LEIDEN UNIVERSITY

FACULTY OF HUMANITIES

MASTER THESIS

“Reading China”

The Internet of Things, Social Management and Surveillance

Pieter Velghe

S1578472

MA Politics, Society and Economy of Asia

2016 - 2017

Table of Contents

1. Introduction

China has recently pledged to make “infomatization” the leading engine in its quest for developing the country and reinvigorating the economy. Among a wide range of promising new information and communication technologies (ICTs), the Internet of Things (IoT) is widely praised for having the potential to severely alter anything from manufacturing to medical care, as it allows for any object or process to be digitally connected and managed, and therefore optimized. Chinese policymakers have thus incorporated IoT-technology and services in its economic and social development plans. However, as internet-use in China was quickly regulated and controlled by the Chinese state to avoid the spreading of public discontent and social unrest, it remains to be seen how the Chinese state will deal with an internet made ubiquitous through IoT-technology – and if this new technology will ultimately harm the one-party rule, or if the Chinese Communist Party (CCP) will be able to harness the power of the IoT to strenghten its rule as it has done with the internet.[1]

By analysing the Chinese IoT-policy, I hope to identify what the overal plans and the main themes are for IoT-development envisioned by Chinese policymakers and how this fits in wider plans of “informatization”. More specifically, I will focus on how and if it is stated in these documents that the IoT is to be used to improve the state’s governing capacity in the form of e.g. improving social management, creating feedback mechanisms, and/or build surveillance networks. As more dependency on technology comes with more risks, the importance of improved security for ICTs and the IoT in particular as mentioned in Chinese policy will also be discussed. Hereby, I hope to answer the question whether or not the widespread adoption of more advanced ICTs, such as the IoT, by the Chinese state, will ultimately improve and expand the state’s governing capacity and thus strengthen its rule, or if it will make the state more dependent on technology that it can’t control and thus weaken its power.

The outline of my dissertation includes the following: firstly, I will discuss the IoT-technology and its projected development and capabilities to be able to assess how much the IoT can or will change current internet-enabled socio-political relations; secondly, I will examine the state of current

[1] Following Curran et al. (2012), I will refrain of referring to the internet with a capital “I”. Just like the telephone or the radio before it, it is just a communication technology after all.

internet- use and -control in China to then elaborate on the literature on the Chinese plans for "informatization" and their consequences for Chinese state power. After the methodology-section follows the analysis which consists of two parts: the first part deals with general IoT-policy to identify the main themes in envisioned IoT-development, and the second part deals with more specific IoT-development plans to identify concrete examples of how the IoT is to be used to increase the state's governing capacity according to Chinese policymakers.

2. The IoT: Prospects and profits

The Internet of Things (IoT) is one of the latest additions to the information and communication technologies (ICTs). In essence, the IoT consists of multiple "smart things" connected to the internet and also connected to each other. These "things" can range from anything "smart" or "digital-first" – that is: devices that are made to connect to the internet such as smart phones, smart wrist bands, smart thermometers, smart toasters, smart locks, drones, self-driving cars, … – to "physical-first" objects that are made to connect to the internet through attaching a microchip to it (Greengard 2015: 16-7). Connected things can exchange data between devices, and thus provide valuable information in areas and on a scale which was previously impossible (ibid.). The possibilities for connecting devices to the internet are seemingly endless. IoT devices are fundamentally changing the internet as, unlike most previous web-applications, the IoT devices and services have a direct impact on the physical world.

The IoT has been lauded for having the potential of being a "second wave of a powerful digital revolution that began with the widespread adoption of computers" and thus commencing an "Industry 4.0" (ibid: xiv, 51).[2] Accordingly, predictions are that by 2020, 20.8 billion devices will be connected worldwide, while in 2016 that was about 6.4 billion devices (Gartner 2015). Still other predictions put the number on over 50 million devices by 2020 (Cisco 2014). The application service revenue of the IoT is estimated to be around $1.3 trillion by 2025 (Machina Research 2016). Even though the technology still is in an "early adapter phase", according to Greengard (2015: xviii), the question is not so much over "whether the IoT will take place," rather "how exactly it will happen and how much it will change the world."

What makes the IoT so revolutionary according to its pundits, is not so much as in having so many more devices connected to the internet; rather its success lies in the fact that each of these devices tracks data (Greengard 2015). Especially in areas where this before was not so much possible, such as in the manufacturing process or in logistic chains. This allows for a much deeper insight in these processes; as for example damage or wear and tear to equipment can be detected and dealt with

[2] The previous waves of industrial innovation are the adaption of mechanization, mass production, and the introduction of computers and electronics (Greengard 2015).

instantly, or the usage of a certain product can be monitored from a central data-control point to, based on the immediate feedback of the data, further improve the product (ibid.).[3] This data in turn can then be used in combination with "big data" techniques to achieve greater oversight and insight in certain processes, and ultimately achieve greater efficiency, reduce costs and obtain greater profits (ibid).[4] So it is in its marriage with big data, but also cloud services, mobile technology and even social media that the IoT can achieve its full potential. As data can be generated, stored, aggregated and triangulated, all from multiple and different platforms, all with seemingly infinite possibilities and applications as it will in time encompass all industrial and increasingly also many social processes (ibid.).[5]

In China, the IoT-industry has already been well underway for a couple of years and all major ICT businesses such as Huawei, Alibaba, Xiaomi, Baidu, Tencent, ZTE; together with the three telecom providers China Unicom, China Telecom and China Mobile, are competing heavily to capture domestic and international markets. The IoT-market in China in 2015 was worth up to 750 billion RMB and accounted for 31% of the global total (ECNS 2016). These businesses all realize that the IoT, combined with technologies such as 5G mobile communications, cloud computing, big data analytics, and even virtual or augmented reality, could be the future of ICTs, and that the next big technological push may well come from one of the many research facilities in China (SCMP 2017). Businesses in industries as diverse as transportation, medicine, agriculture, military, social management, and public

[3] A famous example of this is the Rolls-Royce jet engines that are being monitored worldwide for their performance and behaviour and to implement predictive maintenance (Robinson 2016). Similar techniques are being used for oil-drilling equipment, freight trains … but also to track information of trees and even livestock like cows (Greengard 2015).

[4] It is however important to note that for many manufacturers, the IoT is not about "just the attaching of a sensor or chip to any product or any part of the production or customer usage process". What the IoT is enabling is a complete metamorphosis of the manufacturing industry towards a model of "servitization". In this businesses model, companies don't just sell products anymore, but they offer the product to be used by the customer as a service (Neely 2007). In this sense, Rolls-Royce stopped from selling jet engines to selling "power-by-the-hour" in which Rolls-Royce offers its customers the service of providing them with always-reliable power for it planes, as Rolls-Royce will constantly be monitoring the engine for predictive maintenance so the product is always in a state where it can function without errors (Neely 2013). But the same is happening for example in your future smart home: your smart fridge does not just want to warn you when you are in the shop that you should buy milk because you just finished your last pack this morning. No, perhaps the manufacturer of your smart fridge (or of your smart home in its totality) will maybe want to make a deal with the shop so they can automatically bring you your product and you never again run out of milk. By offering a service, not a product, the interests of the manufacturers and the customer are more aligned and this offers ways for companies to offer businesses services of higher value and thus move up the value chain (Baines et al. 2009).

[5] Atzori et al. (2010) identify four domains in which IoT-applications can be deployed: transportation and logistics, healthcare, smart environment (this includes the home, office and plant), and the personal and social domain. The applications really seem endless as basically every device can be made be part of the IoT by attaching a microprocessor to it.

security are implementing the technology;[6] but consumer goods such as wearables, smart home appliances and connected cars are also in increasingly high demand (GSMA 2015).

This great leap that China has made in the field of innovation and manufacturing, as the country now holds many leading technology businesses and research institutes, is part of an elaborate plan by the top government to transform the country into a “manufacturing superpower” over the coming decades (State Council 2015; Wübbeke et al. 2016). With a focus on “smart manufacturing”, things like the IoT, but also big data analytics, cloud computing, mobile technology, and the likes, are prone to become key for the Chinese industry and its economy as a whole. There are however some issues and potential pitfalls surrounding the IoT, which will continue to shape its implementation. I will firstly turn to these, in order to then give an overview of the adoption and development of ICTs in China in order to be able to assess how the IoT will be used in China and what then the possible impact will be on Chinese society and politics.

2.1. Security, surveillance, and countersurveillance in the IoT

Before the IoT can reach its full potential, there are still some issues to be resolved. In terms of technology, there is still work to be done in developing batteries for mobile devices that last longer, finding ways to embed sensors in everything from clothing to machinery, and developing standards and platforms to enable and maintain compatibility between devices, networks and data streams (Greengard 2015; Drake et al. 2016). But as the home, the office, and the entirety of the public domain become a sensor network that constantly collects information about individuals and possibly shares it with third parties, privacy also is a major concern for the IoT (Atzori et al. 2010). Especially since most of the IoT-devices will be controlled by other people, governments or businesses (Ziegeldorf et al. 2014).

The IoT’s greatest pitfall however is its low security standard. As became clear in two major cyberattacks in late 2016,[7] most of these devices connected to the internet are barely secured and also

[6] A good example of the sprawling IoT in China is the many security cameras being used throughout the country, mostly in cities (cf. Zeng 2016). But many other IoT-applications are still being developed and tested before being implemented more widely.

have no way to receive security updates or patches, and unlike computers, they are usually used for longer periods of time (Schneier 2016a).[8] As the IoT increasingly collects valuable data – from financial transactions or important businesses insiders to personal data, it can become a hot target for hackers, especially since it is known it is easy to hack. Moreover, every technology can be used for malicious purposes, but with the IoT, the impact into the physical world can be severe and even fatal as it involves applications such as driverless cars or drones that could be comprised by malicious actors (Greengard 2015).

Many scholars and instances have thus warned about the possible dangers of the IoT and the need for industry-led security standards (Goldstein 2016; Hamblen 2016; Schneier 2016; Drolet 2016). Also in Chinese official and technological discourse, the need to ensure "safe and controllable" (*anquan kekong*) IoT-products and services is stated as being of paramount importance; as it is noticed that "as far as implementation [of security measures in the domestic IoT] is concerned; compared to abroad, there is still a certain disparity" (CNITSEC 2017: 77).[9] Security in IoT is thus becoming an important driver for the Chinese IoT-policy and has e.g. already resulted in the international adoption of three security standards developed by Chinese researchers in the last two years (ibid.).

Still, with many issues of technology, security, and ethics still unresolved while the IoT-products and services are already being put on the market at an incremental pace, it remains to see how society will deal with these changes brought about by these devices (Sicari et al. 2015). As Howard (2015: 10) writes, "the latest smartphones, watches, and wearable technologies reveal how immersive and pervasive the internet of things will be."[10] Moreover, the internet and the devices we already

[7] On September 20 and October 20, 2016, respectively the site of cybersecurity expert Brian Krebs and Dyn, a Domain Name Service provider (an important piece of internet infrastructure as it "powers" many websites), were attacked by a botnet that was created through the Mirai malware. This malware infects poorly-secured IoT devices such as DVRs and internet-connected cameras to turn them into a "bot" that can be used to send data to a target. As enough bots do this, in a Distributed Denial-of-Service attack (DDOS), the target shuts down due to an overload of information that the site or server can't process, as happened in these two attacks (Krebs 2016; Williams 2016).

[8] According to Schneier (2016b), security for the IoT often is "an externality", as the buyer only cares about a cheap price and the manufacturer is pressured to put its products on the market as he probably is already on to developing newer and better secured models.

[9] An important reason that is given for this is the fact that most of the more advanced IoT-technology is controlled by foreign companies, which leaves Chinese IoT-production in a "backward position" with inferior and insecure technology (CNITSEC 2017: 77).

[10] A nice addition to this list of pervasive IoT-devices is connected sex toys. These devices collect a lot of intimate user data and many of them are very poorly secured (BBC 2017; CNET 2017).

connect to it now, as a result of severely transforming the way information and communication is being channeled, stored and processed, already enables what the leading internet security scholar calls "the golden age of surveillance [we are living in]" (Schneier 2015: 4).[11]

As many IoT-devices already make up an important part of people's daily lives (such as smart phones, but increasingly also other "networked devices") and thus are in fact increasingly managing our political, economic and cultural lives, control over these devices thus entails enormous power (Howard 2015). How will having even more devices connected to the internet impact the power relation between the state, big internet corporations and internet users in society? According to Howard (2015), this would possibly put more power to the already powerful actors in the internet-era, that is: the businesses who offer services and own your data, governments and political leaders with strong cyber capabilities, and capable hackers who can get access to valuable data.[12] But this is not a given. Howard (ibid.) also argues that this new infrastructure can be used by less-powerful actors to create own networks of people and information, which in turn can be used to for example advocate for better rights or protest against state or corporate actors by presenting own information of for example deteriorating quality of nature or government or corporate abuse. This way, because of their decentralized nature or advantages of scale, new digital media or infrastructure has already many times "caught elites off guard" (ibid: 58).

In the face of all these changes brought about by rapidly evolving technologies, how does the Chinese government cope with it? With the IoT technology and applications, the internet "will be [of] a different kind … : larger, more pervasive, and ubiquitous." (Howard 2015:11); could this mean an opportunity for the Chinese leadership, a threat, or both? I.e., in what different ways does the Chinese government engage with a technology such as the IoT? These are the questions I would like to answer. As the People's Republic of China has a record of controlling media and internet in the country to

[11] Not only can objects like smartphones track your location through GPS, smart-TVs and laptops listen in to what you are doing or watch you through a build-in camera, we willingly share all kinds of personal information on social media or disclose it to search engines, our email contacts, or in many other digital – and thus recorded – way. Even if we ourselves would not use social media or the internet, it is most likely that much of your personal information would end up on the internet anyway through other people's social media or blog postings (Schneier 2015; Zuboff 2015).

[12] For more on who holds power on the internet and thus has an important part in shaping, governing, and controlling the internet, its resources and its infrastructure cfr. Lessig (2006); Mueller (2010); Schiller (2014).

avoid any kind of social unrest, how will it then deal with the possibly very disruptive IoT? To be able to assess that, I will first give an overview of how ICTs have been adopted and developed in China.

3. ICTs in China: Building resilience

With the advent of the internet, many pundits in the West were celebrating what would be the end of many authoritarian regimes as information would spread freely and uncontested across borders and walls to "liberate" oppressed people by showing them how they are being oppressed and what freedom and opportunities awaits them if they manage to get rid of their shackles (Rutten 2009). The Chinese government recognized at an early stage the internet's potential for improving and accelerating its economy while also possibly posing the risk to "disrupt" society in a to the Chinese Communist Party (CCP) dangerous way (Creemers 2016). Therefore, the rapid development of its ICT infrastructure (with an explosive growth in its amount of internet users as a result), was followed relatively quickly by, e.g., crackdowns on social media, elaborate censorship mechanisms, and efforts to implement real-name registration systems to remove anonymity from the Web (Tsui 2003; MacKinnon 2011; Ng 2013). Through a diverse set of techniques, ranging from governmentality (controlling of flows), sovereignty (the application of national laws on cyberspace), to pure disciplinary (arrests and fines); control of this space was asserted (Foucault 2004/2007; Paltemaa and Vuori 2009).[13]

With the country holding the biggest number of internet users in the world and having developed a number of major players on the global ICT market (CNNIC 2016; Creemers 2016)[14], the Chinese internet is flourishing despite the controlling measures (Yang 2009). Moreover, the Communist Party seems confident to rely ever more on the internet as it is adamant in making "informatization" (*xinxihua*) the "main power driving the country's overall economic and social development" (Qu 2010), with the ultimate goal of becoming a "strong Internet power" (*wangluo qiangguo*) (Creemers 2016). Despite that many voices have claimed that China has reached "the

[13] Authoritarian regimes control measures on the internet or in which the internet is used are, as those of the CCP, often portrayed as creating an Orwellian nightmare of total control and surveillance (i.e., the state as "Big Brother"); while the internet as a Huxleyan, hedonistic entertainment-bonanza is often not accounted for (Morozov 2011). In the case of China, the power of the internet is thus used by the CCP both as a stick (in the form of censorship and ubiquitous surveillance) and a carrot (in the form of endless entertainment and new forms of propaganda through the many apps and platforms). Cf. Schneider 2016; (forthcoming).

[14] Its number of netizens surpassed that of the United States in 2008 and by June 2016, China had 710 million internet users. With 51.7% internet penetration, users may well continue to grow, especially in rural areas (CNNIC 2016).

tipping point" due to a number of factors such as protests emerging from inequalities caused by the market reforms, widespread corruption within the Party and state (Brødsgaard 2013), and also because of the presumed "liberating effect of the internet";[15] the CCP has so far proved very resilient in the face of these many challenges, and no break with one-party system or the current leadership seems due (Nathan 2003). Moreover, almost exactly like the adoption of a market economy – which was adopted only after making some strategic tweaks and balances – has seemed to make the Party stronger (Pieke 2016), so also by customizing the internet, the CCP could stay in control and make this new, seemingly omnipotent technology cater to its every need.

In what scholars have called "revolutionary authoritarianism" (Zhao 2008), "networked authoritarianism" (MacKinnon 2011) or "iDictatorship" (Austin 2014), the Chinese leadership aims for the appropriation of "the power of information technology to tackle the Party's key challenges in propaganda, public opinion and social management [for the purpose of] maintaining stability, ensuring Chinese Communist Party (CCP) dominance, preventing organized opposition and enhancing intra-Party discipline" (Creemers 2016: 4). By placing the internet (and technology in general) in the centre of an ambitious reform agenda (ibid.), the focus is very much on innovation to improve the government's governing capacity (People's Daily 2011).[16]

Due to the success of the (intended) commodification of technology by the Chinese leadership, and the fact that social, economic and political transactions now increasingly play out on the internet (Lu and Weber 2007); there is an enormous potential for the government to tap into all the data that is being generated on the internet (Creemers 2016). This could exponentially increase the grasp on Chinese society by the Chinese leadership in many ways: e.g., by using this data as a real-time, much more accurate set of statistics (ibid.), by surveilling the populous with elaborate CCTV networks and by tracking people's phones; all the way down to monitoring people's phone and internet usage (Zeng

[15] Perhaps rising discontent due to deteriorated air quality and environmental standards could now also be added to this list.

[16] In the 2011 18th Party Congress report, the term "social management" was used to replace "e-government" and by invoking "social management" the Party calls for governmental organs at all levels to innovate to "improve the online services and advocate healthy themes on the internet. … [S]trengthen social management of the internet and promote orderly network operations in accordance with laws and regulations. [And] crack down on pornography and illegal publications and resist vulgar trends" (quoted in Noesselt 2014: 456). According to Zeng (2016: 1452), "social management … refers to social control activities while downplaying its coercive connotations".

2016). All this would possibly allow the CCP to act timely and even pre-emptively to avoid or limit the damage of economic fall-outs, natural disasters, social unrest, or other disruptive events with the ultimate goal of creating “a predictable political environment” (Creemers 2016: 13).

3.1. The IoT: Changing the game

Most of the scholarship studying Chinese state action with regards to the internet has focussed on the web as constituting the social web, also called Web 2.0 (Creemers 2016). Web 2.0 consists of an internet of user-generated content, ease of use, and interoperability (DiNucci 1998). This has led to a flourishing of diverse applications such as social networking, blogs, crowd-sourcing, video-sharing, … , as it gave the possibility to anyone with an internet connection to “actively” contribute to the internet (ibid.).[17] Due to the success of many of these Web 2.0 applications in China and the following harshness of the government measures to counter online government criticism and mobilization, topics such as censorship, astroturfing, online feedback mechanisms have already been studied extensively.[18]

However, as the internet, through the IoT and other technologies, evolves from Web 2.0 to encompass all aspects of life, concerns also rise about the internet being used as a potent tool for surveillance and social management, for hacking and espionage, even up to sabotage and warfare. In the Chinese domestic context, Creemers (2016) has recently focused on how the CCP tends to use rapid evolving internet technology to “upgrade” its propaganda, public opinion work and social management, while Zeng (2016), focusing on Big Data, [19] has shown how this technology is used to greatly increase the state’s surveillance capabilities and could potentially also be used to monitor the

[17] This is in contrast to the “passive” consumption of Web 1.0 websites (DiNucci 1998).

[18] Cf. Ng (2013); King et al. (2013) on censorship, King et al. (2017) on astroturfing, Tsang (2009); He and Warren (2011) on government deliberative mechanisms using the internet, and Schlaeger and Jiang (2014) on government use of social media.

[19] As the development of big data was officially announced by the State Council of China in November 2015, thus making it into a national strategy (Creemers 2016); Zeng (2016: 1444) does argue that big data in China is not a uniform concept and is sometimes used as a catchphrase, so the approach of the Chinese government to big data “is best considered as a broad and less than coherent strategy of adaptation to governance by electronic means.”

opinions and ideological trends of students and soldiers – and adjust where necessary.[20] As intrusive as these matters may appear, it seems that the biggest obstacles for the Chinese leadership to implement these plans and more, are merely of a practical or technical nature as it does not lack the means and will to do so, and because civil society or awareness of civil rights is too weak to oppose it (Zeng 2016).[21]

However, these ambitious plans don't come without risks. Besides the security concerns of having increasing amounts of personal data stored and therefore increasing the danger of data breaches (as these servers or data centers will also become a hot target for foreign intelligence services and hackers) (ChinaFile 2016), Creemers (2016) also warns that as the government will be more aware of crimes or abuses, it will also be held more accountable for not acting on the information. Additionally, Zeng (2016: 1458) also warns for the potential danger of sensitive data (generated from people's internet usage or activities under surveillance) being used in internal Party strife, resulting in a possible "authoritarian backfire".

Also, as noted above, when it comes to securing the IoT, this remains a big difficulty. As more aspects of public life, the economy and critical infrastructure (such as power grids, banks, …) operate through ICTs, obtaining a higher level of cybersecurity becomes a matter of utmost importance and even national security. Security on the Chinese internet is already below standard due to the fragmented bureaucracy, the fact that many people use outdated and unsupported operating systems, and general public education is inadequate (Lindsay 2015). This causes much harm to the Chinese economy on a daily basis (ibid.).[22] So especially with a whole industry for connected devices in the make, proper security in these devices will be key for obtaining consumer's trust and fulfilling the government's plans of "informatization" (Creemers 2016).

[20] One article examined by Zeng (2016) even talks of ideological indoctrination in the fashion of the increasingly effective online advertisements (Hu and Huang 2014).

[21] Some of these plans can also prove to be too politically dangerous for parts of the Chinese leadership, as has happened with a pilot for the "Social Credit System", a modern version of the *dang'an* system that uses innovative technologies (such as social media, apps and big data) to rate citizens for "good" or "patriotic" behaviour online and offline (FT 2016). The criteria used for rating behaviour are politically controversial and often far-fetched, making it that there will be some hard political choices that will have to be made before a pervasive system like that can succeed (Economist 2016).

[22] Zhuge et al. (2012) estimate that the overall damage to the Chinese economy exceeded 5.36 billion RMB ($USD 0.852 billion) in 2011, affecting 110.8 million Chinese users (about 22 percent of all Chinese internet users at the time) and 1.1 million websites (or 20 percent of all Chinese websites at the time).

4. Methodology

With the Chinese leadership boasting such ambitions concerning the development of the internet and for using innovative means to increase its governing capacity, it is therefore relevant to look at government policy and policy recommendations to have an idea of how this technology-driven vision of good governance will materialize (Creemers 2016; Zeng 2016). The IoT, as it has been lauded by industry and government alike to being able to "read China" in unprecedented ways, will therefore be my focus of study. By looking at IoT-development policy in China, I want to find out how the CCP envisions using the IoT not only to generate economic growth but more importantly to increase its grasp on Chinese society in different ways. Therefore I will look at the main themes brought up in these documents and the concrete examples given where is stated how the IoT is to be used for e.g. improving social management, creating feedback mechanisms, and/or build better surveillance systems.

Moreover, as Chinese society becomes more reliant on internet-enabled systems and the Chinese leadership does too, the CCP is constantly trying to use innovative means of improving its governance capacity; cybersecurity becomes a crucial element in all these "informatization" plans – as without proper security many of the technologies and devices become useless or even dangerous. However, discussing cybersecurity policies of the IoT is goes beyond the scope of this thesis and will only be touched upon shortly where necessary. With these two elements; how the IoT is envisioned to be used for improving the governing capacity of the Chinese state, and how these plans should be secured, I argue that a successfully developed IoT on the terms of the CCP, could make the Chinese leadership possibly ever more resilient as it will have always increasingly accurate information on much more of the goings-on in Chinese society.

The scope of the study entails all the Chinese policy documents from the beginning of the policy on IoT-development in 2009 and the more general technology policy linked to the policy for the development of the IoT, until policies issued at the beginning of 2017 (around March). The general outline of the thesis will be as following: I will first give an overview on the general IoT-development policy in China to identify the main themes discussed in these documents in which the Chinese leadership wants to see the IoT developed and why. In the second part, I will elaborate on the more concrete usages of the IoT as discussed in these policy documents. More specifically, I will focus on these IoT-usages which could improve the Chinese government's social management and surveillance capabilites.[23]

For an overview of the used policy documents and speeches, see table 1 in the appendix. Also, I included the documents used for analysis in the references for clarity.

[23] Following Rexhepi (2016), who argues that caring for surveillance is a "liberal luxury" that many people that have to struggle for food or survival on a daily basis or people who are used to many intrusive state (and corporate) surveillance schemes based on their low position in society, race, gender or religion; it is important to note that solely focussing on (state) surveillance from a Chinese perspective also risks of missing the wider power dynamics between state and society in Chinese society and the myriad of ways in which these dynamics take shape to reiterate the status quo (cf. Foucault 1988).

5. IoT-policy in China

Constituting such a promising new turn for industry, the IoT has thus been on the cross hairs of Chinese policy makers for some time. The recipe for IoT development has remained the same as it goes for other new ICTs such as big data, cloud computing, and mobile internet; the development of IoT technology and services, and the creation of a "vanguard" of successful businesses capable of competing on international markets, is seen as a prerequisite for the IoT (together with symbiotic technologies such as the cloud and big data) to aid in the country's overall development and to help resolve a certain set of persistent issues in Chinese society (cf. Creemers 2016; Zeng 2016). However, due to the nature of the IoT, it is identified by Chinese policymakers as being particularly useful to help tackle some problems that big data or mobile computing alone are not designed to fix.

By going over policy documents related to the "informatization" agenda and to the IoT specifically, I will identify the main themes in IoT-policy to be able to gauge the Chinese leadership's ambitions concerning ICTs, and critically analyze these. First I will discuss the "guiding" policy, the policy which mostly comes from the high authority of the State Council and serves to lead to more detailed or practical documents issued by ministries or other government organs, as these documents always refer to these leading texts.

5.1. "Reading China": Setting the scope for IoT-development

The IoT was recognized in premier Li Keqiang's 2015 Government Work rapport as being a vital part of the country's ambition of making the country into a "strong internet power" (*wangluo qiangguo*), together with mobile internet, big data and cloud computing.[24] This new turn in technology policy, which he coined "Internet Plus", was set out in an elaborate implementation plan to ensure these information technologies are being leveraged to achieve stable economic growth and development for the country as a whole.[25]

[24] State Council, '2015 nian zhengfu gongzuo baogao' (2015 Government Work Report), March 5, 2015.

[25] State Council, "Guanyu jiji tuijin 'Hulianwang+' xingdong de zhidao yijian" (Guiding Opinions Concerning

These policies however were already long in the making. On August 7, 2009, on his third inspection trip to Jiangsu province, former premier Wen Jiabao visited the Wuxi Hi-Tech Micro nano SensingNet R&D Center of Chinese Academy of Science (中科院无锡高新微纳传感网工程技术研发中心), a research center for IoT-technology which was founded the previous year in November. Once there, Wen called for the "speedy establishment of China's information sensing center, or by a different name: the 'Reading China' Center" (*'Ganzhi Zhongguo' zhongxin*).[26] From that year on, the city of Wuxi, and more specifically its industrial park Wuxi New Area (*Wuxi xin qu*), was transformed to become a "sensing net model city" (*chaunganwang shifan chengshi*) with the ambition of becoming China's and the world's top IoT innovation hub.[27]

In an official reply to the Ministry of Industry and Information Technology (MIIT) in 2012, the State Council formally ratified the plan to develop the "Wuxi National Sensing Net Innovation Model Area" (锡国家传感网创新示范区).[28] In it, the State Council calls upon the MIIT to work together with the provincial government to make Wuxi into a success. In the elaborate MIIT "Development Plan Outline" for the Wuxi Area, the precise conditions and "guiding principles" of Wuxi's development are given, as is a fairly detailed "development target" with the necessary tasks and most important areas in which the IoT should be developed.[29]

The Outline identifies the "sensing net" (as a synonym for the IoT), as a "high-end technology with comprehensive usage" and a "piece of important substance of the strategic new industry". Moreover, it positions the IoT's strategic importance in a post-financial crisis world in which the developed countries (the United States, Europe and Japan) have a strong competitive advantage in

Vigorously Promoting "Internet Plus" Activities), July 5, 2015. Translation available at: https://chinacopyrightandmedia.wordpress.com/2015/07/01/state-council-guiding-opinions-concerning-vigorously-moving-forward-the-internet-plus-plan/ (accessed 11/06/2017).

[26] 'Wen Jiabao: jinkuai jianli Zhongguo chuangan xinxi zhongxin' (Wen Jiabao: speedy establishment of China's information sensing center), *Xinhua*, August 5, 2010. Available at: http://news.xinhuanet.com/eworld/2010-08/05/c_12412927.htm (accessed 11/06/2017).

[27] Mei Fangquan, 'Zhihui diqiu yu ganzhi zhongguo – wulianwang de fazhan fenxi' (Smart Earth and Reading China - Analysis on Development of Internet of Things), *Agricultural Internet Information*, vol. 12, 2009, pp. 5-21.

[28] State Council, 'Guanyu Wuxi guojia chuanganwang chuangxin shifanqu fazhan guihua gangyao (2012-2020) nian de pifu' (Official Reply Concerning the Wuxi National Sensing Net Innovation Model Area Development Plan Outline (2012-2020)), August 5, 2012.

[29] Ministry of Industry and Information Technology, 'Wuxi guojia chuanganwang chuangxin shifanqu fazhan guihua gangyao (2012-2020) nian' (Wuxi National Sensing Net Innovation Model Area Development Plan Outline (2012-2020), August 17, 2012.

terms of IoT usability and industry development. By doing so, it legitimizes China to, from its acknowledged relatively weak position, try to close the gap with these countries and create a set of internationally-renowned IoT businesses itself. As far as the Wuxi Area is concerned, this approach seems to already be proving successful with the private sector gladly taking advantage of the favorable conditions set up by the state. Reportedly, close to two thousand IoT-businesses have settled in the Area and the industry worth exceeded 150 billion yuan in 2017.[30]

The vigor of the Outline resembles that of a State Council document issued in 2010, about a year after Wen's visit at Wuxi. The document, entitled "Decision on Accelerating the Fostering and Development of Strategic Emerging Industries", seeks to build on the success of the then more than 30 years' rapid development since the reform and opening-up policy was adopted and aims to further tackle "major problems" such as "a weak enterprise technology innovation capability, few controlled key and core technologies, incomplete policy and regulation systems facilitating the market access of new technologies and new products; and imperfect investment, financing, fiscal and taxation policies, systems and mechanisms supporting innovation and venture capital.".[31] Many of the more practical IoT-development policy documents that will be discussed in next section refer to this document.

By indicating the strategic importance of the IoT and other technologies, which was enforced in the following year in the "Twelfth Five-Year Plan", the development of these technologies is set up as one of the most important goals for the nation as a whole.[32] The importance and urgency in calling for the development of these "new generation information technology industries", is then a direct forerunner of later technology policy such as the "Internet Plus" agenda or the "National Informatization Development Strategy" which aim to make these technologies as the core of Chinese economy and society. In doing so, it acknowledges the dire need for further economic development as China's economy is starting to struggle to keep up with its former growth rates, and that this growth is

[30] Wuxi New Area Investment, '2017 shijie wulianwang bolanhui yi zai jin luo mi gu choubei' (The 2017 World IoT Fair is already starting Preparations), February 7, 2017. http://cn.bizwnd.gov.cn/2017-02/07/c_50197.htm (accessed 11/06/2017).

[31] State Council, 'Guanyu jiakuai peiyu he fazhan zhanlüexing xinxing chanye de jueding' (Decision of the State Council on Accelerating the Fostering and Development of Strategic Emerging Industries), October 10, 2010. Translation available at: http://en.pkulaw.cn/display.aspx?cgid=139218&lib=law (accessed 11/06/2017).

[32] National People's Congress, 'Di shier ge wunianguihua gangyao' (Twelfth Five-Year Guideline), March 14, 2011.

most likely to be obtained by applying ever more advanced technologies in the country's economy, thus making these technologies of the uttermost strategic significance.

The Wuxi document published by the MIIT already outlines the broad scope of possible IoT applications in which the government has strong interest to see the technology developed. Through its pragmatic nature of not only identifying these key fields of usage for IoT, but also how to achieve successes in them, the document already much so sets the tone for later, more specific IoT development policy, which will be discussed in the next section.

The three main areas identified for IoT-development are industrial processes concerned with manufacturing, storage and logistics, to improve management and safety; improving management capabilities and safety measures for government facilities; and making improvements in the field of social management and public service. The second, with its "quick-response capabilities to sudden incidents and environment monitoring and protection capabilities", does not sound very innocuous in the hands of an authoritarian regime, if these capabilities would be used to control and limit the actions of individuals or groups. As Zeng (2016: 1452) points out the "coercive connotations" of "social management" in China, it remains to be seen in what way it is stated more clearly in these documents how exactly the IoT is envisioned to be used for this.

Further in the document are these three main areas distilled in "eight big usage model constructions" which give a clearer view of what is included in the three main areas and what the most important issues are in IoT development according to the CCP. These eight categories are: manufacturing, electric power, logistics, traffic, public security, environmental protection, medical treatment, and house appliances. The eight categories already show that plans are to use IoT-technology in all facets of industry, but also much of public life and into people's private lives. This comprehensive plan shows how a "smart" city model like this could leave little of public life (through e.g. smart traffic and ubiquitous cameras and sensors), and parts of private life (through e.g. smart home devices), undocumented and possibly unregulated.

Among the specific applications are described: using the electric grid for monitoring with data from smart meters as entrance point or using "high towers for emergency relief", surveillance mechanisms covering focal areas to "prevent intrusions" and improve city's public management, to creating a public security platform for surveillance, early warnings and emergency relief; using smart home appliances to improve the quality of life for families, their safety, informatization, and energy reduction, and this up onto the level of the community.

The example from the "electric power" section does specify further in the section that the monitoring, which should occur in a centralized manner, is to ensure the "safety, stability and reliability of the smart electric net". As in the other cases, the schemes described here do not have any inherent malign intent (to for example stating to want to create a totalitarian "*1984"*-like state) but are made to serve common ends of e.g. public service or state building, such as using this technology to tackle pollution or flooding, or prevent people from breaking into your house. Still, the same or similar schemes could also be used to closer monitor people's actions and prevent them from criticizing the government or mobilize to stage a protest. It is therefore important to be wary of such elaborate schemes as the data generated by this technology or the surveillance capabilities that it allows for, can always be used for other purposes as e.g. targeting and silencing opposition to the state.[33]

The document also requires all technology to be of a certain standard, to be "manageable and controllable" (*keguan kekong*) and is very specific on the different areas of IoT it seeks to cover. Moreover, compatibility between systems and devices (meaning they use compatible standards) and data processing (in the form of big data analysis, real-time data banks, and smart analysis and decision-making) are also stated of being key to a successful IoT development.

An important goal of the policy is to create "significant model example constructions" which can then be exported to different localities and also be successful there so that the demanded "increase in spreading efforts" is obtained. To assure the success of the policy, the document also asks for the establishment of a national-level IoT science & technology university campus in Wuxi, as also to set up a coordinating small leading group that can complement this document with more specific policy to ensure a successful development of the Wuxi Area.

[33] I choose these examples as they make for the most recognizable cases of possible privacy infringements. But with the whole environment turning into a "smart" environment, issues of ubiquitous data aggregation and possible damaging uses of data analytics (e.g. in the form of inhibiting freedoms or reaffirming existing biases), obviously span much wider and also include e.g. smart vehicles and smart medical equipment (cf. Boyd and Crawford 2012; O'Neil 2016).

Approximately half a year after the Wuxi documents, the missing, more comprehensive ideological guidance is then provided for in the "Guiding Opinions of the State Council on Promoting the Orderly and Healthy Development of the Internet of Things", published by the State Council.[34] In this top-level document, the high demand for IoT-development is set out, as the technology is said to possess the "characteristics of having strong permeability, driving on a wide field of usage, and having good all-around benefits". According to the document, the IoT is of strategic importance for improving the level of informatization of the Chinese economy and society, and it is "beneficial to the advancement of the change in orientation in style of production, living and social management towards smartization, refinement and internetization". These are terms that will reappear in many of the more practical development policy documents discussed in the next section.

The IoT's strategic importance is underscored in this document as it is stated that, besides it being vital for the informatization of Chinese economy and society (as was already mentioned in the 2010 State Council document), it is also crucial for the "deepening of military-civil integration" (*junmin ronghe*) and even for the construction of national defense, as is mentioned in respectively the "guiding thought" and "basis principles" of the document. This is further reinforced with the "safeguarding measure" of "setting up robust IoT development coordinating mechanisms between ministries, industries, regions, and the army".

The document also stands out for the importance placed on the need for innovating in social management, but does not elaborate on what that actually entails. It does however says that the to be constructed "smartizised" social management and public service systems should be "highly effective, safe and reliable" (*anquan kekao*). This is slightly different from the important "basic principle" in the text of "safe and controllable" (*anquan kekong*), which comes as a strong prerequisite as China is transforming into an information society which depends on the reliability of its technology. As a "safeguarding measure", it is stated that information security, together with privacy protection, should be improved by setting up laws and regulations.

[34] State Council, 'Guanyu tuijin wulianwang youxu jiankang fazhan de zhidao yijian' (Guiding Opinions Concerning Promoting the Orderly and Healthy Development of the Internet of Things), February 5, 2013.

The goal is set out to “create a batch of core technology, build an early form of an IoT industry system, and have a clear increase in safety guarantee capabilities.” by 2015. But the real importance of the document is that it sets out the general conditions for IoT-development in terms of crucial application areas, tasks and principles. By doing so, it sets the tone for the more practical IoT-development policy that follows this one. The calls in the document’s “safeguarding measures”-section are also very emblematic for the policy to come, which will be discussed in next section, as it states to “speedily set up concrete implementation plans”.[35]

The last of the top-level guidance for the IoT concerns the content of a meeting held on February 18, 2014 in Beijing on the auspices of the State Council, called the “Nationwide Internet of Things Work Television Conference Call Meeting” (*quanguo wulianwang gongzuo dianshi dianhua huiyi*), which was broadcasted on national television.[36] The content of the meeting is later referred to as the “Spirit of the Nationwide Internet of Things Work Television Conference Call Meeting” (*quanguo wulianwang gongzuo dianshi dianhua huiyi jingshen*) in many more practical policy documents on IoT, as they should act in accordance with that “Spirit”.

The later published draft of the meeting includes summaries of the speeches of the important officials and industry leaders who spoke at the meeting, e.g. the mayors of Shenzhen and Wuxi who both call for the further development of the IoT in their region, and the speech of vice premier Ma Kai, which is of most importance. The deputy director of the National Development and Reform Commission (NDRC) Zhang Xiaoqiang gave a report in which he emphasized the “five plans to be stressed for IoT development”. Those are: coordination between key sectors, the coordination of the relation between development and safety, focus on local development, the coordination of resource sharing, and the coordination of “military-civil integration” development.[37]

Ma Kai in his speech very much emphasized using the IoT, not only for the purpose of obtaining steady growth and increasing the country’s competitiveness, but also very much for

[35] The Wuxi Development Plan Outline also counts to that, as it’s more concrete envisioned IoT-applications for development were discussed above. But still it is also an important document to “guide” following IoT-policy as it was the first comprehensive plan and because of the importance of the Wuxi Area in the whole national IoT-development effort.

[36] ‘Quanguo wulianwang gongzuo dianshi dianhua huiyi geji lingdao jianghua zhengligao’ (Nationwide Internet of Things Work Television Conference Call Speech Draft), June 24, 2014. Available at: http://www.wendangku.net/doc/4f092eea1a37f111f1855bbd.html (accessed 11/06/2017)

[37] Ibid.

improving social management capabilities. He stated: “The second point is [the IoT] should benefit safeguarding and improving people’s livelihoods. In a broad application in the fields of education, medicine, hygiene, social safeguards, community service, managing government affairs, etc., the IoT should deepen the transformation of social management, public service and human life; bring about innovation in the model of social management and public service; to largely increase the effectiveness and level of public service; to drive the improvement in public service; and to better fulfil the needs of the masses.” He also quotes chairman Xi: “Let IoT better drive production, enter life, and create happiness for the ordinary people.” He also stressed developing the IoT in the face of its poor security that still needs tackling, and the policy and legal system which is still not robust.[38]

5.2. IoT and Informatization

In these documents, the core requirements of IoT development in China and how to achieve these is laid out in a comprehensive big picture complementary to the wider “informatization” plans, as for example also laid out in the “Internet Plus” agenda. The central element in these plans for IoT-development is the strategic importance of the IoT for economic purposes. Flowing from this is the social use (in the form of improved social management and public service) of the technology and to have the security mechanisms in place to safeguard an economy and society which is regulated for a big part through vulnerable technology and hardware. Therefore, the emphasis on local pilot projects which, on the basis of “try-first” (*xianxing xianshi*), should gather experience to be used in other localities. This way, the wider plans of “informatization” can be accomplished. By making everything “smart”, the legibility of society improves significantly, making it possible to “read China” in unprecedented ways and thus gain much more control over society.

By positioning the IoT as a promise able to generate “stable growth” after the financial crisis (as stated in the 2010 State Council document), the IoT also becomes critical to the other goals of the Chinese leadership. With the IoT functioning as a new “pole of profitable growth” in today’s economy

[38] Ma Kai: Zai quanguo wulianwang gongzuo dianshi dianhua huiyi shang de jianghua (Ma Kai: Speech at the Nationwide Internet of Things Work Television Conference Call Meeting), February 18, 2014. Available at: https://wenku.baidu.com/view/0885947933687e21ae45a90c.html (accessed 11/06/2017)

(Schiller 2014: 146), its anticipated commodified success thus has the potential to make the IoT (in combination with big data analytics and other new technologies) function as a new “scopic regime” which could have the potential to give the leadership much more power viz-à-viz its datafied subjects (Scott 1998; Cetina 2016).

The envisioned scope for the IoT is therefore very wide, even all-encompassing; as it is said to involve all industry, society and also the realms of people’s homes. There were little concrete examples mentioned in the documents discussed here, but the examples given in the Wuxi document show already a bit more of the intentions and their possible implementations for the Chinese government’s IoT-plans. Such as: using the electric grid (including smart meters) for monitoring, elaborate surveillance mechanisms in “focal areas” and systems for early warnings and emergency relief, having more smart devices in the home. These examples on itself may perhaps not say much[39] but in the bigger scheme of things, i.e. China’s “informatization” plans, if we combine this information with the more recent, more comprehensive Chinese cyber policy, we get a more accurate picture in which to scrutinize these IoT-applications.

For instance, the mentioning of military-civil integration in the 2013 State Council document on IoT Development from then onwards also applies to other IoT related policy, such as for the whole Wuxi area. But it also has to be seen in the wider context of the Chinese military increasingly embracing digital technologies, as is mentioned in the National Informatization Development Strategy from 2016, which talks of “Accelerating a strong information army, building a modern military forces system” as one of the Informatization goals.[40] Similarly, the recent focus on social management in Chinese technology policy is difficult to gauge without also e.g. mentioning the recent attempts for setting up a Social Credit System. These schemes thrive on the collecting of as much data as possible, of both online and offline processes, and sharing it between government institutions and industry. The importance for sharing data between different ministries, businesses, localities and even the military is

[39] Although there has been already much opposition against many of these practices by privacy advocates, including against for example smart meters, but definitely of course ubiquitous CCTV networks and smart home devices. Cf. Cuijpers and Koops 2011; Lyon 2001; Ziegeldorf et al. 2014.

[40] Cyberspace Administration of China, ‘Guojia xinxihua fazhan zhanlüe gangyao’ (Outline of the National Informatization Development Strategy), July 27, 2016. Translation available at: https://chinacopyrightandmedia.wordpress.com/2016/07/27/outline-of-the-national-informatization-development-strategy/ (accessed 11/06/2017)

expressed in almost all documents discussed above. The recent '"13th Five-Year Plan" for National Informatization' talks of the plan of "Building data centres covering the entire country, linked together smoothly. … [which will be] bringing together three kinds of data, from netizens, enterprises and governments, [with the aim of] rais[ing] the timeliness, completeness and accuracy of information." [41]

Still, apart from some examples given in the Wuxi Document which only show limited details of the plans, the actual scope or nature of many of the sought-for IoT applications, and how exactly they will fit in the wider "informatizisation" plan, is still not very clear. Therefore, I will turn to the more practical IoT implementation policy documents in the next section in order to scrutinize concrete cases of IoT-usage as described in these documents.

5.3. Implementing "Reading China": Spreading models

From the start of the Chinese IoT-policy in around 2009 until the moment of study, I count five documents which I consider being part of the more practical IoT-development policy. Often laying out precise development plans, with certain deadlines and the required means and measures of how to get there, these plans are mostly being published by the MIIT and the NDRC. In this section I will discuss the examples given in these plans in order to be able to scrutinize what exactly these plans of e.g. "improving social management and public service" or other seemingly intrusive schemes are in which the IoT is to be used.

The first document to set the tone is the "Notice Concerning the Printing and Distributing of the "Internet of Things 'Twelfth Five-Year Plan' Development Plan", issued by MIIT in 2011.[42] The document refers to the "Twelfth Five-Year Plan" and the "Decision on Accelerating the Fostering and Development of Strategic Emerging Industries", and thus also calls the IoT a "strategic and rising new industry, which has an important use in the accelerated promoting of transforming the way of economic development."

[41] State Council, 'Guanyu "shisanwu" guojia xinxihua guihua de tongzhi' ("13th Five-Year Plan" for National Informatization), December 27, 2016.

[42] Ministry of Industry and Information Technology, 'Guanyu yinfa "wulianwang "shierwu" fazhan guihua" de tongzhi' (Notice Concerning the Printing and Distributing of the "Internet of Things 'Twelfth Five-Year Plan' Development Plan), November 28, 2011.

The focus of the document is on which “core technologies” of the IoT are to be developed, the importance of the setting of international technical standards, and how the IoT industry should further be developed. These goals are set out in more detail in separate “special columns”. The document does mention “social management” but offers no new information. There is one interesting passage in the section “Strengthening processing technology research” that shows the range of different data that will be available through different IoT-applications. It states to “Greatly support research suitable for storing and processing the great volume of IoT data, as well as data mining, smart image and video analysis technologies.”

The so-far most comprehensive policy document on IoT-development, is the “Notice on Print and Distribute 10 Internet of Things Development Special Action Plan” issued by multiple agencies in 2013.[43] As the Action Plan encompasses so many aspects of life and public police, that’s why it is being carried by such a wide range of organizations, including e.g. the Ministry of Education, the Ministry of Public Security, and of course the MIIT, but also many other governmental bodies as well as research institutes. The Plan comes with two attachments, of which the second one is very large and detailed on every topic related to IoT-development. The second attachment also includes a detailed list explaining which organizations are responsible for what topic or task exactly.

In the “Usage Promotion Special Action Plan (2013-2015)”-section, the wide range of areas in which IoT-technology and applications should be developed is restated, as well as the focal role the “Wuxi National Sensing Net Innovation Model Area” in the creation of pilot projects with “strong influence power”. These areas are laid out in the “Important tasks” and contain the following: the smartization of industrial production and management capabilities, the refinement of agricultural production and the management of produce distribution, the smartization and standardization of logistic management, the monitoring of pollution sources and the ecosystem, the monitoring and internetization of safety in production and supervising trends, traffic management and smartization of service, the smartization and refinement of resource management, irrigation information collection and processing, guarding public security and supervising trends, for use of hospital management and

[43] National Development and Reform Commission et al., ‘Guanyu yinfa 10 ge wulianwang fazhan zhuanxiang xingdong jihua de tongzhi’ (Notice Concerning the Printing and Distributing 10 Internet of Things Development Special Action Plan), September 5, 2013.

community medical and health services, the refinement of cities basic facilities management, and for use of smart home appliances.

This wide range of areas on closer look shows how all these areas are of great importance to China as they all deal with large and persistent issues in Chinese society, such as ensuring food and resource security (in a nation with so many mouths to feed and houses to provide electricity for etc.), tackling pollution (e.g. all the smog, flooding, and desertification which are major long term challenges for the country), and resolving persistent traffic problems (such as the many traffic jams in big cities). But others examples in these “tasks” are even more revealing. Such as the “guarding public security and supervising trends”, where the IoT is summoned to help deal with issues of food safety, which entails ensuring the quality of meat, vegetables, ingredients for Chinese medicine, alcohol and even baby milk powder. As there have been many food scandals in China which e.g. also involved baby milk powder and which caused a national uproar, the issue of ensuring food safety becomes important enough for Chinese policymakers to include it in these plans as to have some IoT-application help resolve it.

Other “tasks” are for the IoT to be used to “develop usage models for safeguarding important happenings and places, controlling the entirety of motor vehicles, managing the floating population, and for preventing and controlling and have an early warning system for the occurrence of sudden public incidents in the center of cities,”. What is described here are plenty of instances of monitoring and surveillance, which could possibly go as far as using this technology to create better ways of preventing people from taking to the streets to protest, as was also the case in documents discussed in the previous section.

The document also states which institutions have the main task of acting on each different task, as well as providing some extra information regarding the task. E.g., for the last case described here, it stated that the Ministry of Public Security should perform it, and should “as early basic work, set up two model constructions in 2014, to in 2015 start to gradually widen the model cases”. This is described for every separate task, so also for e.g. which institutions are charged with ensuring “military-civil integration”.

A notice published by the General Office of the NDRC in late 2013 offers little new insights into how precisely, and in what fields, the IoT should be further developed, but just rehashes the guiding policy as for it to be implemented correctly in the pilot projects that the NRDC aims to promote.[44] A joint notice published by the General Office of MIIT and the General Office of the Ministry of Finance (MOF) does provide some more insights as it, due to its technical nature, discusses many technologies and precise areas of IoT-usage.[45]

Besides the many technical details and standards, the document discusses a similar content as the "Notice on Print and Distribute 10 Internet of Things Development Special Action Plan"; such as IoT-applications for tackling pollution in the form of air and water quality meters, food safety measures, or medical aid where the IoT e.g. could be used for medical check-ups from a distance. Furthermore, it mentions other things such as telematics and telematics security, and "long-distance family safekeeping and guarding systems" which include IoT devices (such as a wristband) to track the location of the elderly and children.

All of the points that have already been put forward in many guiding documents discussed in the first section and some of the more concrete examples discussed in this section, are found in the notice "MIIT 2014 Internet of Things Work Main Points", published by the General Office of MIIT.[46] In the attachment it again gives an outline of all the important elements of IoT development, such as the importance of cooperation between ministries, industries, and the military (in the form of "military-civil integration"), which is explicitly stated to be necessary for the purpose of data sharing. Another key aspect that resurfaces in this text is the importance of pilot projects to test IoT-applications for certain uses so they may be used elsewhere, with Wuxi as a focal point for developing these pilots.

[44] National Development and Reform Commission General Office, 'Guanyu zuzhi kaizhan 2014-2016 nian guojia wulianwang zhongda yingyong shifan gongcheng quyu shidian gongzuo de tongzhi' (Notice concerning the Organizing and Launching of the 2014-2016 National Internet of Things Important Application Model Project Area Pilot Work), October 31, 2013.

[45] Ministry of Industry and Information Technology General Office and Ministry of Finance General Office, 'Guanyu zuohao 2014 nian wulianwang fazhan zhuanxiang zijin xiangmu shenbao gongzuo de tongzhi' (Notice Concerning the Proper Handling of the 2014 Internet of Things Development Special Fund Declaration), May 4, 2014.

[46] Ministry of Industry and Information Technology General Office, 'Guanyu yinfa "gongyehexinxihuabu 2014 nian wulianwang gongzuo yaodian" de tongzhi' (Notice Concerning the Printing and Distributing the "Ministry of Industry and Information Technology 2014 Internet of Things Work Main Points"), May 21, 2014.

Interesting is that in the section at the top of the document, where it outlines to which administrative units the document applies, the responsible department for industry and informatization of the Xinjiang Production and Construction Corps is mentioned separately, as is in some other of the documents discussed in this section. The only other separate mentioned entity is the Wuxi National Sensing Net Innovation Model Area. As the Wuxi area is used for the economic development, could the area in Xinjiang also be used for testing out some of these IoT applications, but than in a much different political context? Perhaps due to the volatile situation in Xinjiang, the IoT-devices and technologies used there have to do more with surveillance and crowd-control? This is nowhere stated in these documents but the IoT does allow for very advanced surveillance capabilities so it is important to note how these devices can be used in different circumstances and for what purposes.[47]

5.4. Improved governance through surveillance?

The examples given here, although few and not always very detailed, already show how the IoT is envisioned by Chinese policymakers to constitute a possibly large part of the solution of solving even “hard problems” such as the battle against pollution, food security (in the sense of providing enough food for the Chinese population), and persistent traffic congestion. Some of the applications mentioned in these documents however, such as the location-tracking for the elderly and children, look odd next to all the other issues which no doubt are of greater national concern. Nonetheless, through the setting up of elaborate policy and by pushing for pilot projects to be tried and tested in many areas, the state is very involved in the calling for development of the IoT as it is of such strategic importance to it.

Other examples in some of these texts show a glimpse of what could be the other side of possibilities afforded by these technologies, and in which could thus also be of interest to the state. E.g. what is described in the “Special Action Plan” of 2013 constitute plenty of instances of far-reaching

[47] This is only speculation but the Xinjiang Production and Construction Corps is known for its crucial role in the sinification of Xinjiang and could therefore operate as a base for testing new techniques of surveillance and control (cf. McMillen 1981; Seymour 2000; Zenz and Leibold 2017). Recently, it has gotten involved in the “Belt Road Initiative” to aid agricultural and technological development in neighboring countries such as Pakistan and Tajikistan (FT 2017; Xinhua 2017).

monitoring and surveillance capabilities. Such as the above mentioned “models for safeguarding important happenings and places, controlling the entirety of motor vehicles, managing the floating population, and for preventing and controlling and have an early warning system for the occurrence of sudden public incidents in the center of cities,” If more devices and vehicles get connected to the internet, the monitoring of individuals and larger groups will soon be in reach, and Chinese policymakers are aiming to be able to have these capabilities.

As Zeng (2016) has described, the Chinese government already constructed one of the most expensive and sophisticated closed-circuit television (CCTV) networks on the planet, consisting of millions of panoramic cameras in public spaces working 24 hours a day, seven days a week, covering highways, public parks, public transport and taxis, lifts and public streets.[48] Moreover, as early as 2011, the government could track the precise movement of 17 million people in Beijing using the signal of these people’s phones (Cheng 2014). When using phones, surveillance cameras, these devices all already constitute the IoT. However, as the amount of devices each person owns increases, or more cameras are build, or by “smartification” in general; many other mundane processes will also record and monitor people’s activities more closely.

Therefore, the Chinese government is doing good work to keep up with these developments and to try to use these opportunities to its advantage. E.g., in the “Notice Concerning the Printing and Distributing of the “Internet of Things ‘Twelfth Five-Year Plan” Development Plan” the call is made for developing better techniques of IoT data storage and processing and data mining, smart image and video analysis technologies. These are all technologies that are crucial in a “smart world” where everything is being datafied and recorded. If we combine these plans with other plans mentioned in more recent technology policy, the picture gets clearer yet again. E.g. in the “artificial intelligence” section of the “Internet Plus” plan is mentioned: “Support security protection enterprises to launch cooperation with Internet enterprises to develop and popularize accurate image recognition and other

[48] The government even boasts that in Beijing, thanks to at least 30 million cameras and the participation of 4,000 police, they manage to monitor 100 per cent of public streets (Zhang 2015). That is, if the pollution does not get in the way (Hall 2013).

such big data analysis technologies, and enhance the intelligence and service levels of security protection products."[49]

With techniques such as advanced image recognition (of which facial recognition is an important part) that get better every year, there will be no more hiding your identity, as it will be possible to be identified (and have your actions recorded) almost everywhere where there will be a camera or sensor.[50] Facial recognition is already being used in train stations in China to check if people's tickets match the person,[51] or soon it will be possible to pay by just showing your face.[52] Speech recognition is already being used to identify criminals using phone scams, but this technology can of course also be used to identify basically anyone using their voice.[53]

All these possible avenues for monitoring and surveillance, from the more economic-motivated ones to the ones described here, all show how there exists an irresistible urge within the Chinese leadership to try to control its environment more, with the aim of obtaining better governance capabilities in every sense. But what "better governance" means, is only determined by the Party itself.

It remains to be seen if these technologies really would allow for such great control-mechanisms, but they definitely can already make a big change in people's behavior. If your identity is not even safe by using your voice or showing your face somewhere, all these schemes are prone to having very chilling effects on people's sense of freedom to express themselves or take part in any kind of association or activity. Moreover, there are real dangers associated with relying ever more on digital technology, as technology and devices can malfunction, be short of energy supply, or be hacked to steal its information or be tampered with. Moreover, the danger of using biometrics is that once people's accounts or information linked to their face, voice or fingerprint is leaked or stolen, it is near

[49] State Council, "'Hulianwang+' xingdong".
[50] Of course, many other actions already make it easy to identify a person, such as credit card records etc. (cf. Schneier 2015).
[51] "Face recognition ticket checking comes to Beijing West Railway Station" China Daily, November 30, 2016. http://usa.chinadaily.com.cn/china/2016-11/30/content_27529029.htm (accessed 11/06/2017).
[52] "Face-detecting systems in China now authorize payments, provide access to facilities, and track down criminals. Will other countries follow?", MIT Technology Review. https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/ (accessed 11/06/2017).
[53] "Minitrue: "Voiceprint Analysis Can Recognize Swindlers"" China Digital Times, February 28, 2017. http://chinadigitaltimes.net/2017/02/minitrue-delete-article-voiceprint-analysis-can-recognize-swindlers/ (accessed 11/06/2017).

impossible to change your biometrics to prevent harm being done to your person or information.[54] Crucial to the government's plans of "informatization" therefore is the need for reliable and "controllable" systems, of which proper security is the most important trait.

[54] "The end of passwords: biometrics are coming but do risks outweigh benefits?" The Guardian. December 8, 2015. https://www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits (Accessed 11/06/2017)

6. Conclusion

The IoT, as a promising new turn in the ICTs-landscape, could potentially transform many economic and societal processes previously not connected or recorded by internet connection. As China is putting such great emphasis on using the power of ICTs to develop its economy and society, the IoT is just the next logical step on its path of modernization. In the policy-documents analyzed here, the strategic importance of the IoT is clearly stated as it is being summoned to transform anything from manufacturing to medical care and government services. With the IoT and related technology (such as big data, the cloud, mobile technology and data storage) rapidly developing, the ambitions of the Chinese leadership embodied in these documents, is to follow, or even lead these trends and use these technologies to increase its grasp over, it seems, as much as possible of all economic and social processes.

These documents show the wide scope of envisioned IoT-applications, as they range from schemes to increase the state’s grasp on much of the population through manifold surveillance systems, to schemes to tackle quite specific and persistent problems in China today, such as food safety and pollution. Military-civil integration is also stated as an important requisite for IoT-development, showing that the Chinese state is very serious about its very elaborate plans of “informatization”. Ultimately, the goal seems to be to create a predictable environment where the state will never be surprised by sudden bursts of discontent, mass mobilization, or economic turmoil. As successful models of using IoT for the purposes of creating feedback and surveillance spread to the whole of China; by controlling all the information through the networks of cameras, sensors and other data points, the central leadership will be in a much better position to act on this information and increase its governing capacity – if these plans will be implemented successfully that is.

These plans however are not without risks. As the state becomes more reliant on this data, it, together with the technology, will have to prove trustworthy to not give a skewed representation of reality. Moreover, the ability to ensure the security of these systems will become paramount as everything becomes connected and many vulnerabilities and technical issues still persevere – especially with the still developing IoT. Therefore, the recent turn towards improved cybersecurity in

Chinese policy is already noteworthy but more specific action on IoT-security is still mostly lacking. This is due to change in the near future: with many efforts recently being made to implement a comprehensive, holistic cybersecurity policy effort, more specific IoT-security policy is sure to also come. This could give much food for further research, but unfortunately fell out of the scope of this thesis.

This study has shown the importance of studying Chinese technology policy documents in the face of the great ambitions of the Chinese top leadership to become the world's leading innovator and information society, and as new technology catches up much faster with solid scholarship. However, only studying policy documents only shows part of the picture of a quickly developing nation and economy. Therefore, it is important to complement these studies with proper case studies and work on the ground to see the actual implementation of these plans. In doing so, more light can be shed on the role of the private sector in making the myriad plans of "informatization" a success, and to which extent it works together with the government in mutual interest.

7. Appendix

General policy documents

IoT-specific policy documents

Date of publication	Policy document	Releasing institution
10/10/2010	*Decision on Accelerating the Fostering and Development of Strategic Emerging Industries (关于加快培育和发展战略性新兴产业的决定)*	State Council
14/03/2011	Twelfth Five-Year Guideline (第十二个五年规划纲要)	National People’s Congress
28/11/2011	Notice Concerning the Printing and Distributing of the “Internet of Things ‘Twelfth Five-Year Plan’ Development Plan (关于印发《物联网“十二五”发展规划》的通知)	MIIT
5/08/2012	Official Reply Concerning the Wuxi National Sensing Net Innovation Model Area Development Plan Outline (2012-2020) (关于无锡国家传感网创新示范区发展规划纲要（2012-2020年）的批复)	State Council
17/08/2012	Wuxi National Sensing Net Innovation Model Area Development Plan Outline (2012-2020) (无锡国家传感网创新示范区发展规划纲要（2012-2020年）)	MIIT
5/02/2013	Guiding Opinions Concerning Promoting the Orderly and Healthy Development of the Internet of Things (关于推进物联网有序健康发展的指导意见)	State Council
5/09/2013	Notice on the Printing and Distributing 10 Internet of Things Development Special Action Plan (关于印发10个无联网发展专项行动计划的通知)	NDRC, MIIT, MOE, MOST, MPS, MOF, MLR, MOC, …
31/10/2013	Notice concerning the Organizing and Launching of the 2014-2016 National Internet of Things Important Application Model Project Area Pilot Work (关于组织开展2014-2016年国家物联网重大应用示范工程区域试点工作的通知)	NDRC
4/05/2014	Notice Concerning the Proper Handling of the 2014 Internet of Things Development Special Fund Declaration (关于做好2014年物联网发展专项资金项目申报工作的通知)	MIIT, MOF
21/05/2014	Notice Concerning the Printing and Distributing the “Ministry of Industry and Information Technology 2014 Internet of Things Work Main Points” (关于印发《工业和信息化部2014年物联网工作要点》的通知)	MIIT
24/06/2014	Nationwide Internet of Things Work Television Conference Call Speech Draft (全国物联网工作电视电话会议各级领导讲话整理稿)	State Council
5/03/2015	*2015 Government Work Report (2015年政府工作报告)*	State Council
5/07/2015	*Guiding Opinions Concerning Vigorously Promoting*	State Council

	“Internet Plus” Activities (关于积极推进“互联网+”行动的指导意见)	
27/07/2016	*Outline of the National Informatization Development Strategy (国家信息化发展战略纲要)*	CAC
27/12/2016	*"13th Five-Year Plan" for National Informatization (“十三五”国家信息化规划)*	State Council

8. Bibliography

Austin, G. (2014). *Cyber Policy in China*. Cambridge: Polity Press.

Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: a Survey. *Computer Networks*. 54: 15, pp. 2787-2805.

Baines, T.S., Lightfoot, H.W., Benedettini, O., Kay, J.M. (2009). The servitization of manufacturing: A review of literature and reflection on future challenges. *Journal of Manufacturing Technology Management*. 20:5 , pp. 547-567.

BBC. "Can a sex toy spy on you?" March 17, 2017. Accessed 11/06/2017.
http://www.bbc.com/news/world-us-canada-39280941

Boyd, D. and K. Crawford (2012). Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*. 15: 5, pp. 662-679.

Brødsgaard, Kjeld Erik. (2013) Chinese Studies and Beyond. *Asian Studies*. 59: 3-4, pp. 33-49.

Bruce, R. , S. Dynes , H. Brechbuhl , B. Brown , E. Goetz , P. Verhoest (2005). *International policy framework for protecting critical information infrastructure: A discussion paper outlining key policy issues* (TNO report 33680). Delft: TNO.

Cetina, K.K. (2016). "What if the Screens Went Black? The Coming of Software Agents" In Introna, L., Kavanagh, D., Kelly, S., Orlikowski, W., and S. Scott. *Beyond Interpretivism? New Encounters with Technology and Organization*. Working Conference on Information Systems and Organizations, Dublin, Ireland, December 9-10, 2016.

Cheng, J. (2014). "Big data for development in China, UNDP China working paper." Accessed 11/06/2017.
http://www.cn.undp.org/content/dam/china/docs/Publications/UNDP%20Working%20Paper_Big%20Data%20for%20Development%20in%20China_Nov%202014.pdf.

ChinaFile. "Is Big Data Increasing Beijing's Capacity for Control?" August 10, 2016. Accessed 11/06/2017. https://www.chinafile.com/conversation/Is-Big-Data-Increasing-Beijing-Capacity-Control%3F#sthash.xBE72CC2.dpuf

China Internet Network Information Center, *"Disanshiba ci Zhongguo hulian wangluo fazhan zhuankuang tongji baogao"* [38rd Statistical report on Internet development in China], July 2016.

China Securities Journal, "*guanfang: 2020 nian dashuju chanpin ji fuwuyewu shouru jiang yu 1 wanyi*" [Official: Big data products and services revenues will exceed 1 trillion by 2020], 17/01/2017. Accessed 11/06/2017. http://www.cs.com.cn/xwzx/cj/201701/t20170117_5157997.html

Cisco Systems. "How Many Internet Connections are in the World? Right. Now. Accessed 11/06/2017. http://blogs.cisco.com/news/cisco-connection-counter.

CNET. "Buzz off! This smart vibrator is vulnerable to peeping hacks." April 5, 2017. Accessed 11/06/2017. https://www.cnet.com/news/vibrator-camera-sex-toy-hacking-security/

CNITSEC, "*2016 nian wangluo xin xinxi jishu lingyu anquan saomiao*" [2016 new information technologies security scan], 2017, januari, pp. 74-80.

Creemers, R. (2016). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century, Journal of Contemporary China, DOI: 10.1080/10670564.2016.1206281

Cuijpers, C. and B. Koops. (2011). “Smart metering and privacy in Europe: lessons from the Dutch case” In S. Gutwirth, R. E. Leenes, P. de Hert, & Y. Poullet (Eds.), *European data protection: Coming of age*. Amsterdam: Springer, pp.269-293.

Curran, James, Fenton, Natalie, and Freedman, Des. (2012). Misunderstanding the Internet. In Misunderstanding the Internet. Abingdon, Oxon: Routledge.

Deibert, R., John Palfrey, Rafal Rohozinski and Jonathan Zittrain (2011). *Access Contested: Security, Identity, and Resistance in Asian* Cyberspace. Cambridge: The MIT Press.

DiNucci, Darcy (1999). "Fragmented Future". *Print*. 53: 4, p. 32.

Drake, W., Vinton Cerf, and Wolfgang Kleinwächter, Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper, January 2016.

Drolet, M. “IoT could be our downfall.” Networkworld. December 20, 2016. Accessed 11/06/2017. http://www.networkworld.com/article/3151912/internet-of-things/iot-could-be-our-downfall.html

ECNS. “China urges fresh standards for the internet of things” December 30, 2016. Accessed 11/06/2017. http://www.ecns.cn/business/2016/12-30/239651.shtml

Economist. “Just spend: China’s consumer credit-rating culture is evolving fast—and unconventionally.” November 19, 2016. Accessed 11/06/2017. http://www.economist.com/news/finance-and-economics/21710292-chinas-consumer-credit-rating-culture-evolving-fastand-unconventionally-just

Financial Times. “China: when big data meets big brother.” Januari 19, 2016. Accessed 11/06/2017. http://www.ft.com/cms/s/0/b5b13a5e-b847-11e5-b151-8e15c9a029fb.html#axzz40G2n0kmE.

Financial Times. “China takes ‘project of the century’ to Pakistan.” May 17, 2017. Accessed 11/06/2017. https://www.ft.com/content/05979e18-2fe4-11e7-9555-23ef563ecf9a.

Foucault, M. (1988). “Technologies of the Self”, in Luther H. Martin, Huck Gutman, and Patrick H. Hutton, *Technologies of the Self: A seminar with Michel Foucault.* Amherst: The University of Massachusetts Press, pp. 16-49.

Foucault, M. (2004/2007). *Security, Territory, Population: Lectures at the College De France 1977-1978.* Houndmills: Palgrave.

Gartner. “Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015.” November 10, 2015. Accessed 11/06/2017. http://www.gartner.com/newsroom/id/3165317

Goldstein, Phil. “NSA, DHS and DOJ Highlight Security Threats Posed by IoT.” FedTech. October 12, 2016. Accessed 11/06/2017. http://www.fedtechmagazine.com/article/2016/10/nsa-dhs-and-doj-highlight-security-threats-posed-iot

Greengard, S. (2015). *The Internet of Things*. Cambridge: MIT Press.

GSMA. “How China is scaling the Internet of Things” GSMA Connected Living Programme, July 2015.

Hall, John. “China’s CCTV culture suffers as record high pollution and smog levels render country’s 20 million surveillance cameras effectively useless.” Independent, November 6, 2013. Accessed 11/06/2017. http://www.independent.co.uk/news/world/asia/chinas-cctv-culture-suffers-as-record-high-pollution-and-smog-levels-render-countrys-20-million-8924572.html#gallery.

Hamblen, M. “After DDOS attack, senator seeks industry-led security standards for IoT devices.” Computerworld. October 28, 2016. Accessed 11/06/2017. http://www.computerworld.com/article/3136650/security/after-ddos-attack-senator-seeks-industry-led-security-standards-for-iot-devices.html

Harwit, E. (2008). *China’s Telecommunications Revolution*. Oxford: Oxford University Press.

He Baogang and Mark Warren (2011). Authoritarian deliberation: the deliberative turn in Chinese political development. *Perspectives on Politics*. 9: 2, pp. 269–289.

Howard, P. N. (2015). *Pax Technica: How the Internet of Things may set us free or lock us up*. New haven: Yale University Press.

Hu Zhongyu and Huang Liya, “Dashuju shidai daxuesheng sixiang zhengzhi jiaoyu mianlin de wenti yu yingdui” [Problem and solution of college students’ political education in the era of big data], Xuexiao dangjian yu sixiang jiaoyu [Party building and political education in universities], no. 484, 2014, pp. 64–6.

King, Gary, Jennifer Pan and Margaret Roberts (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review* 107: 2, pp. 1–18.

King, Gary, Pan, Jennifer and Margaret E. Roberts. Forthcoming. How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument. *American Political Science Review*.

Krebs, Brian. “KrebsOnSecurity Hit With Record DDoS.” KrebsOnSecurity. September 21, 2016. Accessed https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Lampton, D. M. (2008). *The Three Faces of Chinese Power: Might, Money, and Minds*. Berkeley: University of California Press.

Lessig, L. (2006). *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books.

Lindsay, Jon R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security*. 39: 3, pp. 7–47.

Lindtner, S. (2015). “Hackerspaces and the Internet of Things of China: How Makers Reinvent Industrial Production, Innovation, and the Self” In Yang Guobin (ed.) *China’s Contested Internet*. Copenhagen: NIAS Press.

Li Yuxiao, “Cyberspace Security and International Cooperation in China”, China and Cybersecurity: Political, Economic, and Strategic Dimensions. Workshop Report, April 2012, University of California, San Diego.

Li Zhangjun, ‘Zhazha shishi tigao shehui guanli kexuehua shuiping, jianshe zhongguo tese shehui zhuyi shehui guanli tixi’ [Improve scientific level of social management, construct social management system with Chinese characteristics], People’s Daily, 19 Feb. 2011. Accessed 11/06/2017. http://news.xinhuanet.com/politics/2011- 02/19/c_121100198.htm.

Lu, Jia, and Ian Weber (2007). “State, power and mobile communication: a case study of China” *New media and society*. 9: 6: 925-944.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Machina Research. “Forecasting the Totality of the IoT Revenue Opportunity.” April 28, 2016. Accessed 11/06/2017. https://machinaresearch.com/report/forecasting-the-totality-of-the-iot-revenue-opportunity/

MacKinnon, Rebecca (2011). China’s “networked authoritarianism. *Journal of Democracy*. 22: 2, pp. 32–46.

McMillen, D. (1981). Xinjiang and the Production and Construction Corps: A Han Organisation in a Non-Han Region. *The Australian Journal of Chinese Affairs*. 6, pp. 65-96.

Morozov, E. (2011). *The Net Delusion: the Dark Side of Internet Freedom*. New York: Public Affairs.

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge: MIT Press.

Nathan, Andrew (2003). Authoritarian Resilience. *Journal of Democracy*. 14.1, pp. 6-17.

Neely, Andy (2007). “The Servitization of Manufacturing: An analysis of global trends” 14th European Operations Management Association Conference, Ankara, Turkey.

Neely, Andy (2013). “What is Servitization?” November 30, 2013. Accessed 11/06/2017. http://andyneely.blogspot.nl/2013/11/what-is-servitization.html

Ng, Jason (2013). *Blocked on Weibo: What Gets Suppressed on China’s Version of Twitter (and Why)*. New York: New Press.

Noesselt, Nele. (2014) Microblogs and the adaptation of the Chinese party-state’s governance strategy. *Governance*. 27: 3, pp. 449–68.

O’Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Paltemaa, L. & Vuori, J. A. (2009). Regime Transition and the Chinese Politics of Technology: From Mass Science to the Controlled Internet. *Asian Journal of Political Science*, 17: 1, pp. 1-23.

Pieke, F. (2016). *Knowing China: A Twenty-First Century Guide*. Cambridge: Cambridge University Press.

Powers, S. and Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana et al: University of Illinois Press.

Qu Weizhi (2010). *China’s Path to Informatization.* Hong Kong: Cengage Learning Asia.

Rexhepi, P. (2016). Liberal Luxury: Decentering Snowden, surveillance and privilege. *Big Data & Society* July-December 2016, pp. 1-3.

Riley, M. “NSA Said to Exploit Heartbleed Bug for Intelligence for Years,” Bloomberg, April 12, 2014. Accessed 11/06/2017. http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html.

Robinson, D. “Rolls-Royce to use Microsoft IoT and analytics tools for jet engine predictive maintenance.” V3. July 11, 2016. Accessed 11/06/2017. http://www.v3.co.uk/v3-uk/news/2464481/rolls-royce-to-use-microsoft-iot-and-analytics-tools-for-jet-engine-predictive-maintenance

Rutten, Tim. “Tyranny’s New Nightmare: Twitter.” Los Angeles Times, June 24, 2009.

Schlaeger, J. and Min Jiang (2014) Official microblogging and social management by local governments in China. *China Information.* 28: 2, pp. 189–213.

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

Schneier, B. (2013). “Power in Age of the Feudal Internet” in U. Gasser, R. Faris and R. Heacock (eds.) Internet Monitor 2013: Reflections on the Digital World, Cambridge (Mass.): The Berkman Center for Internet and Society, pp. 10-14.

Schneier, Bruce. “Regulation of the Internet of Things.” November 10, 2016. Accessed 11/06/2017. https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html

Schneier, Bruce. “We Need to Save the Internet from the Internet of Things” Motherboard. October 6, 2016. Accessed 11/06/2017. https://motherboard.vice.com/read/we-need-to-save-the-internet-from-the-internet-of-things

Schiller, D. (2014). *Digital depression: Information technology and economic crisis.* Urbana, IL: University of Illinois Press.

Schneider F.A. (2016). China’s ‘info-web’: How Beijing governs online political communication about Japan. *New Media & Society.* 18: 11, pp. 2664-2684.

Schneider F.A. (2017). forthcoming

Scott, James (1998). *Seeing Like a State; How Certain Schemes to Improve the Human Condition Have Failed.* New Haven, CT: Yale University Press.

Seymour, J. (2000). “Xinjiang’s Production and Construction Corps, and the Sinification of Eastern Turkestan.” *Inner Asia* 2: 2, pp. 171-193.

Sicari, S., Rizzardi, A., Grieco, L. A., and Coen-Porisini, A. (2015). Security, Privacy and Trust in Internet of Things: The Road ahead. *Computer Networks.* 76, pp. 146-164.

South China Morning Post. “Alphabet soup is the top draw on China’s 2017 technology menu” January 6, 2017. Accessed 11/06/2017. http://www.scmp.com/business/china-business/article/2059661/alphabet-soup-top-draw-chinas-2017-technology-menu

State Council, “Guanyu jiji tuijin ‘Hulianwang+’ xingdong de zhidao yijian” (Guiding Opinions Concerning Vigorously Promoting “Internet Plus” Activities), July 5, 2015.

Stockmann, D. (2013). *Media Commercialization and Authoritarian Rule in China*. New York: Cambridge University Press.

Suttmeier, R. and Shi Bing (2008). “Success in ‘Pasteur’s quadrant’? The Chinese Academy of Sciences and its role in the National Innovation System.” In Rowen, H., Gong, Hancock, M., and

Miller, W. (eds) *Greater China's Quest for Innovation*. Walter H. Shorenstein Asia Pacific Research Center, Stanford CA, pp. 35-56.

Tsang, S. (2009). Consultative Leninism: China's new political framework. *Journal of Contemporary China*. 18 62, pp. 865–880.

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, pp. 65–82.

Wang, Fei-Yue, Zhuo Feng, Qingpeng Zhang, Hui Wang, Daniel Zeng, James A. Hendler, Guanpi Lai, Yanqing Gao (2010). A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge. *Computer*. 43: 3, pp. 45-53. doi:10.1109/MC.2010.216

Williams, C. "Today the web was broken by countless hacked devices – your 60-second summary." The Register. October 21, 2016. Accessed 11/06/2017. http://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained

Wübbeke, J., Meissner, M., Zenglein, M., Ives, J., and B. Conrad (2016). "Made in China 2025: The making of a high-tech superpower and consequences for industrial countries." Merics. Papers on China No. 2, December 2016.

Xia, J. (2012). Competition and regulation in China's 3G/4G mobile communications industry: Institutions, governance, and telecom SOEs. *Telecommunications Policy,* 36: 10, pp. 798–816.

Xinhua. "Feature: Chinese idea brings innovation to B&R countries." May 12, 2017. Accessed 11/06/2017. http://news.xinhuanet.com/english/2017-05/12/c_136276466.htm.

Yang Guobin (2009). "Historical imagination in the study of Chinese digital civil society." In Zhang Xiaoling and Zheng Yongnian, *China's Information and Communications Technology Revolution: Social changes and state responses*. Oxon and New York: Routledge, pp. 17-33.

Zeng Jinghan (2016). China's date with big data: will it strengthen or threaten authoritarian rule? *International Affairs*. 92: 6, pp. 1443–1462.

Zenz, A. and James Leibold (2017). Xinjiang's Rapidly Evolving Security State. *Jamestown China Brief*. 17: 4. Accessed https://jamestown.org/program/xinjiangs-rapidly-evolving-security-state/

Zhang, Jingya. 'Benshi chengqu jiaoqu chengguan tantou quan fugai' [Probes fully cover our city], Beijing Chenbao [Beijing morning], October 3, 2015. Accessed http://bjcb.morningpost.com.cn/html/2015 10/03/content_368559.htm.

Zhao Yuezhi (2008). *Communication in China: Political Economy, Power, and Conflict*. Lanham: Rowman & Littlefield Publishers.

Zheng, Yongnian (2009). "The political cost of information control in China: The nation-state and governance." In Zhang Xiaoling and Zheng Yongnian, *China's Information and Communications Technology Revolution: Social changes and state responses*. Oxon and New York: Routledge.

Zhuge Jianwei, Gu Lion, and Duan Haixin, "Investigating the Chinese Underground Economy of Information Security" China and Cybersecurity: Political, Economic, and Strategic Dimensions. Workshop Report, April 2012, University of California, San Diego.

Ziegeldorf, J., Garcia Morchon, O., and K. Wehrle (2014). Privacy in the Internet of Things: Threats and Challenges. *Security and Communication Networks*. 7: 12, pp. 2728-2742.

Zuboff, Shoshana (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*. 30: 75. doi:10.1057/jit.2015.5