China’s Date with Big Data: will it strengthen or threaten the authoritarian rule?

Abstract
The rise of big data has brought with it tremendous possibilities, for better or worse. In China, the government has been enthusiastically preparing for the coming of the big data era. This article examines how the authoritarian regime in China has been employing big data to improve its governance and to move towards a “big brother 2.0” model. The regime has combined co-optation with coercive control to exploit digital technology, in order to maximize its utility and thus maintain authoritarian rule. Moreover, existing debates on digital technology largely focus on the changing power structures between state and society, but neglect power structures within regimes and their implications for authoritarianism. This article argues that the use of massive digital data may backfire against the authoritarian regime as it may change the power structure within the state. That is to say, efforts to embrace big data may also undermine the authoritarian rule. A more accurate understanding of the Chinese authoritarian regime’s resilience and vulnerability in the information age will help us grasp the essence of China’s rise as a fragile global power.
Introduction

Big data is perhaps one of the most fashionable terms nowadays. The data revolution has allowed the application of big data to be expanded to every aspect of our digital society. While big data has been heavily invested in by the private sectors, it also attracts the attention of public sectors, given its great potential to contribute to governance. In the public healthcare sector, for example, big data has launched a revolution by reducing overall cost, improving efficiency, predicting epidemics and curing disease.\(^1\) Despite its recent emergence, the rise of big data has already generated considerable attention on its implications for transforming governance. Yet, the primary focus is about democratic states with little attention on autocracy. While this may be understandable enough given digital technology is more developed in democratic countries as well as greater motivation to improve public governance, it is a shortcoming nevertheless.

Indeed, the rise of big data has brought no less changes to autocracy like China than to democracy – for better or worse. In order to adapt to the digital era, the Chinese government has also been enthusiastic about big data. In November 2015, the State Council of China officially announced the development of big data as a national strategy.\(^2\) The Chinese government is not only interested in big data’s business potential and technological innovation, but also its potential to improve governance and upgrade state surveillance. China’s weak civil awareness, powerful state financial capacity and strong state willing to push back social autonomy has made the state’s transformation through cutting-edge ‘big data’ technology into the most sophisticated electronic police state in this planet more than a possibility. Policymakers and scholars can learn a great deal about China’s political development from paying greater attention to this phenomena.

This article details China’s governance strategy in regards to big data and its implications for the authoritarian rule by examining policy documents and academic studies of big data in China. While the authoritarian regime in China aims to utilize digital technology to strengthen its rule, its authoritarian nature might make this approach dangerous. This article argues that the possibility of authoritarian backfire – the use of massive digital data may backfire against the authoritarian regime – should not be under-estimated. When data is highly concentrated in the hands of a few powerful individuals or agencies, it may be sufficiently destructive to the entire authoritarian regime when it is used in the interests of power struggles. In this regard, the regime’s efforts to strengthen authoritarian rule by embracing big data may end up undermining it.

The following sections will elaborate on the above arguments in further detail. It will first review the current debate over the implications of digital technology for autocracy. After a brief overview of the growing interest in big data in China, the article will explore how the government has employed big data to improve its governance and upgrade its state surveillance in order to strengthen its authoritarian rule. Following this, it will discuss how the use of big data may backfire against the authoritarian regime, followed by the concluding remarks over the resilience of authoritarianism.

Debating digital technology: “liberating technology” versus “repression technology”

Before reviewing the debate on the implications of digital technology, it is important to define big data first. Big data is an umbrella term that refers to many meanings in different contexts. In China, it is not a uniform concept, and is sometimes used as a catch phrase. Thus, the Chinese government’s big data approach is better considered as a broad, incoherent adaptation strategy towards e-governance. While many Western states may be using a similar strategy, the nature of the political system has made a key difference. In the case of democratic states, the main purpose of the adaption strategy is to build a more efficient and capable government in order to deliver better public service – despite the debatable use of state surveillance. While this is also a part of the plan in China, the most important goal is to ensure the continuity of the one-party system. In other words, it is about how the one-party system can adapt in the era of big data and ultimately stay in power. Needless to say, the incoherent understanding of big data has further complicated the actual impact of big data on China’s authoritarian rule.

While big data may also include traditional (non-digital) sources of data, this article will primarily focus on digital ones. Thus, big data broadly refers to an “explosion in the quantity and diversity of high frequency digital data” in this article. It is also important to draw a distinction between big data as a phenomenon and the way attempts are made to use those data. In China, words like “to promote the development of big data” or “develop big data” frequently appears in official documents. However, those words refer to improvements in the way that big data is used and applied instead of developing big data as a phenomenon.

With the development of the Internet, user-generated content has gradually become dominated. This has sparked vivid discussion about the changing nature of information dissemination in authoritarian regimes. What are the implications of the development of digital technology for autocracy? Will it undermine or strengthen autocracy? The literature presents two contrary perspectives: “liberation technology” and “repression technology”. The first perspective argues that modern information and communication technology can deliver liberation to individual citizens by “expand(ing) political, social, and economic freedom”. Unlike traditional media, the Internet has empowered society by promoting information flow.

The Internet, in particular, exposes netizens to foreign ideas that were not available before. Thus, it leads to the spread of Western ideas including democracy and freedom and undermines pro-authoritarian values. At the domestic level, information flow led by Internet and communication technology also facilitates the organization of social protest and opposition forces. In particular, social media sites have attracted considerable academic attention owing to their potential nature as a “liberating technology” that challenges authoritarian rule through collective mobilisation. For example, some argue that social media played a significant role during the Arab Spring by facilitating communication among individuals and thus organizing political protests. Thus, Arab Spring is also termed by many as a “Facebook/Twitter Revolution.” It is argued that the development of the Internet and social media empowers

---

4 Diamond, “Liberation Technology,” p.70
5 Lynch, “After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State.”
individuals, and fundamentally changes the way in which information is produced, consumed and shared. As a result, this presents a systematic challenge to authoritarian rule, and inevitably undermines the latter.7

Others, however, are sceptical about digital technology (especially social media) as a potential liberating factor. Digital technology is a neutral tool, and its actual impact depends on how it is deployed. Terrorist organizations including Islamic State and other criminal groups have also taken advantage of social media for sinister goals, instead of liberating purposes. In addition, the view that Arab Spring as a “Facebook/Twitter Revolution” may also overstate the role of social media.8 While social media certainly matters, it is not the decisive factor that led to Arab Spring.

The “repression technology” perspective considers digital technology as a tool for authoritarian regimes to strengthen their repression. Internet censorship obviously plays a key role. Studies by Gary King, Jennifer Pan, and Margaret Roberts show how the Chinese government strategically uses Internet censorship to allow for criticism of the government, but represses the possibility of using the Internet to call for social protest.9 In addition to eliminating social mobilization through the Internet, autocracies employ the Internet to provide information in favour of the government.10 Digital technology makes this possible by blocking information flow. The authoritarian regime has benefited from its heavy investment on the Great Firewall of China. Instead of serving liberalising purpose, the relevant technology prevents Chinese citizens from being exposed to foreign liberal ideas.

Meanwhile, the Chinese government has been keen to spread pro-government views on Weibo (Chinese version of twitter), especially after Xi Jinping took power in 2012.11 On the one hand, it has taken efforts to contain negative opinions about the government on Weibo. For example, the Weibo accounts of opinion leaders such as Zhang Lifan were closed because of their out-spoken criticism towards the government. Xue Manzi, an influential opinion leader, was even arrested for soliciting prostitution. On the other hand, the regime has launched a series of media offensives. It has encouraged party media and officials to open Weibo accounts in order to win the online battlefield of public opinion. These efforts have successfully contained the spread of negative comments on the government on Weibo.12

Therefore, instead of undermining authoritarian rule, the “repression technology” perspective holds that digital technology actually empowers authoritarian states by making them more capable of repressing civil rights. This article will contribute to the debate by

---

8 Sara Reardon, Was the Arab Spring really a Facebook revolution? New Scientist, available at https://www.newscientist.com/article/mg21428596-400-was-the-arab-spring-really-a-facebook-revolution/ accessed on 11 April 2016 (2012)
12 Ibid.
providing more recent evidence to show how big data is used for state repression and governance in China.

Will the regime’s efforts in embracing big data deliver regime security? Will cutting-edge digital technology strengthen the authoritarian rule in the end? This article argues that it is too early to conclude the final outcome of the proactive approach taken by the Chinese government. Nonetheless, there is a potential danger that has been neglected by the relevant literature. The current “liberating technology” versus “repression technology” debate mainly focuses on the social challenge of digital technology to the state: whether digital technology would empower society or the state. To be sure, the changing nature of power structure between the state and the society (i.e. state-society-dimension of e-governance) is certainly important. However, what is missing is the changing power structure within the authoritarian system.

How will digital technology affect power structure among political elites in authoritarian regimes? Arguably, this question is as important, if not more so than that of the impact of digital technology on society-state relations. Indeed, empirical studies show that the majority of authoritarian regimes failed not because of being overthrown by the masses, but because of divisions amongst the elites. In other words, the internal challenge is far more dangerous than that posed by society to authoritarian regimes.

The current debate neglects the potential impact of digital technology on power structure within autocracy especially top ruling elites. As this article will note, the Chinese government’s big data approach further complicates the information war within the regime, i.e. use data for power struggle. This may be potentially destructive to offset all the previous efforts that the regime has made to maintain its rule. The following section will first explain the development of big data in China and the governance strategy towards big data, and will be followed by a discussion as to the potential danger of this approach.

China’s date with big data

In order to adapt to the forthcoming digital era, the Chinese government has made a series of efforts to prepare itself. Big data has been officially announced as an “emerging industry” in China, and thus specific national policies have been made to support its development. In 2015, the State Council of China has issued “the platform for action to promote the development of big data” in order to encourage social innovation and improve governance.

According to Chinese Premier Li Keqiang, the Chinese government will make an effort to promote China’s "cloud computing" to the international market as it did to China’s high-speed rail and nuclear power. The institutional approach has placed emphasis on big data as being more than just a slogan. The regime has established the Central Leading Group for Internet Security and Informatization, led by top leaders including the President Xi Jinping and Li Keqiang in order to embrace the digital era.

---


14 China, “国务院关于印发促进大数据发展行动纲要的通知 (State Council's Decision on Promoting the Development of Big Data).”

China has the largest population of mobile phone, internet and social media users. Up to late 2015, China has 688 million netizens and 620 million mobile phone users.\(^\text{16}\) Given that this is only half of its population, the number of netizens and mobile phone users may continue to grow, especially in rural areas of China. As such, there is considerable potential for the application of big data in China.\(^\text{17}\) In this context, the regime views data as a national strategic resource, and promotes better use of big data as a national strategy, with the hope of unlocking its business potential, as well as improving regime security and governance in China.

The regime’s growing interest in big data has sparked academic enthusiasm. China has organized the largest big data conferences in the world, including “Big Data World Forum”, “Big Data Technology Conference”, and “Big Data & Analytics Innovation Summit”.\(^\text{18}\) Although these conferences focus on the aspect of business potential and technological innovation, the Chinese government is also interested in the use of big data for the public sector. Thus, it has generously funded social sciences projects in order to understand the implications of big data for regime security and governance. The author’s brief search in late 2015 shows that the National Social Science Foundation of China has so far funded one hundred and twenty-one projects with “big data” in the title, ranging from political communication, to socialist ideology, to public governance.\(^\text{19}\) The National Social Science Foundation of China is the largest and the most authoritative official institution funding social sciences in China. It is directly led by China’s National Planning Office of Philosophy and Social Science, and its key purpose is to provide rigorous research for policy-making. Thus, its funding distribution reflects to some degree the interests of the government.

Among the one hundred and twenty-one projects on big data, most were funded in 2014 and 2015, and thus their exact research purposes are not yet clear to the public. Nonetheless, a brief review of project titles and subject reveals some valuable information, despite the interdisciplinary nature of some projects. Among the one hundred and twenty-one projects, thirty-four belong to the subject of Library, Information and Documentation Science, which is also the most popular subject. The major focus of the relevant projects is on the application of big data for improving information analysis and monitoring public opinion. Like other Western democratic states, the Chinese government sees big data as an opportunity to upgrade its state surveillance.

Given that big data is also considered as a means of improving governance, we should not be surprised to learn that management is the second most funded discipline. In addition, seventeen and three projects belong to the subjects of statistics and demographics respectively, which are mainly interested in how big data can improve government statistics. As this article will discuss later, the use of big data may lead to a revolution in China’s official statistics. Moreover, seventeen projects belong to Journalism and Communication with a focus on political communication. For example, a few projects are entitled “studies on youth online political participation in the era of big data”, “identity netizens and study public opinion based on the big data of behaviour and relations”, and “the mobilization mechanisms of social media based on the big data analysis”. They are clearly interested in understanding how big data may

---

\(^{16}\) China Internet Network Information Center. 中国互联网络发展状况统计报告 (Report of China’s Internet Development). (2016)


\(^{18}\) Ibid.

\(^{19}\) The search is conducted on 1 November 2015 from [http://fz.people.com.cn/skygb/sk/index.php/Index/search](http://fz.people.com.cn/skygb/sk/index.php/Index/search)
affect online behaviour and political participation – and more importantly, how the government should handle the emerging challenge.

While the above focus is relatively understandable and may commonly exist in other countries, studies on the implication of big data for socialist ideology may be relatively unique. In the subject of Marxism-Leninism and Scientific Socialism, projects such as “ideological security in the era of big data” and “innovative approach and methods to foster socialist core value among youth in the era of big data” are funded. As ideology plays a crucial role in maintaining authoritarian rule in China, the regime is concerned with the potential threat of digital technology to its socialist ideology, and more importantly, is eager to know how to deal with this threat.

As privacy is a major concern of digital data collection, four projects in Law have been funded. However, the focus is different from that of Western democracy countries. It is about how to protect consumers’ rights against enterprises instead of preventing excessive state control. Given the government’s strict control of funding, any project on how to protect civil rights will not be preferred. As this article shall discuss later, the lack of legal obstacle to protect civil liberty in China has allowed the regime to construct omnipresent government surveillance by equipping its security forces with cutting-edge digital technology.

Accordingly, the growing academic interest in big data has already generated a large number of articles studying social implication of big data with specific policy advice to the government, as the following sections will discuss.

Figure 1: A Brief Overview of Projects Funded by China’s National Foundation of Social Science with “Big Data” in the Title

---

**Big Data for Better Governance?**

As previously mentioned, a key motivation for the Chinese government’s enthusiasm is to improve public governance. This should be examined in the broader context of the practice of e-government in China. The idea of e-government is to promote a more effective and efficient public service with increased transparency of administrative acts by digitalization. Since the late 1980s, China has been pursuing this e-government strategy by using modern digital technology as part of its modernization program. With the development of the Internet and social media, the Chinese government has actively adapted its governance strategy to the digital era. For example, Weibo has been adopted into the governance strategy to consult public online opinion in order to rebuild its legitimacy. In this regard, Weibo is used to encourage more political participation and deliberation in the virtual world, and thus strengthen deliberative democracy.

The development of big data has great potential to bring about further changes. Take the Census and Statistics as an example. Since imperial times, China’s central government has been struggling to obtain the real information at the bottom. For thousands of years, the central regime has relied on the mid and local governments to collect and report information for decision-making. Yet driven by various bureaucratic and individual interests, real information is often distorted in the process of collecting and reporting. In Mao Zedong’s China, the false

22 Ibid.
23 Ibid.
reports on food production during the Great Leap Forward was a main reason that led to the Great Famine.24

In contemporary China, inflated GDP is another example. The central government of China relies economic data (especially GDP) to evaluate the performance of local leaders and thus creates a systematic incentive for local officials to manipulate local statistics. As Wallace’s study shows, China’s economic statistics is systematically manipulated by local officials in order to improve their career prospects.25 Even Li Keqiang acknowledged that China’s GDP number was “man-made” and unreliable, and he tracked the economy by using his preferred indicator: “Keqiang index”.26 While the central government is aware of this manipulation, the cost of auditing is often too high, and thus made the traditional way to acquire independent information at the bottom less likely. The development of big data may make this possible, and thus be a key for the central state to solve a governance problem that has lasted for thousands of years. What this means to the centre-provinces relations in China remains to be researched.

In addition to more reliable information, up-to-date statistics, for example, through the use of mobile phones and the Internet, are also a strength of big data.27 It is important to note that the traditional statistics are usually generated annually or even more – for example, China’s population census is usually conducted every ten years. Thus, the “real time” information provided by big data may bring a revolution in official statistics. Not surprisingly, China’s National Bureau of Statistics is motivated to use big data to improve the census and statistics. In the words of its director Ma Jiantang, official statistics should “sincerely embrace and take efforts in using big data”.28

At the local level, local governments have already heavily invested in big data. For example, the provincial government of Guizhou has been working with enterprises such as Alibaba to construct cloud computing infrastructure. Within this Cloud services platform, the provincial government shares its data with enterprises and encourages these enterprises to trade their data on this platform. Improving public services is a key goal of this platform. According to an official of Guizhou’s department of transportation, data integration helps with cooperation between police, fire, health care and thus efficiency was enhanced 1.5 times by joint duty assignments.29 Similarly, by using cloud services platform to obtain the data about tour, the government is able to predict the traffic load, the hotel load, or perhaps even security situation and thus be better prepared. Local citizens could also check road traffic and real-time traffic information services by using their phone or IPad to log in Guizhou’s Intelligent Transportation Cloud. These local initiatives were clearly supported by central leaders, as indicated by China’s

---

27 Cheng, "Big Data for Development in China."
top leader Xi Jinping’s visit to Guizhou’s big data center. During his visit, Xi concluded that “I understand it. It is reasonable for Guizhou to develop big data”.30

As previously mentioned, big data is also a national strategy. In 2015, the State Council of China issued an official document on how to use big data to improve public governance.31 This document assigns specific work to governmental departments with a timeline. For example, Ministry of Commerce, Administration of Quality Supervision, the Ministry of Industry and Information Technology and other governmental entities are asked to employ big data to establish a product information traceability system before 2016.32 In short, the Chinese government has actively adopted big data into its governance strategy in order to improve its bureaucratic efficiency and decision-making capacity.

From Big Data to Big Brother 2.0?

While acknowledging the positive effects of ‘big data’ on bureaucratic efficiency and quality of public services, big data also has the potential to lead to an intensification of state surveillance. Edward Snowden’s revelations astonished the world, in that extensive surveillance could still be secretly implemented in Western liberal democracies, despite the sophisticated and well-defined legal framework to protect citizen privacy against abuse of state power. In this regard, it is a common problem for all governments in the world regardless of their authoritarian or democratic nature.

Yet China’s state surveillance is notable for several reasons. The first is the exceptional economic strength of the Chinese government. After China’s emergence from the 2008 financial crisis, the authoritarian regime has become the most adequately resourced national government in the entire planet. China’s expenditure on internal security even surpasses its defence spending, despite the fact that China’s military budget is the second largest in the world behind the US. Therefore, the regime has the most adequate financial resources to invest in cutting-edge big data technology to equip its security force. This is demonstrated by its heavy investment on the “Golden Shield Project” (also known as “The Great Fire Wall of China”).

Second, there is a strong will to push back social autonomy by employing big data in China. Since 2011, the authoritarian regime has taken extra efforts in strengthens its so-called “social management capacity”33 – an official concept that refers to social control activities but downplays its coercive connotation – with the hope to construct a so-called “social management system with Chinese characteristics”34. The 18th party congress report used the term “social management” to replace “e-government”.35 It states that “We should improve the online services and advocate healthy themes on the Internet. We should strengthen social management of the Internet and promote orderly network

31 China, “国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见 (the State Council’s Decision on Use Big Data to Improve Service and Supervision),” (2015).
32 Ibid.
33 Zhangjun Li, “扎扎实实提高社会管理科学化水平 建设中国特色社会主义社会管理体系 (Improve Scientific Level of Social Management, Construct Social Management System with Chinese Characteristics),” People’s Daily 2011.
34 Ibid.
35 Noesselt, "Microblogs and the Adaptation of the Chinese Party-State's Governance Strategy.":456
operations in accordance with laws and regulations. We should crack down on pornography and illegal publications and resist vulgar trends”.36

Innovation is the key emphasis of “social management capacity” here. The Chinese government has called for all levels of governmental organs to innovate in social management capacity.37 In this context, with its distinct advantages, big data has naturally been adopted into the governance strategy in order to reshape the state-society relations to be in favour of the regime.

Third, related to the previous one, China has strong state power combined with weak civil awareness. As mentioned, the case of Snowden shows how extensive surveillance could still be implemented in democratic societies in which there is a strong legal framework for protecting civil rights. In comparison, the Chinese government faces almost no legal and practical obstruction when implementing ‘big data’ surveillance projects. The major obstacle to implementing big data for state surveillance lies in technical aspects instead of legal ones. At the same time, China’s evolving legal framework pertaining to citizen privacy seems to be erring on the side of the government – the recent announced state security law has allowed the security bureau full access to the data.38

This strong state power has also led to a different government-business relationship. Despite the majority of Internet giants in China not being state-owned enterprises, this does not prevent the regime from winning their full cooperation. Baidu, the Chinese version of Google, for example, is famous for its close relations with the regime and for following government guideline such as Internet censorship. The price of saying no to the government is likely to be unaffordable. In 2009, despite its size and global influence, Google’s unwilling stance to censor its service at the request of the Chinese government was made at the expense of losing almost the entire Chinese market – the largest Internet market in the world. Seven years later, Google might return to China with a more cooperative attitude to comply with the tight censorship requirements and Chinese law to store data locally in China39 – despite there is no guarantee that this attitude would help Google to win back what it lost in the Chinese market in the past few years.

Google’s painful lessons have demonstrated how helpless an enterprise can be when confronting the state power in China, despite Google’s global influence. This kind of government-business relationship has led to fewer obstacles for the Chinese government to access data owned by the private Internet giants than that in democratic societies. Therefore, adequate financial resources and strong institutional incentives combined with strong state power in China, has made the most sophisticated state surveillance more than a possibility.

While stepping up Internet censorship, the Chinese government has been strengthening its efforts to obtain private digital information. For example, at the request of the government, Weibo has introduced a real-name registration scheme since 2012 despite the operator’s

36 Ibid.:456
37 Li, “扎扎实实提高社会管理科学化水平 建设中国特色社会主义社会管理体系 (Improve Scientific Level of Social Management, Construct Social Management System with Chinese Characteristics).”
concern about its negative impact. All new Weibo users are required to fill in ID registration, as well as provide their real names, in order to sign up. This registration scheme is also linked with the database of Ministry of Public Security, which will verify the submitted registration information. The registration is not complete if the name and ID do not match. Thus, inaccurate registration is not allowed. The database of Weibo users has been shared by the police nationwide.

The government has made it very clear that the goal of this scheme is to “regulate the dissemination of objectionable information over the network”. It argues that this may help to undermine the spread of online information with the potential to lead to social protest. Indeed, the Chinese government is seriously concerned about the eruption of Arab Spring in China. The lesson that it learnt from Arab Spring is that the regime should have strict control over social network and the ability to respond to significant public opinion crisis. The registration system enables the security bureau to track and contain information sources if necessary.

By implementing these measures, the regime is able to make individuals in the real world responsible for their behaviours in the virtual world. This has no doubt created a sort of deterrent effect that forces a kind of self-censorship, by which social media users would be extra cautious when posting any sensitive information. In this regard, the administrative regulation on Weibo has undermined freedom of speech in virtual space. Notably, the control of freedom almost happened at the same time when the regime started to use Weibo to consult public online opinion and make itself more responsive to public demands in order to maintain its legitimacy. This indicates a clear strategy towards social media that combines co-optation with coercive control.

In addition to social media, the Chinese government has tightened its control on phone use. Despite cell phone technology facilitating the organization of rebel groups, the regime’s countermeasures have limited its actual effects. Since 2013, the Ministry of industry and information technology has made a new regulation on phone use which requires all telecom services to verify and register user’s ID when selling new phone cards. With various identity information, the government can track and lock the true identity of phone or Internet users. This enables the regime to contain the information source if there is any, and thus enhances its capacity to crack down on social unrest triggered by petitioners and dissidents. In addition, the regime has attempted to build its capacity to forecast large popular protest. As early as 2011, Beijing was considering an "Information Platform of Realtime Citizen Movement" system, which would track the precise movement of 17 million mobile phone users in the city. Once it is implemented, this would provide real-time information about the movement of the population, and thus inform any large-scale social protects.

Moreover, in order to further enhance its capacity to forecast large gatherings, the Chinese government has also constructed one of the most expensive and sophisticated closed-circuit television network on the planet. This network involves millions panoramic closed circuit cameras in public spaces that are working 24 hours a day, seven days a week. It covers highways, public parks, public transports and taxis, elevators and public streets. Not surprisingly, certain sensitive areas such as Tibet and Beijing have been particularly scrutinized. Since October 2015, Beijing’s Skynet Project has managed to monitor 100% public

---

41 China, “《电话用户真实身份信息登记规定》发布 (Announcement on Regulation of Identity of Phone Users),” (2013).
42 Leo Lewis, "China Mobile Phone Tracking System Attacked as ‘Big Brother’ Surveillance," The Times 2011.
streets in Beijing. This is made possible by at least 30 million cameras and the participation of 4,000 police in Beijing. The Beijing police are not shy to acknowledge that the purpose of these cameras is to prevent “crowd gathering” and street crime. Ironically, the real obstacle to the surveillance scheme is neither a legal obstruction, nor social opposition, but environmental pollution – the Haze has significantly undermined the visibility of these cameras, and the regime has to find new technology to allow its cameras to see through the smog.

In addition to the above surveillance, big data also enables the regime to track real-time information on the ideological trends of particular groups. The development of the media and the Internet has fundamentally challenged the CCP’s ideological indoctrination, as people are exposed to massive information and the traditional way of information control no longer works. Despite this new challenge, the CCP has also made use of this information in order to adapt its ideological indoctrination and political education in the era of big data. Many university educators see it as an opportunity to upgrade ideological indoctrination. Some scholars suggest that data mining should focus on the students’ digital information (including email, blog, Weibo and Wechat) in order to monitor ideological trends of Chinese college students.

It is important to review the historical context in order to understand the regime’s desire to monitor university students. In 1989, the nationwide student protests triggered by liberalism almost overthrew authoritarian rule. Although the CCP managed to end the protest by using military troops, this came at a huge social and political cost. Deng Xiaoping clearly pointed out that his reform program’s “biggest mistake was made in the field of education, primarily in ideological and political education.” Learning from the protest of 1989 and heeding Deng’s warning, the CCP has always kept an eye on the ideological trend of university students. It seems that the development of big data has provided an excellent opportunity to upgrade the regime’s student surveillance scheme. It is argued that big data may identify the ideological trend in a timely manner, and thus allow the regime to be more prepared for (if not prevent the happening of) the coming crises.

It is argued that the development of big data can help university educators improve their ability to lead the ideological trend of students. Some argue that ideological indoctrination could occur in a similar way to the improved delivery of online advertisement. For example, Chinese universities could make use of study record data, library book borrowing records and downloads, dissertations, and clicks on recent news made by students. By analyzing this data,
universities may find the focal point of the students, and thus improve their political education accordingly.49

The Chinese army has also considered big data as a way of strengthening its political education within the army. For example, an article in Liberation Army Daily argues that data is “a valuable resource of education” and suggests to establish a big database to monitor ideological trend of the army, which will collect data about soldiers’ learning and training program, online behavior, communications and liaison as well as their family and social relationship.50 It argues that this system will help to increase the effectiveness of political education in the army. The authoritarian regime in China has held absolute control of the army, and the latter is expected to act as the last line of defence for the regime. As noted above, it is the Chinese army that saved the authoritarian regime from the protest of 1989.

As absolute loyalty is required, the regime has always valued the importance of monitoring the ideological trends within the army. In the past, it relies on various formal and informal observations and talks as well as informants collecting the relevant information. Now, the information may be delivered by the collection of digital data in a more timely and reliable manner. In this case, big data is considered to be a means for the regime to better control the army, which might be used to crackdown social protects whenever necessary. Thus, digital technology serves as an indirect tool to repress the society by strengthening the authoritarian state’s control over its army.

More recently, an ambitious plan has been sketched out by the Chinese government, namely digitalization of individual archives (“dang’an” in Chinese). China’s dang’an system is borrowed from the Soviet Union, and records the performance and attitudes of individual citizens. Dang’an usually includes a resume, autobiography, political historical issues, education, and awards and punishments. Each category may contain detailed information such as grades in primary school and comments given by teachers. That is to say, a mistake made in primary school will follow an individual for their entire life once it is recorded in dang’an. Similarly, if any political mistake (e.g. anti-CCP speech) is made and recorded in the dang’an, one will never get rid of it.

In the old state-owned system, this dang’an was an essential document in deciding on continuing education, employment and promotion. Obviously, negative comments recorded in the dang’an will affect one’s education or professional career. For example, in Mao Zedong’s era, political censorship would decide on college admission. It is unlikely that an individual would get a university offer if political and ideological thought is recorded as negative in dang’an. This dang’an system has become increasingly irrelevant with the rise of the market economy in China. Hence, although it is still crucial to people who work for the government and state-owned enterprises, it has become obsolete and irrelevant for many.

Yet this dang’an system may revive with the development of big data, as the regime is keen to modernize this system.51 In the more recent five year state plan, a blueprint for a "social

---


50 Jun Lan, "政治教育要适应大数据时代要求 (Political Education Needs to Adapt to the Needs of Big Data Era),” 解放军报 (Liberation Army Daily) 2014.

credit system” has been made to strengthen social management.\(^{52}\) This system goes beyond Western (mainly American) financial credit rating systems, insofar as it aims to record the entire digital presence of citizens. In this regard, big data will enable the regime to digitize its dang’an system, and thus strengthen its social control. For example, the system may score citizens “based on a ‘patriotic’ criteria such as the content of their postings on social media”.\(^{53}\) Obviously, if a citizen makes a few speeches to call for popular protest, this may have a negative impact on the person’s future employment, education, and retirement benefit.

In this regard, if the previous state surveillance model is “big brother 1.0”, the development of digital technology and big data has been launching a revolution to upgrade it into “big brother 2.0”. This has shifted the traditional physical surveillance into digital ones, in which the state is more capable of collecting, consuming and sharing mega scale real time data.

**Authoritarian Backfire: the gamer changer of information war among elites?**

The above discussion has explored how the CCP attempts to employ big data to strengthen its authoritarian rule by improving governance and upgrading state surveillance. Will big data strengthen authoritarian rule in the long run? Although it may be too early to draw any firm conclusions at this stage, this article argues that the danger of this approach lies in the nature of authoritarian regime: power is concentrated in the hands of a few, with very few constraints. This nature may lead to the possibility of authoritarian backfire.

For an authoritarian regime, one of the biggest, if not the biggest threats is elite division. Empirical studies show that the collapse of most authoritarian regimes is caused by elite division instead of being overthrown by the masses.\(^{54}\) Instead of maintaining authoritarian rule, big data has great potential to destabilize the regime by intensifying the game of power struggle and enlarging its negative effects. In the era of big data, data means power, and thus, power will be granted to those who control the data. This might change the power structure within the authoritarian regime, in which power is highly centralized and held by a few elites. Massive digital data controlled by the security bureau may turn into a bomb at any moment if it falls into the wrong hands. This goes back to an old dilemma of authoritarian leaders: whether security forces are in the right (loyal) hands. In the era of big data, this dilemma may be whether data is in the right hands.

Indeed, data has always been linked to power struggles. Sensitive information, especially corruption, is frequently used in the interests of power struggles in China. Before China’s once-in-a-decade power transition, various political forces fed the overseas media such as *New York Times* with corrupting materials\(^{55}\), including the family corruption of the then Premier Wen Jiabao and Vice President Xi Jinping who were the political opponent of the then security tsar.

---

\(^{52}\) Ibid.


Zhou Yongkang. Soon after Xi took power, Zhou was arrested and one of the accusations was leaking state secrets.56

In the name of anti-corruption campaigns, Xi also launched waves of purges on Zhou’s supporters and political alliance, including Ling Jihua. Ling had worked for years as the personal secretary of the former Hu Jintao and the Director of the CCP’s General Office, and thus controlled significant amount of sensitive information about the party and leaders. Ling Jihua’s brother Ling Wancheng fled to and shared this information with the US, despite Ling Wancheng’s denial.57 According to different sources, the information includes “details on Chinese procedures for launching nuclear weapons, the personal lives of China’s leaders, and arrangements for their security and for the protection of the Zhongnanhai leadership compound in central Beijing”.58 China’s strong desire to get Ling Wancheng back caused some diplomatic conflicts with the US at the time.59 All these examples demonstrate the importance of data in power struggles among the top Chinese leaders. Driven by Xi Jinping’s ambitious anti-corruption campaign, this kind of political scandal will only become more intense.

With the development of digital technology, data will become less fragmented, decentralized, and non-digital, and thus more powerful. In this regard, the digital sources of data may be the game changer of the power struggle in authoritarian regimes. If confidential data is highly concentrated in the hands of a few powerful individuals or agencies, it may seriously harm regime legitimacy and elite cohesion when misused. It is also important to note the difference between authoritarian and democratic systems here. In democratic societies, the legitimacy of the regime is separate from that of the political system.60 Corruption, for example, will reduce the regime’s legitimacy, and thus lead to regime change without significantly affecting the legitimacy of the democratic system itself. However, in authoritarian systems, the regime and political system are combined into one, as is their legitimacy. Thus, if a Chinese Edward Snowden were to disclose the digital evidence of massive corruption among Chinese leaders, this would not only harm the leadership but the entire political system.

If non-digital corruption materials could intentionally be used for the purposes of combating political opponents, so can the massive digital information. This would grant enormous power to the security forces that controlled the data. The abuse of power by security forces is not new in China – they use their power to purse individual and departmental interests. For example, the Deputy Minister of National Security, Ma Jian, was reported to use technical means (including recording, reconnaissance and eavesdropping) to benefit certain businessmen.61 Similarly, it is reported that some Chinese leaders are using their own security

59 Ibid.
61 Xiankang Cui, Ning Yu, and Ran Liu, "郭文贵围猎高官记：从结盟到反目 (Guo Wengui’s Story to Hunt Senior Officials: From Alliance to Enemy)," 财新周刊 (Caixin Weekly) 12 (2015).
forces to spy and wiretap each other. The former party head of Chongqing, Bo Xilai, was reported to use security force to plant electronic devices to spy on the then Chinese president Hu Jintao. A crime of the security tsar Zhou Yongkang is leaking state secrets. In the future, digital data will definitely be employed in the power struggle. By then, the regime will pay a much higher price to purge the security tsar like Zhou Yongkang, as he or she may control the secrets of all through digital technology.

Similarly, other leaders may hold some digital data through their own institutions and network. In this situation, leaking data to combat political opponents would be more destructive. It may also be a suicide mission, as opponents will also likely to expose the data in their hands as revenge. This orderless data battle during power struggles may cause significant trouble to authoritarian regimes.

There is a further scenario, too. In the previous scenario, digital data may be highly destructive to a regime once it is used for factional struggles. However, precisely because of this massive destruction, it may create a sort of deterrent effect among political actors, and thus change the doctrine of the use of data for power. In this scenario, all political actors rationally recognize the destructive power of the digital data and understand the possible revenges that may be taken by others; therefore, they are likely to be more cautious in using the data. In this sense, digital data becomes the ultimate weapon, and its deterrent effects will serve the purposes of self-defence, and thus a relative stable elite politics might be maintained. This is quite similar to the use of nuclear weapon among nations.

Nonetheless, there is no guarantee that such stability would last for long. Accidents or misjudgement are always possible. One simple mistake may push the button to start the self-destruction of the entire regime. It is too arbitrary to predict the sustainability of this relative stable elite politics in the era of big data, but we should always bear in mind that the use of big data may backfire against the authoritarian regime.

The current use of digital data in China’s anti-corruption campaign has made the above scenarios more than a possibility. The regime has already started to collect personal banking and credit information to identify the network of corrupt officials and collect relevant evidence. How far this will empower security forces certainly merits further observations. Nonetheless, given that China’s anti-corruption campaign is always related to power struggle, the participation of big data in the anti-corruption campaign will be no exception. Even if these data are not deliberately used for power struggle, data leak may significantly undermine regime legitimacy and the possibility of the removal of leaders. This is demonstrated by the Panama papers, which has led to the downfall of Iceland prime minister.

All of the above dates back to an old question but in a new context: how will elites use information against each other in the era of big data? When these massive digital sources of data are used for power struggles, the negative effects may be more damaging to regime legitimacy and elite cohesion than ever before. In this regard, they may offset all the efforts that have been made to strengthen authoritarian rule. That is to say, the Chinese government’s big data approach may also pose a threat to the authoritarian regime. This possibility has made the implications of big data for authoritarian rule more difficult to assess as a whole.

---

Concluding remarks: authoritarian resilience?

The debate over the resilience of authoritarianism tends to be both an ancient and eternal one. To a large extent, this debate has revolved around the question of whether the authoritarian regime possesses sufficient adaptive capacity to stay relevant in the rapidly changing environment. As Internet and communication technology have been transforming our society into a digital one, this debate has become more heated, because the challenges facing authoritarian regimes in governing this dynamic and plural, yet increasingly divisive and crisis-prone society are becoming more serious and multidimensional.

The advent of the big data era has complicated authoritarian governance by being a double-edged sword which has enormous potential to improve public service, or threaten civil liberty, depending on the political context within which it is deployed. As this article has discussed, in China, the authoritarian regime has proactively embraced big data in order to adapt to the digital era. While there is great potential for big data to improve the governance model and strengthen authoritarian rule, the nature of the authoritarian regime has made this approach particular dangerous.

When massive digital data is highly centralized in the hands of a few with few constraints, the damage will be inestimable once it is used for power struggle. While it may also be a problem for democratic system, this damage will only destroy the regime, but not the political system. On the contrary, when it comes to the case of authoritarian regime in which the legitimacy of the regime and political system are combined, big data has great potential to undermine the entire authoritarian system in China that is actively embracing it. In this regard, big data may bring fundamental changes to the game of thrones that is largely neglected by the relevant literature. How will digital technology change the power struggle within authoritarian regimes? This is certainly a topic that deserves further analyses. As mentioned, to authoritarian leaders, it highlights an old question in a new context: how to find loyal individuals who can control security forces, and thus, data itself.

A more accurate understanding of the challenges brought by big data to autocracy may provide us a unique look into the development of authoritarian governance in the digital era. This is especially relevant in the broader context of China’s rise. China’s re-emergence as a global power has profound implications for the future world order. In the pages of this journal, this has already generated a hot debate on the rise of China. Yet, we will not be able to grasp

---


the essence of China’s rise without understanding its domestic dynamics. Observing the resilience and vulnerability of its authoritarian nature in the information age is a vital part of the process.