond the sight of CCTV police are still able to retrieve their data, eliminating the chance of being anonymous.

Mr Shan, a Zhengzhou railway station deputy police chief, also recalls a case the glasses were used as a tool to extract information. A heroin smuggler got apprehended, and the police told the criminal that the lenses would provide all the information they need if he wouldn’t talk, *“because he was afraid of being found out by the advanced technology he confessed”* (Mozur, 2018). Exemplifying that even without fully functioning or providing the right information, the technology can instil fear within citizens. The fear of being identified and detected can thus be used as a tool of persuasion and repression. That same fear is used to reach and maintain the disciplinary threshold of the Panopticon. The fear for the technology in combination with the physical presence will induce a state of permanent visibility leading to the element of self-surveillance. FRT in the shape of facial recognition glasses and surveillance cameras are physical elements upon reminding the citizens that the presence of the all-seeing state is permanent. The uncertainty upon entering a public place with or without surveillance equipment will instil a state of mind of self-surveillance. The approach taken doesn’t require the state to have full coverage of public spaces, as in Beijing, to be effective. It is instilling a state of mind that is similar to that of the Panopticon the Party is aiming for.

A recent change, of late 2019 that was introduced is the compulsory face scans for new phone contracts. The Ministry of Industry and Information Technology announced the rule to *“safeguard the legitimate rights and interest of citizens online”* (Martin, 2019). Telecom operators are now forced to collect face scans before registering new users of phone contracts (Xie, 2019). The telecommunications industry is dominated by three state-run enterprises: China Mobile, China Unicom and China Telecom, making it easier for the Party to implement and oversee the market. It is an upgrade from the old system that required a copy of the identity card — in the event an ID card would be stolen criminals would hypothetically be able to register new phone contracts. It is a protective measurement by the government to protect citizens from possible phone scams while at the same time, it is strengthening the surveillance state. The real-name registration rules of the internet and the facial-requirements for a mobile phone service contract are examples of the fading – digital – anonymity within mainland China, making everybody accountable no matter where and how their actions take place. The Party showcases via the use of facial recognition requirement its capability to securitise the process upon getting a mobile phone contract. The unauthorised registration capability and the aftereffect of possible criminality triggered the government to install a biometric security measure. The unauthorised registration possibility was hence identified as a ‘threat’ while the government soon will have access to phone numbers and the corresponding facial identity, making it easier for future police and intelligence work to identify a caller.

### Innovative drones

FRT is taking to new heights when talking about the newly deployed hi-tech robotic dove. Although the general idea of a robotic bird with surveillance technology sounds far-fetched, it has become a reality within mainland China. Both governmental and military agencies have deployed the hi-tech drone in recent years, including in the autonomous region of Xinjiang (Chen, 2018). The drone is constructed to mimic the action of a bird, thus to turn and dive to give the illusion that an actual bird is flying over instead of a hi-tech drone with surveillance capabilities. The concept of the drone has shifted dramatically by mimicking already 90% of the movements of a real dove, replacing regularly fixed rotor blades. The drones are useful beyond the realm of public surveillance, with the ability to fool the most sensitive radar systems giving it military capabilities. The integrated civilian and military use gives it a dual-purpose, a policy set out by the government to ensure the development and appropriate sharing of resources between the military and domestic corporations (13th Five year-plan, 2016, p. 214). The drones are still in the development process, but with the advancements made within the AI domain, the drone has dystopian possibilities for future surveillance. The drone, with the latest AI and FRT technology, gives a new dimension to the monitoring of citizens without their awareness. They are allowing the government to monitor areas with rough terrain or rural and remote areas, hence spreading the capabilities of surveillance beyond the CCTV scope. The increased capability of observation produces new knowledge for the Party which in turn can be translated to power, a fundamental characteristic of the Panopticon. Fundamentally *"there is no power relation without the correlative constitution of a field of knowledge"* (Foucault, 1977, p. 27). As the tools of surveillance increase the incoming amount of data can be translated to knowledge, which in turn grants the Party power.

### The Shame Game

The government is resorting to public naming and shaming to enforce the rule of law and the implementation, enforcement and compliance with it (Creemers, 2018). It is part of a policy initiated by Xi Jinping against tax fraud, debtors and widespread corruption. It makes it increasingly harder for discredited individuals that are registered in a regional or national database to move freely. Debt evasion is seen as a chronic problem of the Chinese society and the government is resorting to new measurements to tackle the problem.

As previously mentioned in the last chapter are an increasing amount of cities adopting facial recognition systems at crosswalks to name and shame jaywalkers. AI in time will cut out the human factor so that the system could operate autonomously. The systems will eventually be the judge, deciding upon the fine and consequences and shifting the notion from ex-post to real-time. Eventually, it will bolster the feeling of living within a Panopticon.

Guan Yue, a spokeswomen, said that *"people will gossip about the people they will see on the screen, what is too embarrassing for people to take"* (Mozur, 2018). Creating a social mechanism that would behold people from, in this case, jaywalking. It is a method of social interaction that the authorities are increasingly turning to, public naming and shaming also known as 'laolai[10]'(Hornby, 2019; Xiao & Robertson, 2019). It is capturing a dystopian idea of using technology to shame people while also invading their privacy. Another way it was applied was in Zhejiang province, before a movie would start in a cinema the people would see a 30-second clip, accompanied with dramatic music, that displays 60 people that owe money to the State (Xiao & Robertson, 2019). So-called cinema shaming is seen as an effective strategy to shame people that default on payments on court-ordered fines. The images are accompanied by a message that there is zero-tolerance towards people who do not pay fines and that they have the risk of being denied entrance to trains, aeroplanes and hotels.

Interconnected to shaming and the SCS is the *'Laolai map'* or also known as the Deadbeat map. It is a mini-program within Wechat that is released by the Hebei Higher People's Court and introduced at the beginning of 2019. The program pinpoints anybody within a 500 meter radius that is a *laolai* or in other words; has a debt to the Hubei Higher People's Court. By using the app the user can see the reason why a *laolai* has been labelled as untrustworthy, personal information such as their full name and even the court case number in case they

[10] Laolai is a derogatory term for people who fail to pay their fines and are seen as dishonest. The consequence is that they end up on a financial blacklist with severe consequences such as naming and shaming (Zhang, 2019).

have a lead. A court spokesman justified that it was part of a measure to *"enforce the ruling of Hubei Higher People's Court and create a socially credible environment"* (Zhang, 2019; Handley, Xiao, 2019). The initiative was eventually picked up by the Supreme People's Court and the Communist Party's Publicity Department into establishing it as a national policy. Local governments are advised by the Party to set up so-called name-and-shame databases that are searchable by anybody in the nation. It's presented as a move to improve the trustworthiness with the public shaming channels seen as a *'important tool in punishing those regarded untrustworthy'* according to state-run media agent Xinhua (Huifeng, 2017).

The courts are also cooperating with the Chinese telecom providers upon further shaming people in their social network. If you are calling a person that is on the blacklist by the court you are forced to listing to a pre-recorded message that states that *"the number you have dialled is of a user who has been listed as someone who is avoiding his debt repayments. Please remind the person to honour their legal obligations"* (Prevost, 2019; Ong, 2017). It's been named the ringtone of shame, and it will only disappear once a person has paid his debts to the court. Shame is hence used as a form of alternative justice by the Party, incorporating social media elements to shame people into paying their debt.

Citizens are docile for now showing acceptance of the regulations, which is effectively the result of the surveillance. A side-question is how far the Party can push the boundaries of surveillance before citizens are not accepting the rules of the game anymore. Public shaming has however, a long tradition within China and is partially accepted as a tactic deployed by the Party (Muhlhahn, 2010). The asymmetrical relationship and system of social control allow the Party to deploy all elements they deem necessary. The systems in place are looking like a fait accompli, making the future seem only more dystopian with the upcoming SCS.

### Social Credit System

A topic of interest for the Western media, since the introduction, has been the SCS. The design for the SCS was presented in the policy document *"Planning Outline for the Construction of a Social Credit System"* in 2014 by the State Council of China. Human Rights Watch has since labelled the SCS and the increased methods of surveillance as dystopian with severe consequences for the human rights of Chinese citizens (SCMP, 2018a). Western media have depicted the system of credit and the combined methods of surveillance as a uniform and unified system that generates a single score for every individual living within mainland China. Scholars, such as Rogier Creemers in his work *"China's Social Credit System: An Evolving Practice of Control"*, have showcased that this is inaccurate and that the SCS is more of an ecosystem of initiatives sharing an underlying logic.

Back in 2014, China's chief administrative body called for the establishment of a nationwide system for the tracking of the trust wordiness of corporations, government officials and also citizens (Matsakis, 2019). The starting point for the construction of the SCS is hence not to monitor society and label every citizen with a credit score that will determine their path of life. A popular reference is Black Mirror's episode 'Nosedive', a world where citizens rate each other for every action, and if your rating drops too low, then so does your life. This is a rather far-fetched reconstructing of the SCS, building a place of imminent social control by every inhabitant. The SCS is constructed as a basis for building a harmonious socialist society (State Council, 2014) where the SCS will help upon establishing a sincere society.

We can determine that the point of departure for the Chinese state was not to implement a system for labelling every citizen with a credit score. The social credit system is interconnected to a more significant problem within Chinese society, that of legal and regulatory implementation, enforcement and compliance (Creemers, 2018). Enhancing the public trust in government officials and corporations is at the centre, by fighting corruption and business fraud with punishment that can no longer be avoided. Strengthening the rule of law and the awareness is thus a key point within the framework. The implementation of the framework will promote and ensure social stability, vitality and harmony leading to an increase of the social governance capabilities as depicted in the 13th- five-year plan (13th Five year-plan, 2016).

A credit system would provide an incentive for those companies who act in good faith and implement a system of punishment to enterprises that lack credibility, eventually forcing them out of the market. The same general idea can then be applied to citizens. The strengthening of the rule of law was also at the foundation of the laolai concept, making people aware of their wrongdoings by publicly shaming them. A popular phrase regarding the SCS in early policy documents is *"to allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step"* (Hunt, 2018). It is essentially punishing those that lack credibility via a blacklist, restricting access to public goods and services. Movement can be restricted by being on a no-fly list, access in the shape of public schools for your children or a mortgage. The consequences of the SCS can thus be severe for the private life of a citizen or the business environment of an enterprise.

The state of today's SCS is far from being the dystopian image that is being depicted by particular Western Media such as the Wall Street Journal. In its current state, it's more of a patchwork of local and regional pilots that are still in their experimental phase (Matsakis, 2019). Hence, the question remains if the system could develop into the dystopian image constructed by the Western hemisphere, are we witnessing the realization of a Panoptic element or a normative system for restoring public trust?

The SCS is essentially a cooperation between government and private actors for the assembling of various scoring systems, ranking individuals and enterprises for the upholding of the rule of law and social trust. The score is comprised of economic, political and social factors that will reward discounts, exclusive access, or being blacklisted with restricted forms of access. In the current state, various private enterprises are experimenting with the concept. China Rapid Finance, a partner of Tencent, is one party with another one being Ant Financial Services Group (AFSG), run by Alibaba. Sesame Credit, run by AFSG, has a score ranging from 350-950 points based upon five factors that are disclosed by Alibaba: Credit history, fulfilment capacity, personal characteristics, behaviour and preferences and lastly interpersonal relationships.

The SCS is thus not a single system but is composed of government based systems and private companies with, for instance, a credit-history based model. Hence, it is not possible to comment on the individual criteria's, the system is also not fully operational and certainly not at a nation-level, despite what Western media are reporting (Velghe, 2019). The SCS does fit the overall holistic approach of the government towards social management. It exceeds the notion of just lawfulness but is also aimed at the *"morality of the actors' actions, covering economic, social and political conduct"* (Creemers, 2018, p. 2). Social management and the informatization policy are built upon the advancements made within the technological domain, ultimately AI and big data are drivers for achieving the goal of the CCP upon practising self-discipline and performing your legal and social obligations (13th Five year-plan, 2016, p. 200). The capabilities of AI in the future will be a significant driver for the set-up of the SCS on a national level.

The misconceptions regarding the system also covers up the concerns on what is already happening within society, for instance, in the Xinjiang area. The focus, therefore, needs to be adjusted from the potential could happen to what is already happening. There is no all-seeing integrated system that monitors and evaluates every action in mainland China; there are, nonetheless, programs in place that could give the feeling of constant surveillance in certain areas. The Panoptic idea of constant surveillance anywhere you travel is thus not a reality. The feeling of being in Panoptic state could, however, be constructed via programs such as the SCS, the name and shame policy and innovative drones.

### Skynet

Another well-known system that makes use of FRT is named Sky Net, or Tiangwang. It is part of the classical Chinese proverb *"The net of Heaven has large meshes, but it lets nothing through"* (Wright, 2018, p. 3). The system is said to have the capability to scan the entire Chinese population within one second (Asia Times, 2018), even if citizens are travelling by car or escalator. The system is designed to help the Chinese police fight crime and improve the overall security within China. Xinhua reports have stated that the system is using FRT and big-data technology to enhance its reliability, which is according to its lead developer, Yuan Peijang, already at 99,8% (Wright, 2018). The surveillance cameras installed are feeding the police with data of the whereabouts of the citizens, and the CCTV can follow citizens around. It is designed that once a person's face is uploaded into the data bank the surveillance cameras across the nation-state can identify the person, explains Li Wei, a counterterrorism expert at the China Institute of Contemporary Relations (Asia Times, 2018). The Xinhua reports do not specify who the developer is of Tianwang. Experts, however, believe that Hikvision, a well-known party within the security and surveillance industry, is collaborating with the Chinese Ministry of Public Security.

Li Wei has stressed the importance of privacy and acknowledged that the recorded and stored data is safe with strict government oversight to prevent any future unauthorized use of Skynet. Facial information is furthermore only collected within public places; hence Zhao Zhanling a legal counsel of the Internet Society of China says there is no intrusion of people's privacy contrary to Western media. Chinese citizens that are walking in public spaces thus give consent upon getting scanned by FRT via CCTV's. The lack of regulation for the protection of citizens is worrisome and will only be exploited more within the near future. There needs to be a line between security and freedom, especially with the enhanced modern surveillance technology that is upcoming. In turn, it will create a situation where the party will collect a more substantial amount of data what can be rendered into knowledge. Overall FRT Is taking off around the globe. Still, it is not as widely adopted anywhere as it is within mainland China, neither are the systems abroad uniformly of its accuracy and its viability (Wright, 2018).

With the current elements in place for surveillance, the structure is fragmented across the board with increased surveillance capacity in specific regions of the country, most notably Xinjiang area. Previously mentioned systems such as Skynet, the SCS and surveillance technology such as the robotic dove could integrate existing elements to portray a greater sense of surveillance coverage across the nation. In the current state, there is no blanket coverage under the heaven and citizens experience a different kind of surveillance level in each province, county or even city. The Panoptic theory portrays a singular level of surveillance across the board what is not realised within mainland China. Hence, we can distinguish a limitation of the theoretical framework that there can only be a one dimensional level of surveillance which is not achievable at this point in time. Mainland China is seen as the pinnacle of modern surveillance which is still far removed from creating a Panoptic feeling in every province. Information technology is enabling surveillance to be carried out in ways that are less visible compared to those in George Orwell’s Ninety Eighty-Four (Lyon, 1994) — pushing people to comply with the rules simply because they never know if they are being watched. Observation for the Party will result in knowledge and knowledge is forever connect to power (Foucault, 1977, p. 27). The Panopticon concept is used as a sophisticated tool of coercion, giving the impression of constant surveillance what will lead to the goal of self-surveillance.

## 6. Conclusion

FRT and AI are components that are going to supercharge the Chinese surveillance apparatus that is known for its considerable low amount of restraints on how the government can track and surveil citizens (Matsakis, 2019). Most contemporary surveillance cameras are non-intelligent and used as deterrence; AI will change the playing field by giving digital brains to the Panoptic gaze.

Facial recognition and AI are adopted as tools to track and identify citizens with millions of cameras and countless lines of code, but this does not justify the – occasionally – unfettered use of terms such as high-tech authoritarian state and Big Brother. The surveillance apparatus with its components of Xue Liang, SCS and Skynet is far too complex to be boiled down to a single element that can be identified as the Big Brother factor. The cornerstone of the Chinese Panoptic society, the SCS, is furthermore interconnected to a significant problem within Chinese society, that of legal and regulatory implementation, enforcement and compliance (Creemers, 2018). The fight against corruption, prevention of food and drug quality scandals and environmental damage, however, gets overshadowed by buzz-worthy news about personal ratings of the SCS and the all-seeing eye of the Party.

While this research does recognize the need for improving the rule of law and awareness, it also identifies the thin line between overusing the systems in place to set up a large scale police state. The Chinese surveillance apparatus has showcased to be a unique phenomenon, and the question needs to be answered if the current state is a reflection of Foucault's Panoptic society. There are signs of the construction of a hi-tech surveillance state with the help of FRT and AI; the elements of surveillance are, however, still in a fractured state. The current system resembles more of a digital patchwork than an all-seeing surveillance system This results in the questioning of the widespread use of terms as Big Brother and George Orwell's Ninety Eighty-Four classic that is regularly referred to by Western media (Kaplan, 2011).

Starting off, there is no all-seeing eye that is overseeing all actions and communications within mainland China; there are, nonetheless, parts of the system in place that could resemble the feeling of being in a Panopticon. The elements of the Chinese surveillance system are thus fragmented and fail to form a central core of unity due to bureaucratic inefficiencies and the technological capabilities of today (Mozur, 2018). Beijing has large scale ambitions with AI and FRT, but currently, the ambition is greater than its capabilities. In modern-day China, some cities are indulged in high-tech surveillance while other cities within the same prefecture lack the standard surveillance cameras.

The current state of affairs does enable the Party to securitize elements of technology, resulting in the exploitation of technological advancements. FRT and AI will provide enhanced opportunities for both the domestic security industry and the surveillance goals of the state. There is a trade-off to be made between the privacy of Chinese citizens and the enhanced – feeling – of security, if this trade-off is one of equal terms is a question that each answers differently. The lack of privacy rights within the Chinese law is concerning, (Griffith, 2019) resulting in the objectifying of citizens as symbols of information. The construction of a 'multi-modal' biometric portrait of citizens is furthermore a whole new level of privacy infringement that is unseen across the globe. The Chinese government is now not only failing to protect the privacy of its citizens, but it is actively invading it for its self-interest.

The case study concludes that there is no Panoptic state present in mainland China, components of the digital patchwork can, nevertheless, still work towards the element of self-surveillance. The raison d 'être for the surveillance apparatus is not to provide one hundred per cent governmental oversight, but to achieve a state of mind. China's securitizing of technological advancement is heading towards an IT-led social transformation (Mun-Cho, 2004) to indulge a sense of self-surveillance.

Future developments will shift the surveillance system from being an architecture of observation to an architecture of control, affecting the autonomy of citizens and private enterprises. AI will grant the possibility to implement a system of direct punishment, instilling a greater sense among the citizens that they are subject to a centralized discipline. The Party wants to improve its position vis-à-vis the ruled via a mechanism of observation that will lead to knowledge. The perception of constant surveillance will lay the groundwork for self-surveillance, making the Panoptic gaze continues in its effect even it would be discontinuous in its action (Foucault, 1977).

Two out of the four elements of the Panoptic theory are in place regarding the case study of mainland China; there is no singular actor or all-seeing eye, and the widespread coverage is far from being consistent across the board. What is in place is the essence of exploitation of technological innovations that is working towards the goal of social management. Foucault's Panoptic society theory hence partly explains the construction and bolstering of the surveillance apparatus within mainland China. The strength of the Panopticon is that of a *"calculated technology of subjection"* (Foucault, 1977, p. 201) inducing a state of conscious and permanent visibility resulting in the automatic functioning of power, what can be translated to the social management practices of the Party.

A limitation upon working with Foucault's Panoptic theory has been the one-dimensional state of surveillance across the board while in fact, there are numerous of layers. Hence, it does not provide the necessary tools upon scrutinizing the entirety of mainland China. The theory can, however, provide valuable insights if used on a province or city-based level.

Foucault's Panoptic theory and especially the element of self-surveillance has proven to be well-suited to analyse China's surveillance apparatus. The theory is nevertheless out of its depths when considering the scope of the case study. Further research within the domain of Foucault's Panopticon needs to be centred around the province or city level to scrutinize the presence of a Panoptic state adequately. Contemporary types of surveillance are, nonetheless shifting out of the realm of visibility, effectively making state surveillance invisible. Electronic Panopticism could, therefore, provide to be a more suitable approach on a state level. The research has showcased that the concept of the Panopticon is still a powerful metaphor that stays relevant and pushes the boundaries beyond Orwell's Big Brother thought.

The direction China is heading into is concerning but the complicated truth needs to be researched instead of treating the system as one unified force for wrongdoing. Only time will tell if the fragmented state of the surveillance system is a foundation for a sincere society or the build up for a AI-driven Panopticon.

## Bibliography

### Academic Literature

Ahmed, S. (2017). Cashless society, cached data—security considerations for a Chinese social credit system. The citizen lab. Retrieved from https://citizenlab.ca/2017/01/cashless-societycached-data-security-considerations-chinese-social-credit-system/

Allen, G., Chan, T. (2017). Artificial Intelligence and National Security. Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Arsène, S. (2016). Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic World Order? China Perspectives, 135 (2)

Austin, G. (2014). Cyber Policy in China. New York: Polity

Barnett, J. (2001). Security and Climate Change. Tyndall Centre for Climate Change Research, New Zeeland

Bilgin, P. (2011). The politics of studying securitization? The Copenhagen School in Turkey. The Politics of Securitization, 42 (5), 399-412

Buzan, B., Weaver, O., de Wilde, J. (1988). Security: A New Framework for Analysis. Lynne: Rienner Publishers.

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. Social Identities, 16 (5), 621-633

Cave, D., Ryan, F., Xiuzhong Xu, V. (2019, November 28). Mapping more of China’s tech giants: AI and surveillance. Retrieved from https://www.aspi.org.au/report/mapping-more-chinas-tech-giants

Clingendael. (2019, October). Stories to rule the world: China’s narrative strategy and European soft power. Retrieved from https://www.clingendael.org/publication/chinas-stories-rule-world

Creemers, R. (2018). China’s social credit system: an evolving practice of control. Retrieved from https://ssrn.com/abstract=3175792 or http://dx.doi.org/10.2139/ssrn.3175792

Curley, M.G., Wong. S. (2008). Security and Migration in Asia: The Dynamics of Securitisation. London: Taylor & Francis.

Emmers, R., Greener, B.K., Thomas, N. (2008). Securitising human trafficking in the Asia-Pacific: Regional organizations and response strategies. Security and Migration in Asia. London: Taylor & Francis.

Espoti, S.D. (2014, May). When Big Data Meets Dataveillance: The Hidden Side of Analytics. Retrieved from https://www.researchgate.net/publication/262493771_

Ferracane, M.F., Makiyama, H.L. (2017). China's technology protectionism and its non-negotiable rationales. Retrieved from http://ecipe.org/publications/chinas-technology-protectionism/?chapter=all

Foucault, M. (1977). Discipline and Punish: The Birth of the Prison. New York: Pantheon.

Freedom House. (2018, October). Freedom on the Net 2018: The Rise of Digital Authoritarianism. Retrieved from https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf

Galic, M., Timan, T., Koops, B.J. (2017). Bentham, Deleuze and Beyond: An overview of Surveillance Theories from the Panopticon to Participation. The British Society for Phenomenology, 25 (2), 157-169

Government of Canada. (2018, May 17). China's Intelligence law and the country's future intelligence competitions. Retrieved from https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html

Greitens, S. (2016). Dictators and their Secret Police: Coercive Institutions and State Violence. Cambridge: Cambridge University Press

Grother, P., Ngan, M., Hanaoka, K. (2019, December). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Retrieved from https://www.nist.gov/publications

Hacking, I. (1990). The taming of chance. Cambridge: Cambridge University Press

Haggerty, K. & Ericson, R. (2003). The Surveillant Assemblage. The British Journal of Sociology, 51 (4), 605-622

Hoffman, S.R. (2017). Programming China: the Communist Party's autonomic approach to managing state security. Phd Thesis, University of Nottingham. Retrieved from http://eprints.nottingham.ac.uk/48547/1/Hoffman%2C%20Samantha%20Student%20ID %20 4208393%20PHD%20THESIS%20Post%20Viva%20copy.pdf

Hou, R. (2017). Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China. Surveillance & Society 15 (3-4), 418-424

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of Approval. New Media and Society, 21 (7), 1565-1593

Langheinrich, M. (2001). Privacy By Design – Principles of Privacy-Aware Ubiquitous System. Ubiquitous Computing: UbiComp 2001, 2201, p. 273-291

Lee, J.A., Liu, C.Y. (2016). Real-name Registration Rules and the Fading Digital Anonymity in China. Washington International Law Journal, 25 (1)

Linz, J.J. (1988). Legitimacy of Democracy and Socioeconomic systems. Comparing Pluralist Democracies; Strains on Legitimacy. Boulder: Westview Press

Lo Yuk-ping, C., Thomas, N. (2010). How is health a security issue? Politics, responses and issues. Health Policy and Planning, 25 (6), 447-453

Lyon, D. (1994). The Electronic Eye: The Rise of Surveillance Society. Minneapolis, Minnesota: University of Minnesota Press

Marx, G. (2002). What's New About the "New Surveillance"? Classifying for Change and Continuity. Surveillance & Society 1 (1), 8-29

Mathiesen, T. (1997). The Viewer Society: Michel Foucault's Panopticon Revisited. Theoretical Criminology, 1 (2), 215-234

McDonald, M. (2008). Security Studies: An Introduction. Abingdon: Routlegde.

Morozov, E. (2019). Digital Socialism? The calculation Debate in the Age of Big Data. The New Left Review, 116, 33-67

Mun-Cho, K. (2004). Surveillance Technology, Privacy and Social Control: With Reference to the Case of Electronic National Identification Card in South Korea. International Sociology, 19 (2), 193-213

Nathan, A.J. (2003). China's Changing of the Guard: Authoritarian Resilience. Journal of Democracy, 14 (1), 6-17

National Institute of Standards and Technology (NIST). (2019, December). Face Recognition Vendor Test Part 3: Demographic Effects. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Organization for Economic Cooperation and Development (OECD). (2018). China's Belt and Road Initiative in the Global Trade, Investment and Finance Landscape. Retrieved from https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf

Orwell, G. (1989). Nineteen Eighty-Four. London: Penguin Books

Patton, P. (1994). MetamorphoLogic: Bodies and Powers in a Thousand Plateaus. Journal of British Society for Phenomenology, 25 (2), 157-169

Pieke, F. (2012). The Communist Party and Social Management in China. China Information, 26 (2), 149-165

Putten, van der J. (2019). Fabels over China: Hardnekkige westerse misvattingen over de nieuwe wereldmacht. Amsterdam: De Geus

Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. Journal of Democracy, 30 (1), 53-67

Robbins, S., Henschke, A. (2017). Designing for Democracy: Bulk Data and Authoritarianism. Surveillance & Society, 15(3), 582-589

Schermer, B.W. (2009). Surveillance and Privacy in the Ubiquitous Network Society. Amsterdam Law Forum, 11 (3), 63-76

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: Norton & Company

Schwarck, E. (2018). Intelligence and Informatization: The Rise of the Ministry of Public Security in Intelligence Work in China. The China Journal, 80, 1-23

Shaun, B. (2015). Debating Human Security in China: Towards Discursive Power? Journal of Contemporary Asia, 45 (2), 243-265

Snowden, E. (2019). Permanent Record. London: Metropolitan Books.

Svolik, M.W. (2009). Power Sharing and Leadership Dynamics in Authoritarian Regimes. American Journal of Political Science, 53 (2), 477-494

Toshkov, D. (2016). Research Design in Political Science. London: Macmillian Education UK

Trombetta, M.J. (2019). Securitization of Climate Change in China: Implications for Global Climate Governance. China quarterly of International Strategic Studies, 5 (1), 97-116

Tsui, L. (2003). The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China. China Information, 17 (2), 65-82

Upadhyaya, P. (2006). Securitization matrix in South Asia: Bangladeshi migrants as enemy alien. In Caballero-Anthony, M., Archarya, A (eds) Non-Traditional Security in Asia: Dilemmas in Securitisation. Aldershot:Ashgate, 13-39

Vaughan-Williams, N. (2010). Securitization Theory in Critical Security Studies: An Introduction. Oxon: Routlegde

Velghe, P. (2019). “Reading China” – The Internet of Things, Surveillance, and Social Management in the PRC. China Perspectives, 85-89

Waever, O. (1995). Securitization and desecuritization, in Lipschutz, R. (Ed), On Security. Columbia University Press, New York, 46-86

Waever, O. (1998). International Relations Theory and the Politics of European integration. London: Routlegde

Waever, O. (2011). Politics, Security, Theory. Security Dialogue, 42 (4-5), 465-480

Wang, Z. (2014, March). The Chinese Dream: Concept and Context. Journal of Chinese Political Science, 19 (1)

Wei, S.J., Xie, Z., Zhang, X. (2017). Journal of Economic Perspectives, 31 (1), p. 49-70

Wood, D.M. (2017). The Global Turn to Authoritarianism and After. Surveillance & Society, 15(3), 357-370

Yan, B. (2016). Securitization and Chinese Climate Change Policy. Chinese Political Science Review, 1, 94-112

Yang, H., Zhao, D. (2015). Performance Legitimacy, State Autonomy and China’s Economic Miracle. Journal of Contemporary China, 24, 64-82

Yang, Y. (2008). ‘Zhongxing Zhengfu yu Zhongguo de Jingji Qiji’ [The neutral state and China’s economic miracle’]. Twenty-First Century Review, 107, 15-25

Yin, R.K. (1984). Case Study Research: Design and Methods. Beverly Hills. Calif: Sage Publications.

## Investigative Journalism

Ali, Meiryum. (2019, May 31). The Future is Voice Activated: A Look into AI Voice Recognition in China. Retrieved from https://lionbridge.ai/articles/the-future-is-voice-activated-a-look-into-ai-voice-recognition-in-china/

Allen-Ebrahimian, B. (2019, November 24). Exposed: China’s Operating Manuals for Mass Internment and Arrest by Algorithm. Retrieved from https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/

Almond, K. (2018). A Rare look inside Huawei, China’s tech giant. Retrieved from https://edition.cnn.com/interactive/2019/05/business/huawei-cnnphotos/index.html

Alper, A. (2020, January 03). US government limits exports of artificial intelligence software. Retrieved from https://www.reuters.com/article/us-usa-artificial-intelligence/u-s-government-limits-exports-of-artificial-intelligence-software-idUSKBN1Z21PT

Anderlini, J. (2019, June 05). How China’s smart-city tech focuses on its own citizens. Retrieved from https://www.ft.com/content/46bc137a-5d27-11e9-840c-530737425559

Asia Times. (2018, May 08). Surveillance system can scan Chinese population ‘in 1 second’. Retrieved from https://www.asiatimes.com/2018/05/article/surveillance-system-can-scan-chinese-population-in-1-second/

Baraniuk, C. (2018, November 08). China’s Xinhua agency unveils AI news presenter. Retrieved from https://www.bbc.com/news/technology-46136504

BBC. (2013, March 14). Profile Hu Jintao. Retrieved from https://www.bbc.com/news/world-asia-china-20216496

Bischoff, P. (2019a, August 15). The World’s most-surveilled cities. Retrieved from https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Bischoff, P. (2019b, October 15). Surveillance States: Which countries best protect privacy of their citizens? Retrieved from https://www.comparitech.com/blog/vpn-privacy/surveillance-states/

Bloomberg. (2018a, January 17). China Uses Facial Recognition to Fence in Villagers in Far West. Retrieved from https://www.bloomberg.com/news/articles/2018-01-17/china-said-to-test-facial-recognition-fence-in-muslim-heavy-area

Bloomberg. (2018b, January 18). China said to be testing facial recognition system to monitor Muslim-dominated Xinjiang region. Retrieved from https://www.scmp.com/news/china/society/article/2129473/china-testing-facial-recognition-system-monitor-muslim-dominated

Buckley, C., Mozur, P. (2019, May 22). How China Uses High-Tech Surveillance to Subdue Minorities. Retrieved from https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

Burt, C. (2019, October 22). Facial Recognition payments not a hit yet in China, but new services launching. Retrieved from https://www.biometricupdate.com/201910/facial-recognition-payment-not-a-hit-yet-in-china-but-new-services-launching

Chan, T.F. (2018, May 21). A School in China is monitoring students with facial-recognition technology that scans the classroom every 30 seconds. Retrieved from https://www.businessinsider.nl/china-school-facial-recognition-technology-2018-5?international=true&r=US

Chen, S. (2018, June 24). China takes surveillance to new heights with flock of robotic doves, but do they come in peace? Retrieved from https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they

China business Daily. (2018, May 25). 三场演唱会抓到三逃犯　张学友被封“神捕”. Retrieved from http://sc.people.com.cn/n2/2018/0525/c345459-31624714.html

China Power. (2017, May 08). How will the Belt and Road Initiative advance China’s interests? Retrieved from https://chinapower.csis.org/china-belt-and-road-initiative/

Cimpanu, C. (2019, December 23). Russia successfully disconnected from the internet. Retrieved from https://www.zdnet.com/article/russia-successfully-disconnected-from-the-internet/

Cockerell, I. (2019, September 05). Inside China’s Massive Surveillance Operation. Retrieved from https://www.wired.com/story/inside-chinas-massive-surveillance-operation/

Dai, S. (2019a, December 04). China’s Subways embrace Facial Recognition Payment Systems Despite rising privacy concerns. Retrieved from https://www.scmp.com/tech/apps-social/article/3040398/chinas-subways-embrace-facial-recognition-payment-systems-despite

Dai, S. (2019b, May 15). How 9/11 and China’s plan for blanket surveillance created a wave that CCTV camera makes Hikvision and Dahua rode to huge success. Retrieved from https://www.scmp.com/tech/gear/article/3010312/how-9/11-and-chinas-plan-blanket-surveillance-helped-hikvision-and-dahua

Dellinger, A. (2018, July 05). Facial Recognition Used by Wales Police has 90 Percent False Positive Rate. Retrieved from https://gizmodo.com/facial-recognition-used-by-wales-police-has-90-percent-1825809635?

Denyer, S. (2018, February 07). China’s watchful eye. Retrieved from https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/

Dilbert, D. (2019, November 07). Moscow is About to Build A Surveillance System to Rival China’s Dystopian Nightmare. Retrieved from https://www.vice.com/en_us/article/9kej75/moscow-is-about-to-build-a-surveillance-system-to-rival-chinas-dystopian-nightmare?

Doffman, Z. (2019a, May 16). Dutch spies Investigate Huawei ‘Links to Chinese Espionage’ from ‘Hidden Backdoor’. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/05/16/dutch-spy-agency-investigating-huawei-back-door-and-links-to-china-espionage/#7bceeedc1dbd

Doffman, Z. (2019b, November 29). Has Huawei’s Darkest Secret Just been Exposed by this New Surveillance Report? Retrieved from https://www.forbes.com/sites/zakdoffman/2019/11/29/has-huaweis-darkest-secret-just-been-exposed-by-this-new-report/

Faiz, A. (2019, July 18). China is building a global coalition of human rights violators to defend its record in Xinjiang – what is the endgame? Retrieved from http://theconversation.com/china-is-building-a-global-coalition-of-human-rights-violators-to-defend-its-record-in-xinjiang-what-is-its-endgame-120546

Fan, W., Khan, N., Lin, L. (2017, December 26). China Snares Innocent and Guilty Alike to Build World’s Biggest DNA Database. Retrieved from https://www.wsj.com/articles/china-snares-innocent-and-guilty-alike-to-build-worlds-biggest-dna-database-1514310353

Fu, W. (2019). Chinese Tech Giants Baidu, Alibaba, and Tencent are De Facto Tools of Chinese Regime: US Official. Epoch Times. Retrieved from https://www.theepochtimes.com/chinese-tech-giants-baidu-alibaba-and-tencent-are-de-facto-tools-of-chinese-regime-us-official_3084080.html

Gertz, B. (2019, November 07). US and China racing to weaponize AI. Retrieved from https://www.asiatimes.com/2019/11/article/us-and-china-racing-to-weaponize-ai/

Griffith, C. (2019, August 29). Surveillance cameras with AI are watching you. Retrieved from https://www.theaustralian.com.au/inquirer/surveillance-cameras-with-ai-are-watching-you/news-story/78f8244d4c9622d5b003ae514969a083

Guan, W. (2019, December 29). CGTN’s Wang Guan: What’s China’s ‘re-education camp’ in Xinjiang really about? Retrieved from https://news.cgtn.com/news/2019-12-29/What-s-China-s-re-education-camp-in-Xinjiang-really-about--MOepa5AKcM/index.html

Hawkins, A. (2017, May 24). Chinese citizens Want the Government to Rank Them. Retrieved from https://foreignpolicy.com/2017/05/24/chinese-citizens-want-the-government-to-rank-them/

Hernandez, J.C. (2017, October 25). China’s ‘Chairman of Everything’: Behind Xi Jinping’s Many Titles. Retrieved from https://www.nytimes.com/2017/10/25/world/asia/china-xi-jinping-titles-chairman.html

Hoffman, S. & Mattis, P. (2016, July 18). Managing the Power Within: China’s State Security Commission. Retrieved from https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission/

Hornby, L. (2019, February 03). Chinese app names and shames bad debtors. Retrieved from https://www.ft.com/content/2ad7feea-278e-11e9-a5ab-ff8ef2b976c7

Horsley, J. (2018, November 16). China’s Orwellian Social Credit Score Isn’t Real. Retrieved from https://foreignpolicy.com/2018/11/16/chinas-orwellian-social-credit-score-isnt-real/

Huifeng, He. (2017, October 10). China to create national name-and-shame system for ‘deadbeat borrowers’. Retrieved from https://www.scmp.com/news/china/economy/article/2114768/china-create-national-name-and-shame-system-deadbeat-borrowers

Human Rights Watch. (2017a, May 15). China: Police DNA Database Threatens Privacy: 40 million Profiled Included Dissidents, Migrants, Muslim Uyghurs. Retrieved from https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy

Human Rights Watch. (2017b, October 22). China: Voice Biometric Collection Threatens Privacy. Retrieved from https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy

Hunt, P. (2018, December 04). China’s Great Social Credit Leap Forward. Retrieved from https://thediplomat.com/2018/12/chinas-great-social-credit-leap-forward/

Jing, M. (2019, December 02). Chinese tech companies are shaping UN Facial Recognition standards, according to leaked documents. Retrieved from https://www.scmp.com/tech/policy/article/3040164/chinese-tech-companies-are-shaping-un-facial-recognition-standards

Kaplan, C.S. (2001, February 02). Kafkaesque? Big Brother? Finding the Right Literary Metaphor for Net Privacy. Retrieved from https://www.nytimes.com/2001/02/02/technology/kafkaesque-big-brother-finding-the-right-literary-metaphor-for.html?auth=login-facebook&login=facebook

Keane, S. (2019, December 19). Huawei Ban: Full timeline as house bars US government from buying Chinese company’s gear. Retrieved from https://www.cnet.com/news/huawei-ban-full-timeline-house-us-government-china-trump-ban-security-threat-mate-x/

Long, Q. (2018, March 30). China aims for Near-Total Surveillance, Including in People’s Homes. Retrieved from https://www.rfa.org/english/news/china/surveillance-03302018111415.html

Lucas, L. & Feng, E. (2018, July 20). Inside China’s Surveillance State. Retrieved from https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d5404543

Martin, N. (2019, December 01). China launches compulsory face scans for new phone users. Retrieved from https://www.dw.com/en/china-launches-compulsory-face-scans-for-new-phone-users/a-51489212

Mason, P. (2017, July 31). Democracy is dying – and startling how few people are worried. Retrieved from https://www.theguardian.com/commentisfree/2017/jul/31/democracy-dying-people-worried-putin-erdogan-trump-world

Matsakis, L. (2019, July 29). How the West got China’s Social Credit System Wrong. Retrieved from https://www.wired.com/story/china-social-credit-score-system/

McCarthy, N. (2018, August 23). China now boasts more than 800 million internet users and 98% of them are mobile. Retrieved from https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/

McMullan, T. (2015, July 23). What does the Panopticon mean in the age of digital surveillance? Retrieved from https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

Mollman, S. (2019, October 05). China’s new weapon of choice is your face. Retrieved from https://qz.com/1721321/chinas-new-weapon-of-choice-is-facial-recognition-technology/

Mozur, P. (2017, July 20). Beijing wants A.I. to be made in China by 2030. Retrieved from https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html

Mozur, P. (2018a, July 08). Inside China’s Dystopian Dreams: AI, Shame and Lots of Cameras. Retrieved from https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

Mozur, P. (2018b, July 16). Looking through the eyes of China’s Surveillance State. Retrieved from https://www.nytimes.com/2018/07/16/technology/china-surveillance-state.html

Mozur, P., Kessel, J.M., Chan, M. (2019, April 24). Made in China, Exported to the World: The Surveillance State. Retrieved from https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Muhlhahn, K. (2010, July 31). How shaming was used in Chinese history. Retrieved from https://www.nytimes.com/roomfordebate/2010/07/31/china-shaming/how-shaming-was-used-in-chinese-history

O’Connor, S. (2019, May 06). How Chinese Companies Facilitate Technology Transfer from the United States. US-China Economic and Security Review Commission: Staff Research Report. Retrieved from https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf

Ong, T. (2017, July 26). A Court in China is shaming people who owe money by telling everyone who calls them. Retrieved from https://www.theverge.com/2017/7/26/16034118/china-court-shaming-people-voice-messages

Petricic, S. (2017, January 11). Big Brother collecting big data – and in China- It’s all for sale. CBC News. Retrieved from https://www.cbc.ca/news/world/china-data-for-sale-privacy-1.3927137

Phillips, T. (2018, January 18). China testing facial-recognition surveillance system in Xinjiang report. Retrieved from https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report

Prevost, T. (2019, May 22). China is testing ‘The Ringtone of Shame’ for Debtors. Retrieved from https://www.konbini.com/en/politicsandsociety/chine-testing-ringtone-shame-for-debtors/

Privacy International. (n.d.). Visual Surveillance Technology. Retrieved from https://privacyinternational.org/topics/visual-surveillance-technology

Qin, A., Hernandez, J.C. (2018, November 25). How China’s Rulers Control Society: Opportunity, Nationalism and Fear. Retrieved from https://www.nytimes.com/interactive/2018/11/25/world/asia/china-freedoms-control.html

Radio Free Asia. (2015, October 05). Beijing ‘100 Percent Covered’ by Web of Surveillance Cameras. Retrieved from https://www.rfa.org/english/news/china/cameras-10052015120935.html

Ramzy, A. (2019, November 16). Five Takeaways from the Leaked Files on China’s Mass Detention of Muslims. Retrieved from https://www.nytimes.com/2019/11/16/world/asia/china-muslims-detention.html?

Ramzy, A. & Buckley, C. (2019, November 16). ‘Absolutely No Mercy’: Leaked Files Expose How China Organized Mass Detentions of Muslims. Retrieved from https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html?

Robles, P. (2018, October 01). China plans to be a world leader in Artificial Intelligence by 2030. Retrieved from https://multimedia.scmp.com/news/china/article/2166148/china-2025-artificial-intelligence/index.html?src:article-launcher

Schlein, L. (2019, June 26). UN: Freedom of Expression under threat from surveillance industry. Retrieved from https://www.voanews.com/silicon-valley-technology/un-freedom-expression-under-threat-surveillance-industry

Schmitz, R. (2018, April 03). Facial Recognition in China is Big Business as Local Government Boost Surveillance. Retrieved from https://www.npr.org/sections/parallels/2018/04/03/598012923/facial-recognition-in-china-is-big-business-as-local-governments-boost-surveilla?t=1574697818373

South China Morning Post. (2016). China’s tiered city system explained. Retrieved from https://multimedia.scmp.com/2016/cities/

South China Morning Post. (2018a, January 18). China said to be testing facial recognition system to monitor Muslim-dominated Xinjiang region. Retrieved from https://www.scmp.com/news/china/society/article/2129473/china-testing-facial-recognition-system-monitor-muslim-dominated

South China Morning Post. (2018b, October 30). China’s Sharp Eyes surveillance system puts the security focus on public shaming. Retrieved from https://www.scmp.com/news/china/politics/article/2170834/chinas-sharp-eyes-surveillance-system-puts-security-focus-public

South China Morning Post. (2019). China Internet Report 2019. Retrieved from https://www.scmp.com/china-internet-report#secondSubscriptionForm

The Guardian. (2019, December 02). Big Brother is watching: Chinese city with 2.6m cameras is world’s most heavily surveilled. Retrieved from https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled

The Wall Street Journal. (2018). China’s All-Seeing Surveillance State is Reading its Citizens Faces. Retrieved from https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1498493020

The White House. (2013, June 7). Statement by the President: Fairmont Hotel, San Jose California. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president

Wang, M. (2017, August 18). China’s Dystopian Push to Revolutionize Surveillance. Retrieved from https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance

Wang, M. (2018). China’s Bumbling Police State. Human Rights Watch. Retrieved from https://www.hrw.org/news/2018/12/26/chinas-bumbling-police-state

World Bank. (n.d.). The World Bank in China. Retrieved from https://www.worldbank.org/en/country/china/overview

Wright, D.C. (2018). Eyes as Bright as Snow: Facial Recognition Technology and Social Control in China. Retrieved from https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/3859/attachments/original/1528764387/Eyes_as_Bright_as_Snow_-_Facial_Recognition.pdf?1528764387

Wu, A. (2018, October 08). Chinese Regime Escalates Efforts to Cover Countryside with Surveillance Cameras. Retrieved from https://www.theepochtimes.com/chinese-regime-escalates-efforts-to-cover-countryside-with-surveillance-cameras_2573351.html

Xiao, B., Handley, E. (2019, January 24). China test opening up social credit scores to social media platform Wechat with debt map. Retrieved from https://www.abc.net.au/news/2019-01-24/new-wechat-app-maps-deadbeat-debtors-in-china/10739016

Xiao, B., Robertson, H. (2019, April 30). Chinese debtors named and shamed on cinema screens during Avengers: Endgame film premier. Retrieved from https://www.abc.net.au/news/2019-04-30/chinese-debtors-shamed-on-cinema-big-screen/11049726

Xiaonan, W. (2019, December 30). CGTN Exclusive: A tour of a closed ‘re-education camp’ in Xinjiang. Retrieved from https://news.cgtn.com/news/2019-12-30/CGTN-Exclusive-A-tour-of-a-former-re-education-center-in-Xinjiang-MQ7rursV3i/index.html

Xie, E. (2019, December 01). China launches facial recognition for mobile phone users. Retrieved from https://www.scmp.com/news/china/politics/article/3040134/china-launches-facial-recognition-mobile-phone-users

Yang, Y. [Yuan]., Yang, Y. [Yingzhi]. (2017). China seeks dominance of global A.I. industry. Retrieved from https://www.ft.com/content/856753d6-8d31-11e7-a352-e46f43c5825d

Yi, D. (2019, November 28). Government Asks SenseTime to Lead Plans for National Facial- Recognition Standards. Retrieved from https://www.caixinglobal.com/2019-11-28/government-asks-sensetime-to-lead-plans-for-national-facial-recognition-standards-101488228.html

Yi, Z. (2017, October 15). People’s Daily expands reach with English-language news app. Retrieved from https://www.chinadaily.com.cn/china/2017-10/15/content_33284554.htm

Zand, B. (2018, July 26). A Surveillance State Unlike Any the World has Ever Seen. Retrieved from https://www.spiegel.de/international/world/china-s-xinjiang-province-a-surveillance-state-unlike-any-the-world-has-ever-seen-a-1220174.html

Zens, A. (2019, July 12). Beyond the Camps: Beijing’s Grand Scheme of Forced Labor, Poverty Alleviation and Social Control in Xinjiang. Retrieved from https://osf.io/preprints/socarxiv/8tsk2

Zhang, P. (2019a, December 05). China ‘world’s worst’ for invasive use of biometric data. Retrieved from https://www.scmp.com/news/china/society/article/3040710/china-worlds-worst-invasive-use-biometric-data

Zhang, P. (2019b, January 24). Is someone in debt nearby? Chinese court uses chat app to alert people as part of social credit system. Retrieved from https://www.scmp.com/news/china/society/article/2183494/someone-debt-near-you-chinese-court-uses-chat-app-tell-you-part

Zhang, Y. (2017, October 20). Security Innovation Seen as Crucial. China Daily. Retrieved from https://www.chinadaily.com.cn/china/2017-09/20/content_32225951.htm

## Governmental Documents

CCP Central Committee. (2014, October 28). CCP Central Committee Decision concerning Some Major Questions in Comprehensively Moving Governing the Country According to the law Forward. Retrieved from https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decision-concerning-some-major-questions-in-comprehensively-moving-governing-the-country-according-to-the-law-forward/

China Academy for Information and Communications Technology (CAICT). (2019, February 21). Artificial Intelligence Security White paper. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/

China Institute for Science and Technology Policy Tsinghua University. (2018, July). China AI Development Report 2018. Retrieved from http://www.sppm.tsinghua.edu.cn/eWebEditor/UploadFile/China_AI_development_report_2018.pdf

Ministry of Industry and Information Technology. (2017, December 12). Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018-2020). Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/

National People’s Congress. (2016). The 13th Five-year Plan. Retrieved from https://en.ndrc.gov.cn/newsrelease_8232/201612/P020191101481868235378.pdf

State Council of China. (2014, June 14). Planning Outline for the Construction of a Social Credit System (2014-2012). Retrieved from https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

State Council of China. (2016, July 27). Outline of the National Informatization Development Strategy. Retrieved from https://chinacopyrightandmedia.wordpress.com/2016/07/27/outline-of-the-national-informatization-development-strategy/

State Council of China. (2017, July). China’s New Generation of Artificial Intelligence Development Plan. Retrieved from https://flia.org/notice-state-council-issuing-new-generation-artificial-intelligence-development-plan/

State Council of China. (2019, March). The Fight Against Terrorism and Extremism and Human Rights Protection in Xinjiang. Retrieved from http://english.www.gov.cn/archive/white_paper/2019/03/18/content_281476567813306.htm

State Council of China. (2019, September). China and the World in the New Era. Retrieved from http://english.www.gov.cn/archive/whitepaper/201909/27/content_WS5d8d80f9c6d0bcf8c4c142ef.html