"Reading China"

The Internet of Things, Surveillance, and Social Management in the PRC

PIETER VELGHE

ABSTRACT: The "informatisation" agenda of the CCP calls upon a wide range of ICTs to transform everything from manufacturing to social management. The umbrella of versatile Internet of Things technology therefore serves as a key component of policy makers' efforts to further digitalisation. This paper explores claims that Chinese ICT policy appropriates the Internet of Things to improve surveillance and social management in order to increase the governing capacity of the Chinese state apparatus. Finally, the paper discusses the emerging credit systems in the face of a shift towards digitalisation and reliance on data-driven analysis, and the increased attention given to cyber security that results from the Chinese state' reliance on technology.

KEYWORDS: Internet of Things, ICTs, informatisation, social management, surveillance, Social Credit System, cyber security, PRC.

Introduction

Since the 18th Party Congress, the government of the People's Republic of China (PRC) pledged to make digitalisation the leading engine to strengthen the Chinese nation and economy. With the transition to the Xi administration, all matters concerning "informatisation" (*xinxihua* 信息化) were given top priority so as to make the PRC into a "strong Internet power" (*wangluo qiangguo* 网络强国). Through the widespread appropriaton of a host of advanced information and communication technologies (ICTs), most notably mobile internet, big data analytics, cloud computing, and the Internet of Things (IoT), the aim is to create an innovation-led economy and improve the government's governing capacity (Arsène 2016).

As the PRC has connected itself to the World Wide Web, government policy has been a continuous balancing act to suppress dissent and "harmful content" (*youhai neirong* 有害内容) online, while not having censorship and other measures hamper the development of the Internet economy (Tsui 2003). China now boasts the largest number of Internet users in the world (CNNIC 2016) and a vibrant community of developing and successful ICT companies. With President Xi personally taking charge of a number of regulatory bodies concerning the Internet, and close ties between the Party and Chinese Internet businesses, the Chinese leadership is confident in its ability to maintain control and stimulate growth and innovation (Hong 2017).

One particular strand of ICT technology, the IoT, has recently figured more prominently in the plans for "informatisation." This technology, due to its revolutionary potential and potential omnipresence in a "connected" or "smart world" deserves more scrutiny. Unlike other network technologies, IoT technology enables a host of different physical "things" – such as smart phones, smart wristbands, smart locks, drones, self-driving cars, surveillance cameras, or anything with a microchip attached to it – to be connected to the Internet. Once connected, devices and servers exchange data, thus providing real-time information in new areas and on a potentially massive scale (Greengard 2015). The IoT creates a different Internet, as unlike most previous web applications, IoT devices and services have a direct impact on the physical world.

By having many more devices connected to the Internet, all of which log, store, and exchange a wide variety of data, much more activity is documented (Greengard 2015). With the Internet as we know it now and the connected devices already in use now (including smart phones and smart watches, etc.), we already live in "the golden age of surveillance" according to a leading Internet scholar (Schneier 2015: 4). The IoT will only aggravate this. As the Internet comes to encompass more aspects of our lives, concerns increase about it serving as a potent tool for surveillance and social management, for hacking and espionage, and for sabotage and warfare (Howard 2015; Schneier 2018).

Given the ambivalent nature of the Chinese leadership concerning ICTs, I want to explore in this article how exactly the IoT fits into the wider agenda of "informatisation." I will focus in particular on how it is said to improve the surveillance and social management capabilities of the Chinese state. We will therefore first look into current government plans for IoT development in order to trace how the IoT and related technology relate to the "informatisation" agenda, and to surveillance and social management in particular.

Developing Chinese IoT

The IoT policy was kicked off during the Hu-Wen administration when then Premier Wen Jiabao on 7 August 2009 visited a research centre for IoT technology that was founded the previous November in Wuxi, Jiangsu Province. There, Wen called for the speedy establishment of China's "Information Sensing Centre" (*chuangan xinxi zhongxin* 传感信息中心), otherwise known as the "Reading China Centre" (*ganzhi Zhongguo zhongxin* 感知中国中心).[1] From that year on, the Wuxi New Area (*Wuxi xin qu* 无锡新区) industrial park was transformed into a "sensing net model city" (*chuangan-wang shifan chengshi* 传感网示范城市) with the ambition of becoming China's and the world's top IoT innovation hub (Mei 2009). The plan was ratified by the State Council and the Ministry of Industry and Information Technology (MIIT) identified the "sensing net" as a "new high-end technology with comprehensive usage" and an important element of the strategic new industry (MIIT 2012).

1. Wen Jiabao, "尽快建立中国传感信息中心" (Jinkuai jianli Zhongguo chuangan xinxi zhongxin, Speedy establishment of China's information sensing centre), *Xinhua*, 5 August 2010.

This came at the time when, according to Hong (2017: 1755-6), "policy makers came to terms with the pitfalls of the old growth model and were embarking on transitional measures." In advance of the 18th Party Congress, the State Council stated that IoT together with other ICTs should be called upon to further economic development in a post-financial crisis world, and that domestic ICT development was also needed to reduce reliance on foreign technology (State Council 2010). This sentiment coalesced into the 12th Five-Year Plan, and the new Xi-Li administration brought these plans completely to the fore in the 2015 plan "Internet Plus" (*hulianwang+* 互联网+). There, IoT, together with mobile Internet, big data, and cloud computing, was recognised as a vital part of the country's ambition to make China into a "strong internet power" (State Council 2015a).

The goal the State Council set out in early 2013 to "create a batch of core technology" and to build an early form of an IoT industry system by 2015 (State Council 2013) was certainly met. Reportedly by 2017 close to 2,000 IoT businesses, with an estimated industrial value exceeding 150 billion RMB, settled in the Wuxi Area alone (Wuxi 2017). Other major ICT businesses such as Huawei, Alibaba, Xiaomi, Baidu, Tencent, and ZTE, together with the telecom providers China Unicom, China Telecom, and China Mobile, are also competing heavily to capture domestic and international markets with innovative IoT appliances. [2] The IoT-market in China in 2015 was worth up to 750 billion RMB and accounted for 31% of the global total, [3] and Chinese investment continues to drive the global IoT boom. [4] Businesses in industries as diverse as transportation, medicine, agriculture, military, social management, and public security are implementing the technology. Consumer goods such as wearables, smart home appliances, and connected cars are also in increasingly high demand (GSMA 2015). Given the trend towards digitalisation as the new "pole of profitable growth" in today's economy (Schiller 2014: 146), the anticipated economic success of the IoT will very likely push the "informatisation" agenda to many unexpected places.

Setting the scope

The range in which the IoT is stated to be developed and employed in government technology policy is set very wide, as it furthers the overall plans towards "smartisation, refinement and internetisation" (*zhinenghua, jingxihua, wangluohua* 智能化，精细化，网络化) (State Council 2013). Under the auspices of the Xi administration, "informatisation" is called upon to not merely usher in new modes of production and manufacturing (as was also the case under the previous administration), but also to transform or "upgrade" many societal and political processes through the means of technology. As smart devices start to permeate industry and society, the potential for the Chinese government to tap into all the data that is being generated, and therefore its ability to "read" the country, has grown immensely. The government plans for the IoT to be "beneficial to advancing the changing orientation in the style of production, living, and social management" (State Council 2013) should therefore be understood as part of a comprehensive effort by the Chinese Communist Party (CCP) to appropriate the clout of ICTs to "tackle the Party's key challenges in propaganda, public opinion and social management [for the purpose of] maintaining stability, ensuring CCP dominance, preventing organised opposition and enhancing intra-Party discipline" (Creemers 2016: 4).

To achieve this goal, surveillance has become a top priority. Since the process of "securitisation" of the Chinese state since the 1990s, much of the Party's governing capacity has increasingly been set up to function as a tool for "stability maintenance" (*weiwen* 维稳) (Wang and Minzer 2015). Their effects are most visible in politically sensitive areas such as Tibet and Xinjiang, where ubiquitous check-points and surveillance cameras equipped with the latest iris scanners and facial recognition technology hamper the local population in going about their daily business. People in Xinjiang are reportedly also required to install a spyware app on their mobile phones to track their online activity, and to get a QR code containing their personal info engraved on any knives they purchase. [5] Similar systems are spreading to the rest of the country as government policing schemes and intelligence gathering projects using "grid management" (*wanggehua guanli* 网格化管理) are being set up to integrate ICTs with traditional street-level policing, social services, and both cooperative and coercive forms of management. [6]

The authorities are all able to rely on ever better technology to analyse ever-larger amounts of data, and thus increase surveillance and improve feedback mechanisms that ultimately enable them to pre-emptively act on incidents and social unrest (Schwarck 2018). Using these methods, reportedly as early as 2011, the government has been able to track the precise movements of 17 million people in Beijing using the signal from people's phones. [7] On top of that, elaborate closed-circuit television (CCTV) networks, consisting of millions of panoramic cameras, cover much of urban public spaces. 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% of public streets. [8] Recently, the 2015 "Sharp Eyes Project" (*Xueliang gongcheng* 雪亮工程) aims to reach 100% coverage of all of China's public areas and key industries by 2020, relying not only on CCTV but also on cameras installed inside smart devices in people's homes, such as smart TVs. [9]

Smart phones, surveillance cameras, and other smart devices all constitute the IoT. As the number of smart devices each person owns increases and public spaces are turned into "smart cities," many more processes will be recorded, and people's activities will be monitored in novel ways. Much of this is described in IoT policy documents: e.g., using the electric grid for monitoring with smart meters as the entrance point, or using "high towers"

2. Recently however, Chinese ICT companies (and in particular Huawei) have faced a lot of backlash in their operations abroad for their supposed links with the Chinese state and the risks that would come with Chinese companies controlling the next generation of Internet infrastructure, such as 5G networks. It is therefore expected that other aspects of Chinese ICT companies' operations, such as their development and selling of IoT appliances, will come under increased scrutiny as well; especially with relations heating up between China and the US as the two countries are engaged in a "trade war," and the US having only started to address issues such as IPR theft by China.
3. "China urges fresh standards for the Internet of Things," *ECNS*, 30 December 2016, http://www.ecns.cn/business/2016/12-30/239651.shtml (accessed on 8 December 2018).
4. Maxwell Cooter, "Chinese investment drives IoT boom," *Techradar.pro*, 9 January 2018, https://www.techradar.com/news/chinese-investment-drives-iot-boom (accessed on 8 December 2018).
5. "China has turned Xinjiang into a police state like no other," *The Economist*, 31 May 2018, https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other (accessed on 8 December 2018).
6. Samantha Hoffman, "Managing the State: Social Credit, Surveillance and the CCP's Plan for China," *The Jamestown Foundation*, 17 August 2017, https://jamestown.org/program/managing-the-state-social-credit-surveillance-and-the-ccps-plan-for-china/ (accessed on 8 December 2018).
7. Leo Lewis, "China mobile phone tracking system attacked as 'big brother' surveillance," *The Times*, 4 March 2011, http://www.theaustralian.com.au/news/world/china-mobile-phone-tracking-system-attacked-as-bigbrother-surveillance/story-e6frg6so-1226015917086 (accessed on 8 December 2018).
8. Zhang Jingya 张静雅, "本事城区郊区城管探头全覆盖" (Benshi chengqu jiaoqu chengguan tantou quan fugai, Probes fully cover our city), *Beijing Chenbao*, 3 October 2015.
9. Qiao Long, "China Aims For Near-Total Surveillance, Including in People's Homes," *Radio Free Asia*, 30 March 2018, https://www.rfa.org/english/news/china/surveillance-03302018111415.html (accessed on 8 December 2018).

for emergency relief, surveillance mechanisms covering focal areas to prevent intrusions and improve the public management of cities, and creating a public security platform for surveillance, early warnings, and emergency relief (MIIT 2012). Other tasks mentioned in these documents are to develop models for safeguarding important events and places, controlling all motor vehicles, and managing the floating population (NDRC *et al.* 2013). The IoT in these examples offers the necessary infrastructure for the increase in surveillance that the Chinese government seeks. But the true success of China's "informatisation" and surveillance plans lies with a larger number of ICTs, among which facial recognition, AI, and machine learning are crucial.

The State Council, for example, claims to "[s]upport security protection enterprises to launch cooperation with Internet enterprises to develop and popularise accurate image recognition and other such big data analysis technologies, and enhance the intelligence and service levels of security protection products" (State Council 2015b). The MIIT also claims to "greatly support research suitable for storing and processing great volumes of IoT data, as well as data mining, smart image, and video analysis technologies" (MIIT 2011). Facial recognition is already being tested in many places in China. Some train stations use it to check if a ticket matches its holder,[10] jaywalkers are publicly shamed in some cities,[11] and it will soon be possible to pay by just showing your face.[12] Related technology such as speech recognition has already been used to identify scammers through the phone.[13] Companies working with the government and providing it with the latest technology obviously benefit from access to all of this data. In the field of facial recognition alone, three Chinese start-ups (SenseTime, Megvii or Face++, and Yitu) are valued at over a billion dollars.[14]

"Automating" social management

As indicated above, a big motivation underlying many of these developments is the will of the CCP to use the most advanced technology to improve its social management capacity in order to maintain political stability. The term "social management" has become central in Party discourse since it came into use under the 11th Five-Year Plan, when it was made a "key target" (*zhuyao mubiao* 主要目标) for governing (Pieke 2012). The emphasis on "management" is employed to tackle issues that sprang out of newfound social mobility and stratification after "reform and opening" (*gaige kaifang* 改革开放) and aims to proactively help maintain public order by means of communication and consultation, and if necessary, by coercion, in order to strengthen the Party's control over society (*ibid.*). Under the auspices of Zhou Yongkang – the man largely responsible for the expansion of China's domestic security apparatus, but who in 2014 was convicted of corruption-related charges and expelled from the CCP – social management developed into "a catch-all solution for all kinds of issues that have to do with social stability" (*ibid.*: 16). In a 2006 *People's Daily* article entitled "Strengthen and improve social management – promote social stability and harmony." Zhou advocated the construction of a public security platform for surveillance, early warnings, and emergency relief.[15] Five years later, in the 11th Five-Year Plan, this idea was developed as "one of the main pillars of social management and upholding social stability" (*ibid.*: 18).

The language used by Zhou, i.e., when advocating the construction of an emergency response system, is directly echoed in many "informatisation" policy documents, including in that of the IoT (MIIT 2012; NDRC *et al.* 2013). Here we see the links between the "social management" agenda and the surveillance schemes mentioned above. Zhou himself also pointed out that some of the tasks of social management, such as conflict mediation and complaints and public opinion expression, could be improved through use of the Internet (Pieke 2012). Social management goes beyond mere surveillance, however, as its holistic approach to "managing" society, combined with the techno-optimism of the Chinese government, urges it to always find better and more complete ways to manage social stability.

This is where projects such as the Social Credit System (*shehui xinyong tixi* 社会信用体系) (SCS) come in. The SCS is an amalgam of different credit or scoring systems that is being developed and tested by different government and private actors for the purpose of ranking individuals or companies on the basis of certain economic, social, and political (mis)behaviour. On the basis of this score or ranking, users face being either rewarded with discounts or exclusive access, or being blacklisted or denied access to bank loans, certain housing, or certain modes of travel, for example. As these different systems show a great deal of difference amongst them (e.g., between government systems and the more loyalty-based or credit history-based systems of private companies) and are not yet fully operational or at least not on a large or nation-wide scale (despite what some Western media report), it is impossible to comment on the criteria used for scoring and their implications, or on their perceived "success" in the eyes of either the state or the Chinese people.

What can be said, however, is how the SCS fits both the government's holistic "social management" agenda, which is based "not just on the lawfulness, but also the morality of [actors'] actions, covering economic, social and political conduct" (Creemers 2018: 2), and its broad "informatisation" agenda as it builds on recent advances in big data analytics and AI and on the vast amounts of data available in the rapidly digitalising China. Especially with a developing IoT, "all aspects of our lives – transactional, educational, medical, legal, recreational, and consumer – leave a digital footprint";[16] and schemes such as SCS, like all big data-driven algorithms, try to make sense of these footprints according to their own criteria and agendas. Another crucial advantage of the IoT is that it has the potential to link and integrate both online and previously offline processes, as well as government institutions and industry, in order to "automate" social management (Hoffman 2017). The importance of sharing data between different ministries, businesses, localities, and even the military is expressed in many IoT policies. Achieving this also requires building data centres throughout the country,

10. "Face recognition ticket checking comes to Beijing West Railway Station," *China Daily*, 30 November 2016, http://usa.chinadaily.com.cn/china/2016-11/30/content_27529029.htm (accessed on 8 December 2018).
11. Meghan Han, "AI Photographs Chinese Jaywalkers; Shames Them on Public Screens," *Medium*, 9 April 2018, https://medium.com/syncedreview/ai-photographs-chinese-jaywalkers-shames-them-on-public-screens-ad0a301a46a6 (accessed on 8 December 2018).
12. Will Knight, "Paying with Your Face: Face-detecting systems in China now authorize payments, provide access to facilities, and track down criminals. Will other countries follow?," *MIT Technology Review*, March/April 2017, https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/ (accessed on 8 December 2018).
13. Samuel Wade, "Minitrue: 'Voiceprint Analysis Can Recognize Swindlers'," *China Digital Times*, 28 February 2017, http://chinadigitaltimes.net/2017/02/minitrue-delete-article-voiceprint-analysis-can-recognize-swindlers/ (accessed on 8 December 2018).
14. Josh Horwitz, "A Chinese e-commerce giant is becoming a major investor in facial-recognition technology," *Quartz*, 9 April 2018, https://qz.com/1247511/alibaba-is-now-a-major-investor-in-facial-recognition-startup-sensetime/ (accessed on 8 December 2018).
15. Zhou Yongkang 周永康, "加强和改进社会管理－促进社会稳定和谐" (Jiaqiang he gaijin shehui guanli – cujin shehui wending hexie, Strengthen and improve social management – promote social stability and harmony), *Renmin ribao*, 25 October 2006.
16. Jeremy Daum, "China through a glass, darkly," *China Law Translate*, 24 December 2017, https://www.chinalawtranslate.com/seeing-chinese-social-credit-through-a-glass-darkly/?lang=en (accessed on 8 December 2018).

with the aim of "rais[ing] the timeliness, completeness, and accuracy of information" (State Council 2016). This way ICTs – with an important role for the IoT – can ensure that "traditional spatial, temporal and quantitative barriers to surveillance and control of individual behaviour are increasingly overcome" (Creemers 2016: 15).

Moving forward

Going beyond the current Chinese plans related to "informatisation" and "social management," there are two important trends for IoT that will affect the development of these agendas and schemes such as SCS. The first relates to the change in business model ushered in by the availability of data generated by "smart devices" and advances in data-driven analysis. The IoT is not just about "smart things" or about "attaching a sensor to anything," but rather is about generating, having access to, and analysing new and more data flows (Zuboff 2019). Through scaling data analytics, companies can offer increasingly efficient use of energy and resources, and make predictions about future behaviour. This way companies can, for example, offer discounts on the basis of your usage of a certain service, or even on your physical fitness. Recently one of the oldest and largest North American life insurers said it will stop selling traditional life insurance and will only offer interactive policies that track health data through wearable devices and smartphone logs. [17]

This nudging of citizens toward "self-management" (instead of using coercion or penal means) seemingly also fits into the logic of behavioural data schemes such as the SCS, [18] as it does with the neoliberal or Silicon Valley model of personal responsibility (often in combination with austerity politics). Neither model claims that societal factors do not matter in determining people's behaviour, but they imply that changing these factors is much harder than changing the behaviour of the individual. [19] The difference is that while the latter, in its "attempt to displace politics with a notion of economic orderliness and naturalness – to neutralise the political clash over irreconcilable normative visions of family, society, and nation by privileging the orderliness of the economic realm" (Harcourt 2015: 98) – tries to hide or deny its political nature, the former (the SCS and other developing Chinese credit scores) embraces the political precisely to achieve the orderliness in the economic (and social) realm that it explicitly pursues.

"Credit scores" or "consumer scores" in themselves are nothing new. They have been proliferating in public and private entities since the 1950s in order to "describe or predict [people's] characteristics, habits, or predilections." [20] But unsurprisingly, as more sensors collect more data about people's behaviour, as data-driven, statistical analysis keeps on improving, and as people's faith in the accuracy, efficacy, and objectivity of hard data continues (Boyd and Crawford 2012; O'Neil 2016), credit scores will increasingly prove irresistible for many companies and governments alike, for whatever commercial or political agenda.

A second trend is the danger of relying on technology and data, as in the Chinese plans for "informatisation." There has been a major increase in attention to internet or cyber security (*wangluo anquan* 网络安全 or *xinxi anquan* 信息安全) in Chinese policy lately, but the level of ICT security in China remains notoriously low, as large-scale hacks, data leaks, and online scams are frequent occurrences (Lindsay 2015). As IoT proliferates in China, ensuring even a basic level of security will also prove challenging, as IoT devices in general are poorly secured, are often used for extended periods, and often lack a mechanism to receive security updates. [21] In recent hacks, IoT devices worldwide have been compromised on a massive scale and used for some of the largest cyberattacks the Internet has ever seen. [22] If IoT devices get hacked, the impact on the physical world can be severe and potentially even have fatal consequences (Greengard 2015).

Therefore, a precondition for the Chinese government in adopting IoT and other ICTs is for them to be "manageable and controllable" (*keguan kekong* 可管可控) and "safe and reliable" (*anquan kekao* 安全可靠) (State Council 2013). A milestone in efforts by Chinese policymakers to improve cybersecurity in China is the 2016 Cybersecurity Law and the National Cyberspace Security Strategy (Standing Committee 2016; CAC 2016). This important piece of policy makes cybersecurity the number one priority for Chinese plans of "informatisation." The Strategy states that there is a danger of the country's critical infrastructure being targeted because "networks and information systems have become critical infrastructure and even nerve centres for the entire economy and society," and attacks on critical infrastructure could therefore lead to "paralysis of critical energy, transportation, telecommunications, and financial infrastructure, etc." (CAC 2016). As the IoT becomes part of this "nerve centre," security of the IoT is destined to become a major topic for Chinese technology policymakers. Security also becomes important when data is shared between multiple bodies in government and outside. With more people having access to different kinds of data, the chance of leaks and security breaches increases. This valuable data trove of personal and possibly sensitive information also becomes a hot target for foreign intelligence services and hackers and can become an important source of power in intra-party conflict (Zeng 2016).

To conclude, it is good to keep in mind that many of the political developments described here or the motivations behind them are not unique to China and will become more ubiquitous as technology improves. These technologies can offer solutions to real problems and don't necessarily have to be harbingers of dystopia. The same applies to the developing SCS: some societal ills spurred by reform and opening raised legitimate concerns for more control. Similarly, IoT policy is set up to help tackle some very specific and persistent issues plaguing China, such as ensuring food and resource security, tackling pollution, resolving persistent traffic problems, and offering

17. Suzanne Barlyn, "Strap on the Fitbit: John Hancock to sell only interactive life insurance," *Reuters*, 19 September 2018, https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN1LZ1WL (accessed on 8 December 2018).
18. Samantha Hoffman, "Grasping Power with Both Hands: Social Credit, The Mass Line, and Party Control," *The Jamestown Foundation*, 10 October 2018, https://jamestown.org/program/grasping-power-with-both-hands-social-credit-the-mass-line-and-party-control/ (accessed on 8 December 2018).
19. Evgeny Morozov, "The rise of data and the death of politics," *The Guardian*, 20 July 2014, https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation (accessed on 8 December 2018).
20. Pam Dixon and Robert Gellman, "The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future," *World Privacy Forum*, 2 April 2014, http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf (accessed on 8 December 2018).
21. Bruce Schneier, "Regulation of the Internet of Things," *Schneier on Security*, 10 November 2016, https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html (accessed on 8 December 2018).
22. Brian Krebs, "Hit With Record DDoS," *KrebsOnSecurity*, 21 September 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (accessed on 14 February 2019); "Today the web was broken by countless hacked devices – your 60-second summary," *The Register*, 21 October 2016, http://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained (accessed on 8 December 2018).

health check-ups to the elderly and people in remote places (NDRC *et al.* 2013). However, under the "informatisation" agenda, the IoT and ICTs in general are increasingly summoned as convenient jacks-of-all-trades offering a quick fix to some of China's "hard problems." As this technological solutionism may offer positive results in the short term (albeit not without dangers due to, for example, low Internet security), in the long term it is bound to permanently alter the playing field between government and businesses vis-à-vis the citizenry.

Pieter Velghe is a Sinologist at the Belgian Embassy in Beijing (pietervelghe@msn.com). All opinions expressed in this article are strictly those of the author.

Academic Sources

ARSÈNE, Séverine. 2016. "Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic World Order?" *China Perspectives* 135(2): 25.

BOYD, Danah, and Kate CRAWFORD. 2012. "Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon." *Information, Communication & Society* 15(5): 662-79.

China Internet Network Information Centre. 2016. "第三十八次中国互联网络发展状况统计报告" (Di sanshiba ci Zhongguo hulianwangluo fazhan zhuankuang tongji baogao, 38rd Statistical report on Internet development in China), July 2016.

CREEMERS, Rogier. 2017. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century." *Journal of Contemporary China* 26(103): 85-100.

CREEMERS, Rogier. 2018. "China's Social Credit System: An Evolving Practice of Control." 9 May 2018, https://ssrn.com/abstract=3175792 (accessed on 14 February 2019).

GREENGARD, Samuel. 2015. *The Internet of Things*. Cambridge: MIT Press.

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

HARCOURT, Bernard E. 2015. *Exposed: Desire and Disobedience in the Digital Age*. London: Harvard University Press.

HOFFMAN, Samantha. 2017. *Programming China: The Communist Party's Autonomic Approach to Managing State Security*. PhD Thesis (on file with author).

HONG Yu. 2017. "Reading the 13th Five-Year Plan: Reflections on China's ICT Policy." *International Journal of Communication* 11: 1755-74.

HOWARD, Philip. 2015. *Pax Technica: How the Internet of Things May Set us Free or Lock us Up*. New haven: Yale University Press.

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

MEI, Fangquan 梅方权. 2009. "智慧地球与感知中国 – 无联网的发展分析" (Zhihui diqiu yu ganzhi Zhongguo – wulianwang de fazhan fenxi, Smart Earth and Reading China - Analysis on Development of Internet of Things), *Agricultural Internet Information* 12: 5-21.

O'NEIL, Caty. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

PIEKE, Frank. 2012. "The Communist Party and social management in China." *China Information* 26(2): 149-65.

SCHILLER, Dan. 2014. *Digital depression: Information technology and economic crisis*. Urbana: University of Illinois Press.

SCHNEIER, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: Norton & Company.

SCHNEIER, Bruce. 2018. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York: Norton & Company.

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

TSUI, Lokman. 2003. "The Panopticon as the antithesis of a space of freedom: Control and regulation of the Internet in China." *China Information* 17(2): 65-82.

WANG, Yuhua, and Carl MINZER. 2015. "The Rise of the Chinese Security State." *The China Quarterly* 222: 339.

Wuxi New Area Investment, "2017世界无联网博览会已在进入准备" (2017 shijie wulianwang bolanhui yi zai jinru zhunbei, The 2017 World IoT Fair is already starting Preparations), 7 February 2017.

ZENG, Jinghan. 2016. "China's date with big data: will it strengthen or threaten authoritarian rule?" *International Affairs* 92(6): 1443-62.

ZUBOFF, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affair.

Policy Documents

Cyberspace Administration of China. 2016. "国家网络空间安全战略" (Guojia wangluo kongjian anquan zhanlüe, National Cyberspace Security Strategy), 27 December 2016.

Ministry of Industry and Information Technology. 2011. "关于印发无联网'十二五发展规划'的通知" (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), 28 November 2011.

Ministry of Industry and Information Technology. 2012. "无锡国家传感网创新示范区发展规划纲要(2012-2020年)" (Wuxi guojia chuanganwang chuangxin shifanqu fazhan guihua gangyao (2012-2020) nian, Wuxi National Sensing Net Innovation Model Area Development Plan Outline (2012-2020)), 17 August 2012.

National Development and Reform Commission *et al.* 2013. "关于印发10个无联网发展专项行动计划的通知" (Guanyu yinfa shi ge wulianwang fazhan zhuanxiang xingdong jihua de tongzhi, Notice Concerning the Printing and Distributing 10 Internet of Things Development Special Action Plan), 5 September 2013.

Standing Committee of the National People's Congress. 2016. "网络安全法" (Wangluo anquan fa, Cybersecurity Law), 7 November 2016.

State Council. 2010. "关于加快培育和发展战略性新型产业的决定" (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), 10 October 2010.

State Council. 2013. "关于推进无联网有序健康发展的指导意见" (Guanyu tuijin wulianwang youxu jiankang fazhan de zhidao yijian, Guiding Opinions Concerning Promoting the Orderly and Healthy Development of the Internet of Things), 5 February 2013.

State Council. 2015. "2015年政府工作报告" (2015 nian zhengfu gongzuo baogao, 2015 Government Work Report), 5 March 2015.

State Council. 2015. "关于积极推进'互联网+'行动的指导意见" (Guanyu jiji tuijin 'Hulianwang+' xingdong de zhidao yijian, Guiding Opinions Concerning Vigorously Promoting 'Internet Plus' Activities), 5 July 2015.

State Council. 2016. "关于'十三五'国家信息化规划的通知" (Guanyu 'shisanwu' guojia xinxihua guihua de tongzhi, '13th Five-Year Plan' for National Informatisation), 27 December 2016.