China’s date with big data: will it strengthen or threaten authoritarian rule?

JINGHAN ZENG*

‘Big data’ is perhaps one of today’s most fashionable terms.¹ The data revolution has allowed the application of big data to be extended to every aspect of our digital society. While the private sector has invested heavily in big data, it also attracts the attention of the public sector, given its great potential to contribute to governance. In the public health care sector, for example, big data has launched a revolution by reducing overall cost, improving efficiency, predicting epidemics and curing disease.² Despite its recent emergence, the rise of big data has already attracted considerable attention on account of its implications for transforming governance. Hitherto, however, the primary focus has been on democratic states, with little attention directed to authoritarian regimes. While this may be understandable enough, given that digital technology is more developed in democratic countries, as is the motivation for improving public governance, it is nevertheless a shortcoming in the overall consideration of the subject.

Indeed, the rise of big data has brought no less change to authoritarian regimes such as China’s than to democratic ones—for better or worse. In adapting to the digital era, the Chinese government has been enthusiastic about big data. In November 2015, the State Council of China officially announced the development of big data as a national strategy.³ The Chinese government is interested not only in big data’s potential in respect of business activity and technological innovation, but also in its potential to improve governance and upgrade state surveillance. China’s weak awareness of civil rights and the strength of the state, both in its financial capacity and in its willingness to resist social autonomy, open up the possibility—perhaps more than a possibility—that cutting-edge ‘big data’ technology could be used to construct the most sophisticated electronic police

* I am grateful to Tim Stevens and two anonymous reviewers of International Affairs for their valuable comments on the earlier version of this article. I am also deeply indebted to Yuefan Xiao for our discussions that generated many valuable ideas included in this article. Of course, all mistakes are my own.

¹ For a working definition of the term in the context of this article, please see the next section.


³ State Council of China, ‘Guowuyuan guanyu yinfa cujin dashuju fazhan xingdong gangyao de tongzhi’ [State Council’s decision on promoting the development of big data], 13 Aug. 2015, http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 25 Sept. 2016.)
state on the planet. Policy-makers and scholars can learn a great deal about China’s political development from paying greater attention to this phenomenon.

This article describes in detail China’s governance strategy with regard to big data and its implications for authoritarian rule by examining both policy documents and academic studies on big data in China. While the regime in China aims to use digital technology to strengthen its rule, its authoritarian nature might make this approach dangerous. This article argues that the possibility of ‘authoritarian backfire’—that the use of digital data on a massive scale might backfire against the authoritarian regime—should not be underestimated. When data is highly concentrated in the hands of a few powerful individuals or agencies, it may be sufficiently destructive to damage the entire authoritarian regime if used in the interests of competing actors in power struggles. In this respect, the regime’s efforts to strengthen authoritarian rule by embracing big data may end up undermining it.

The following sections will elaborate this argument in detail. The first reviews the current debate over the implications of digital technology for authoritarian rule. After a brief overview of the growing interest in big data in China, the article will then explore how the Chinese government has employed big data to improve its governance and upgrade its state surveillance and thereby to strengthen its authoritarian rule. It will then turn to consider how the use of big data may backfire against the authoritarian regime, before offering some concluding remarks on the resilience of authoritarianism.

Debating digital technology: ‘liberating technology’ versus ‘repressive technology’

Before reviewing the debate on the implications of digital technology, it is important to consider what ‘big data’ actually means—particularly as it is an umbrella term that may have different meanings in different contexts. In China, it is not a uniform concept, and is sometimes used as a catchphrase. Thus, the Chinese government’s approach to big data is best considered as a broad and less than coherent strategy of adaptation to governance by electronic means. While many western states may be using similar strategies, the nature of the political system in China introduces a key difference in how this strategy is envisaged. In the case of democratic states, the main purpose of the adaptation 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 there 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 to maintain its hold on 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 here to an
China’s date with big data

‘explosion in the quantity and diversity of high frequency digital data’.\(^4\) It is also important to draw a distinction between big data as a phenomenon and the way attempts are made to use the data. In China, phrases such as ‘to promote the development of big data’ or ‘develop big data’ appear frequently in official documents. However, these phrases refer to improvements in the way that big data is used and applied, rather than to developing big data as a phenomenon.

With the development of the internet, user-generated content has gradually become dominant. This has sparked lively discussion about the changing nature of information dissemination in authoritarian regimes. What are the implications of the development of digital technology for authoritarian rule? Will it undermine or strengthen such regimes? The literature presents two contrary perspectives: ‘liberation technology’ and ‘repression technology’. Those who adopt the first perspective argue that modern information and communication technology can deliver liberation to individual citizens by ‘expand[ing] political, social, and economic freedom’.\(^5\) Unlike traditional media, the internet has empowered society by promoting information flow.

The internet, in particular, exposes ‘netizens’ to foreign ideas that were not previously available to them.\(^6\) 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.\(^7\) In particular, social media sites have attracted considerable academic attention owing to their potential as a ‘liberating technology’ that challenges authoritarian rule through collective mobilization. For example, some argue that social media played a significant role during the Arab Spring by facilitating communication among individuals and the organization of political protests. Thus, the Arab Spring has been described by many as a ‘Facebook/Twitter revolution’. It is argued that the development of the internet and social media empowers individuals, and fundamentally changes the way in which information is produced, consumed and shared. These trends present a systematic challenge to authoritarian rule, and inevitably undermine it.\(^8\)

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 in Iraq and Syria (ISIS), and other criminal groups have also taken advantage

of social media for sinister goals rather than liberating purposes. In addition, the view of the Arab Spring as a ‘Facebook/Twitter revolution’ may overstate the role of social media.\textsuperscript{9} While social media certainly matter, they were not the decisive factor that led to the Arab Spring.

The ‘repression technology’ perspective considers digital technology as a tool by which authoritarian regimes can strengthen their repression. Internet censorship obviously plays a key role. Studies by Gary King, Jennifer Pan and Margaret Roberts show how the Chinese regime strategically uses internet censorship to allow some criticism of the government, but suppresses use of the internet to call for social protest.\textsuperscript{10} In addition to eliminating social mobilization through the internet, authoritarian regimes use the internet to provide information in favour of the government.\textsuperscript{11} Digital technology makes this possible by \textit{blocking} information flow. The authoritarian regime has benefited from its heavy investment in the Golden Shield Project,\textsuperscript{12} otherwise known as the Great Firewall of China. Instead of serving a liberalizing purpose, this 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 (the Chinese version of Twitter), especially after Xi Jinping took power in 2012.\textsuperscript{13} On the one hand, it has made efforts to contain negative opinions about the government through this channel. For example, the Weibo accounts of opinion-formers such as Zhang Lifan were closed because of their outspoken criticism of the government. Xue Manzi, an influential opinion-former, was even arrested on a charge of soliciting prostitution. On the other hand, the regime has launched a series of media offensives, encouraging party media and officials to open Weibo accounts in order to fight for the government on the online battlefield of public opinion. These efforts have successfully contained the spread of negative comments about the government on Weibo.\textsuperscript{14}

Therefore the ‘repression technology’ perspective holds that digital technology, instead of undermining authoritarian rule, actually empowers authoritarian states by making them more capable of repressing civil rights. This article will contribute to the debate by providing more recent evidence to show how big data is used for purposes of state repression and governance in China.

Will the regime’s efforts to embrace big data deliver regime security? Will cutting-edge digital technology strengthen authoritarian rule in the end? This article argues that it is too early to predict the final outcome of the proactive

\textsuperscript{9} Sara Reardon, ‘Was the Arab Spring really a Facebook revolution?’, \textit{New Scientist}, 3 April 2012, https://www.newscientist.com/article/mg21428396-300-was-the-arab-spring-really-a-facebook-revolution/.


\textsuperscript{12} The Golden Shield Project is a blockade and surveillance system that is operated by China’s Ministry of Public Security to block sensitive information from abroad and to monitor domestic cyberspace.

\textsuperscript{13} Zeng, \textit{The Chinese Communist Party’s capacity to rule}.

\textsuperscript{14} Zeng, \textit{The Chinese Communist Party’s capacity to rule}.
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 focuses mainly on the social challenge of digital technology to the state: whether digital technology empowers society or the state. To be sure, the changing nature of the power structure between the state and society (that is, the state–society dimension of e-governance) is certainly important. However, what is missing from this analysis is the changing power structure within the authoritarian system.

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

The current debate neglects the potential impact of digital technology on power structures within authoritarian regimes, especially within the highest ruling elites. As this article will note, the Chinese government’s big data approach further complicates the information war within the regime, that is, the use of data in power struggles. This may be sufficiently destructive to offset all the previous efforts that the regime has made to maintain its rule.

**China’s date with big data**

The Chinese government has made a series of efforts to prepare itself for the digital era. Big data has been officially announced as an ‘emerging industry’ in China, with specific national policies formed to support its development. In 2015, the State Council of China 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 for China’s high-speed rail and nuclear power. The institutional approach has placed emphasis on big data as 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 the Premier Li Keqiang, in order to embrace the digital era.

China has the largest population of mobile phone, internet and social media users of any country in the world. By late 2015, China had 688 million internet

---


users and 620 million mobile phone users. Given that these numbers represent only half the country’s population, they may well continue to grow, especially in rural areas. As such, there is considerable potential for the application of big data in China. 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.

The regime’s growing interest in big data has sparked academic enthusiasm. China has organized the largest big data conferences in the world, including the ‘Big Data World Forum’ (2011–17), ‘Big Data Technology Conference’ (2013–15), and ‘Big Data and Analytics Innovation Summit’ (2015, 2016, 2017). Although these conferences focus on the business potential and technological innovation aspects of big data, the Chinese government is also interested in the use of big data for the public sector. Thus, it has generously funded social science projects in order to gain understanding of 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 116 projects with ‘big data’ in the title, ranging from journalism and communication to socialist ideology to management. 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 allocation reflects to some degree the interests of the government.

Among the 116 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 subjects reveals valuable information, despite the interdisciplinary nature of some projects. Thirty-four projects, the largest group, fall in the category of library, information and documentation science. The primary focus of these projects is on the application of big data for improving information analysis and monitoring public opinion. Like 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 projects form the second-largest group. A further 17 and three projects are on the subjects of statistics and demographics respectively, and are mainly concerned with how big data can improve government statistics. As this article will discuss below, the use of big data may lead to a revolution in China’s official statistics. Another 17 projects focus on journalism and communication, in particular political communication.

---

20 Cheng, Big data for development in China.
21 The search was conducted on 1 Nov. 2015 from http://fz.people.com.cn/skygb/sk/index.php/Index/seach.
For example, the titles of these projects include ‘Studies on youth online political participation in the era of big data’, ‘Identify 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’. The interest is clearly in understanding how big data may affect online behaviour and political participation—and, more importantly, how the government should handle the emerging challenge.

While this focus is understandable and may be replicated in other countries, studies on the implications of big data for socialist ideology are arguably 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 values 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 in western democratic countries: in China, it is on how to protect consumers’ rights against enterprises, not how to prevent excessive state control. Given the government’s strict control of funding, any project on how to protect civil rights will not be favoured. As this

---

22 Zeng, *The Chinese Communist Party’s capacity to rule*. 

---

*International Affairs* 92: 6, 2016
Copyright © 2016 The Author(s). International Affairs © 2016 The Royal Institute of International Affairs.
article will discuss below, the lack of legal civil liberties protection in China has allowed the regime to construct omnipresent government surveillance by equipping its security forces with cutting-edge digital technology.

Thus the growing academic interest in big data has already generated a large number of articles studying the social implications of big data and providing specific policy advice to the government.

Big data for better governance?

As previously mentioned, a key element in the Chinese government’s enthusiasm for big data 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 use digital technology to promote a more effective and efficient public service with increased transparency of administrative acts. China has been pursuing this e-government strategy as part of its modernization programme since the late 1980s. 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 co-opted into the governance strategy as a means of consulting public online opinion in order to bolster the regime’s legitimacy. In this respect, Weibo is used to encourage more political participation and deliberation in the virtual world, and thus to 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 real information at ground level. For thousands of years, the central regime has relied on the regional and local governments to collect and report information for decision-making. Yet these processes have often been distorted by various bureaucratic and individual interests. In Mao Zedong’s China, for example, the false reports on food production during the Great Leap Forward were one of the main reasons for the Great Famine.

In contemporary China, inflated GDP is another example. The central government of China relies on 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 are systematically manipulated by local officials in order to improve their career prospects. Even Li Keqiang has acknowledged that China’s GDP figure was ‘man-made’ and unreliable, and that he tracked the economy by using his preferred

24 Noesselt, ‘Microblogs and the adaptation of the Chinese party-state’s governance strategy’.
25 Noesselt, ‘Microblogs and the adaptation of the Chinese party-state’s governance strategy’.
China’s date with big data

indicator, the ‘Keqiang index’. While the central government is aware of this manipulation, the cost of auditing is often too high, and thus it is unlikely for the central regime to systematically acquire independent information at ground level. The development of big data may make this possible, and thus offer the central state a solution to a governance problem that has lasted for thousands of years. What this means for relations between the centre and the provinces in China remains to be researched.

In addition to offering the prospect of more reliable information, big data also enables more up-to-date statistics to be gathered, for example through the use of mobile phones and the internet. It is important to note that the traditional statistics are usually generated annually or even less frequently—for example, China’s population census is usually conducted every ten years. Thus, the ‘real time’ information provided by big data may bring about a revolution in official statistics. Not surprisingly, China’s National Bureau of Statistics is keen 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’.

Local governments have already invested heavily 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. Improving public services is a key goal of this platform. According to an official in Guizhou’s department of transportation, data integration helps with cooperation between police, fire and health care services, and has resulted in a 50 per cent improvement in efficiency through joint duty assignments. Similarly, by using the cloud services platform to obtain data about tourism, the government is able to predict the traffic load, the hotel load, perhaps even the security situation, and thus be better prepared. Local citizens can also access real-time information on road and other traffic services by using their phones or tablets to log in to Guizhou’s ‘intelligent transportation cloud’. These local initiatives were clearly supported by central leaders, as indicated by China’s top leader Xi Jinping’s visit to Guizhou’s big data centre, during which he commented: ‘I understand it. It is reasonable for Guizhou to develop big data.’

As noted above, big data is also a national strategy. In 2015, the State Council of China issued an official document on how big data was to be used to improve

29 Cheng, Big data for development in China.
public governance. This document assigned specific work to governmental departments, with a timeline. For example, the Ministry of Commerce, the Administration of Quality Supervision, the Ministry of Industry and Information Technology and other governmental entities were asked to employ big data to establish a product information traceability system before 2016. In short, the Chinese government has actively co-opted 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 big data may certainly have positive effects on bureaucratic efficiency and quality of public services, it also has the potential to lead to an intensification of state surveillance. Edward Snowden’s revelations of 2013 astonished the world, in showing that extensive surveillance could still be secretly implemented in western liberal democracies, despite the existence of sophisticated and well-defined legal frameworks to protect citizen privacy against the abuse of state power. In this regard, the surveillance potential of big data is a problem applying to all governments in the world, whether of an authoritarian or a democratic nature.

That said, China’s state surveillance apparatus is notable for several reasons. The first is the exceptional economic strength of the Chinese government. Since China’s emergence from the 2008 financial crisis, the Beijing regime has become the best-resourced national government on the planet. China’s expenditure on internal security surpasses even its defence spending, and China’s military budget is the second largest in the world behind the US. The Beijing regime thus has at its disposal vast financial resources to invest in cutting-edge big data technology to equip its security force. This is demonstrated by its heavy investment in the ‘Golden Shield Project’ or ‘Great Firewall of China’.

Second, there is a strong will to use big data in China to inhibit social autonomy. Since 2011, the authoritarian regime has made extra efforts to strengthen its so-called ‘social management capacity’—an official concept that refers to social control activities while downplaying its coercive connotations—with the hope of constructing a so-called ‘social management system with Chinese characteristics’. The 18th Party Congress report used the term ‘social management’ to replace ‘e-government’, stating that:

34 State Council of China, ‘Guowuyuan bangongting’.
36 Zhangjun Li, ‘Zaza 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].
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 operations in accordance with laws and regulations. We should crack down on pornography and illegal publications and resist vulgar trends.38

The key emphasis in ‘social management capacity’ is on innovation. The Chinese government has called for governmental organs at all levels to innovate in social management capacity.39 In this context, big data, with its distinct advantages, has naturally been adopted as part of the governance strategy in order to reshape state–society relations in favour of the regime.

A third point, related to the second, is that China has strong state power combined with weak awareness of civil rights. As noted above, the Snowden case shows how extensive surveillance can be implemented even in democratic societies in which there is a strong legal framework for protecting civil rights. The Chinese government, by comparison, faces almost no legal or practical obstruction to implementing ‘big data’ surveillance projects. Indeed, the major obstacle to implementing big data for state surveillance is not legal but technical. At the same time, China’s evolving legal framework pertaining to citizen privacy seems to be erring on the side of the government: the recently announced state security law, for example, has allowed the security bureau full access to the relevant data.40

This strong state power has also led to a particular relationship between government and business. Although most of the big internet companies in China are not state-owned enterprises, this does not prevent the regime from achieving their full cooperation. Baidu, for example, the Chinese version of Google, is famous for its close relations with the regime and for following government guidelines on matters 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 unwillingness to censor its service at the request of the Chinese government cost it the loss of almost the entire Chinese market—the largest internet market in the world. Seven years later, Google may be about to return to China with a more cooperative attitude to its tight censorship requirements and Chinese law on local storage of data within China41—even though there is no guarantee that this attitude would help Google to win back what it has lost in the Chinese market in the interim.

This episode demonstrated how helpless an enterprise can be, even one with the global influence wielded by an internet giant such as Google, when confronting...
the state power in China. This kind of government–business relationship has meant fewer obstacles for the Chinese government in seeking to access data owned by the private internet giants than in democratic societies.

As a result of all these factors—vast financial resources, strong institutional incentives and strong state power—the most sophisticated state surveillance is more than a possibility in China.

While stepping up internet censorship, the Chinese government has also been strengthening its efforts to obtain private digital information. For example, at the request of the government, Weibo introduced a real-name registration scheme in 2012 despite the operator’s 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 linked with the database of the 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 possible. 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’.42 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 in China of a phenomenon similar to the Arab Spring. The lesson it learned from the Arab Spring is that the regime should have strict control over the social network and the ability to respond to any significant crisis in public opinion. The registration system enables the security bureau to track and contain information sources should it feel the need to do.

By implementing these measures, the regime is able to hold individuals in the real world to account for their behaviour in the virtual world. This has no doubt created a deterrent effect in the form of a kind of self-censorship, by which social media users will be especially cautious about posting any sensitive information. In this way, the administrative regulation on Weibo has undermined freedom of speech in virtual space. Notably, this control of free expression was imposed at around the same time that the regime started to use Weibo to consult public opinion online and show 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.

The Chinese government has also tightened its control on phone use. While mobile phone technology is widely recognized as facilitating the organization of rebel groups, the regime’s counter-measures have limited its use for such ends in practice. In 2013 the Ministry of Industry and Information Technology introduced a new regulation on phone use which requires all telecom services to verify and register users’ ID when selling new phone cards.43 Armed with such informa-

43 Ministry of Industry and Information Technology, ‘Dianhua yonghu zhenshi shenfen xinxi dengji guiding
China’s date with big data

tion, the government can track the true identity of phone or internet users and lock accounts. This both enables the regime to contain the sources of information and 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-scale 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.44 Once implemented, this would provide real-time information about the movement of the population, and advance warning of any emerging large demonstrations.

Moreover, in order to enhance further its capacity to forecast large gatherings, the Chinese government has constructed one of the most expensive and sophisticated closed-circuit television networks on the planet. This network involves millions of panoramic cameras in public spaces working 24 hours a day, seven days a week. It covers highways, public parks, public transport and taxis, lifts and public streets. Not surprisingly, certain sensitive areas such as Tibet and Beijing have been particularly closely scrutinized. Since October 2015, Beijing’s Skynet Project has managed to monitor 100 per cent of public streets in Beijing.45 This is made possible by at least 30 million cameras and the participation of 4,000 police in the city. The Beijing police are not shy of acknowledging that the purpose of these cameras is to prevent ‘crowd gathering’ and street crime.46 Ironically, the real obstacle to the surveillance scheme is neither a legal obstruction nor social opposition, but environmental pollution—the haze or smog has significantly undermined the visibility of these cameras, and the regime has to find new technology to allow its cameras to see through the occluded air.47

In addition to the surveillance through the means described above, 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 ideological indoctrination by the Chinese Communist Party (CCP), as people are exposed to massive amounts of information and traditional ways of controlling information no longer work. The CCP has responded to this new challenge by itself making use of increased amounts of information to adapt its ideological indoctrination and political education to the era of big data. Many university educators see the new era as offering an opportunity to upgrade ideological indoctrination. Some scholars suggest that data mining should focus

---


46 Jingya Zhang, ‘Benshi chengqu jiaoqu chengguan tantou quan fugai’ [Probes fully cover our city].

Jinghan Zeng

on students’ digital information (including email, blog, Weibo and Wechat—a powerful messaging and calling application) in order to monitor the ideological trends of Chinese college students.48

It is important to see the regime’s desire to monitor university students in historical context. In 1989, the nationwide student protests triggered by tentative moves towards liberalism almost overthrew authoritarian rule. Although the CCP managed to end the protests by using military force, this came at a huge social and political cost. Deng Xiaoping noted explicitly that his reform programme’s ‘biggest mistake was made in the field of education, primarily in ideological and political education’.49 Learning from the protests of 1989 and heeding Deng’s warning, the CCP has since kept a constant eye on ideological trends among 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 ideological trends in a timely manner, and thus allow the regime to be better prepared for (if not prevent the occurrence of) a coming crisis.50

It is also argued that the development of big data can help university educators improve their ability to direct the ideological trend of students. Some argue that ideological indoctrination could occur in a similar way to the improved delivery of online advertisements. For example, Chinese universities could make use of students’ study record data, library book borrowing records and downloads, dissertations, and clicks on recent news reports. By analysing these records, universities may be able to identify the issues on which students are focusing, and adjust their political education accordingly.51

The Chinese Army has also considered big data as a way of strengthening its political education within the armed forces. For example, an article in Liberation Army Daily argues that data is ‘a valuable resource of education’ and suggests that a big database be established to monitor ideological trends in the army by collecting data about soldiers’ learning and training programmes, online behaviour, communications and liaison as well as their family and social relationships.52 It argues that this system will help to increase the effectiveness of political education in the army. The authoritarian regime in China has absolute control over the army, which 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 protests of 1989.

48 Haiying Cui, ‘Dashuju shidai gaoxiao wangluo sixiang zhengzhi jiaoyu de jiazhi weidu yu shixian fangshi’ [Value and practice of online political education in the big data era], Heilongjiang gaojiao yanjiu [Heilongjiang researches on higher education] 3: 251, 2015, pp. 31–6.
50 Haiying Cui, ‘Dashuju shidai gaoxiao wangluo sixiang zhengzhi jiaoyu de jiazhi weidu yu shixian fangshi’ [Value and practice of online political education in the big data era].
51 Zhongyu Hu and Liya Huang, ‘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], Xuesiao dangjian yu sixiang jiaoyu [Party building and political education in universities], no. 484, 2014, pp. 64–6.
China’s date with big data

As absolute loyalty is required of the armed forces, the regime has always set great store by monitoring ideological trends within them. In the past, it has relied for this on various formal and informal observations and talks, and on the collection of relevant information by informants. 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 exercise better control over the army, which may be used to crack down on social protest whenever necessary. Thus, digital technology serves as an indirect tool for social repression by strengthening the authoritarian state’s control over its army.

More recently, an ambitious plan has been sketched out by the Chinese government for digitalization of individual archives. Known as dang’an in Chinese, this system is borrowed from the Soviet Union, and records the performance and attitudes of individual citizens. Each dang’an record usually contains detailed personal and professional biographical information, including any political/historical issues, education, and awards and punishments. For example, the education section may contain detailed information about grades attained in primary school and comments made by teachers, so that a mistake made in primary school will follow an individual for their entire life once it is recorded in the dang’an. Similarly, if any political mistake (e.g. an anti-CCP speech) is made and recorded in the dang’an, it will remain permanently on the individual’s record.

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 an individual’s education or professional career. For example, in Mao Zedong’s era, the political censors would make decisions on college admissions, and it was unlikely that an individual would be offered a university place if his or her political and ideological thought was recorded as negative in the 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, for many others it has become obsolete and irrelevant.

However, the regime is keen to modernize the dang’an system with the development of big data. The most recent five-year state plan includes a blueprint for a ‘social credit system’ to strengthen social management. This system goes beyond western (mainly American) financial credit rating systems in so far as it aims to record the entire digital presence of individual citizens. This digitized dang’an system will enable the regime to strengthen its social control. For example, the system may assess citizens ‘based on “patriotic” criteria such as the content of their postings on social media’. Obviously, if a citizen makes a few speeches calling for popular protest, this is likely to have a negative impact on their prospects of future employment, education and even retirement benefit.

---

54 Yap Yap and Wong, ‘China wants to tap big data to build a bigger brother’.
If the previous state surveillance model may be called ‘Big Brother 1.0’, the development of digital technology and big data has launched a revolutionary upgrade into ‘Big Brother 2.0’. In this new version, the traditional physical surveillance has been transmuted into digital surveillance, giving the state increased capability to collect, consume and share data in real time on a massive scale.

Authoritarian backfire: the game-changer of information war among elites?

The above discussion has explored the CCP’s attempts to employ big data to strengthen its authoritarian rule by improving governance and upgrading state surveillance. But 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 lies in the very nature of an authoritarian regime, where power is concentrated in the hands of a few, with very few constraints. This may lead to the possibility of authoritarian backfire.

For an authoritarian regime, one of the biggest threats, if not the biggest, is elite division. Empirical studies show that the collapse of most authoritarian regimes is caused by elite division rather than overthrow by the masses.\(^5\) Big data has great potential to destabilize such a regime by intensifying the power struggles within it and enlarging their 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 highly centralized authoritarian regime. The massive amounts of digital data controlled by the security bureau could turn into an information bomb at any moment if they were to fall into the wrong hands. This is a new version of an old dilemma for authoritarian leaders: how to ensure the security forces are in the right (loyal) hands. In the era of big data, this dilemma may be whether data are kept in the right hands.

Indeed, data has always been linked to power struggles. Sensitive information, especially about corruption, is frequently used by competing interests in power struggles in China. Before China’s most recent once-in-a-decade power transition, various political forces fed overseas media outlets such as the New York Times with material on corruption,\(^5\) to the detriment of leading figures including the then Premier Wen Jiabao and Vice-President Xi Jinping, who were both political opponents of the then head of security Zhou Yongkang. Soon after Xi took power, Zhou was arrested, and one of the accusations made against him was leaking state secrets.\(^5\)

\(^5\) O’Donnell et al., Transitions from authoritarian rule; Svolik, The politics of authoritarian rule.


In the name of the anti-corruption campaign, Xi also launched waves of purges against Zhou’s supporters and political allies, among them Ling Jihua. Ling had worked for years as the personal secretary of the former President Hu Jintao and director of the CCP’s general office, and thus controlled significant amounts of sensitive information about the party and leaders. Soon after Ling Jihua was arrested, his brother Ling Wancheng fled to the United States in 2015, where he shared this information with the Americans (although he denied having done so). According to a range of 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’. China’s strong desire to get Ling Wancheng back caused a degree of diplomatic conflict with the United States at the time. 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 and more centralized, with much less held in non-digital form, and will thus become more powerful. In this respect, the digital sources of data may be the game-changer for the power struggles 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. Corruption, for example, will reduce the regime’s legitimacy, and may 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 damage not only the incumbent leadership but the entire political system.

If non-digital materials on corruption could intentionally be used for the purposes of undermining political opponents, so could the massive amounts of digital information now held. This would grant enormous power to the security forces that control the data. The abuse of power by security forces is not new in China; they already use their power to pursue both individual and departmental interests. For example, the Deputy Minister of National Security, Ma Jian, was reported to use technical means (including recording, reconnaissance

---

61 Anderlini and Mitchell, ‘Top China defector passes secrets to US’.
and eavesdropping) to benefit certain businessmen. 63 Similarly, it is reported that some Chinese leaders are using their own security forces to spy on each other by wiretapping. 64 The former party head of Chongqing, Bo Xilai, was reported to have used the security forces to plant electronic devices to spy on the then Chinese President Hu Jintao. 65 As noted above, the security tsar Zhou Yongkang is accused of leaking state secrets. In the future, digital data will definitely be employed in these power struggles; and in times to come, the regime will pay a much higher price to purge a 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 networks. In this situation, leaking data to damage political opponents would be more destructive. It might also be a suicide mission, as opponents would be likely to retaliate by exposing the data in their own hands. Such anarchic data battles in the course of power struggles may cause significant trouble to authoritarian regimes.

There is also a further scenario to be considered. In the circumstances outlined above, digital data may be highly destructive to a regime once if used in factional struggles. However, this massive potential for destructiveness 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 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 scenario, digital data becomes the ultimate weapon, and its deterrent effects serve the purposes of self-defence; thus a relatively stable elite politics might be maintained. This scenario is somewhat similar to the principle of nuclear deterrence among nations.

Nonetheless, there is no guarantee that such stability would last for long. Accidents or misjudgements are always possible. One simple mistake may push the button to start the self-destruction of the entire regime. It is impossible to predict the sustainability of this relatively 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 either of 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 the security forces certainly merits further consideration. Nonetheless, China’s anti-corruption campaign is always related to the elite power struggle, and the role of

63 Xiankang Cui, Ning Yu and Ran Liu, ‘Guo wengui weilie gaoguanji: cong jiemeng dao fanmu’ [Guo Wengui’s story to hunt senior officials: from alliance to enemy], Caixin zhounkan [Caixin weekly], no. 12, 2015.


big data in the anti-corruption campaign will be no exception. Even if the data is not deliberately used for power struggle, data leakage may significantly undermine regime legitimacy and thus raise the possibility of the removal of leaders—just as the Panama papers led to the downfall of Iceland’s Prime Minister.\(^{66}\)

All these observations recall an old question 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 as weapons in power struggles, the negative effects may be more damaging to regime legitimacy and elite cohesion than ever before, and thereby negate all the efforts that have been made to strengthen authoritarian rule. That is to say, the Chinese government’s approach to big data may itself 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 is ancient and eternal.\(^{67}\) To a large extent, this debate has revolved around the question of whether the authoritarian regime possesses sufficient adaptive capacity to stay relevant in a 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 governance challenges facing authoritarian regimes are becoming more serious and multidimensional.

The advent of the big data era has complicated authoritarian governance, for big data is 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 particularly dangerous.

When massive amounts of digital data are highly centralized in the hands of a few people subject to few constraints, the damage will be inestimable once it comes to be used as a weapon in power struggles. While this may also be a problem for democratic systems, in that context the damage may destroy the regime, but will not destroy the political system. On the contrary, in an authoritarian regime such as China, in which the legitimacy of the regime and of the political system are combined, big data has great potential to undermine the entire system that is actively embracing it. In this regard, big data may bring fundamental change to

---

66 The Panama papers refer to 11.5 million leaked documents from Mossack Fonseca, a Panamanian offshore law firm. Those data includes detailed financial information that is directly or indirectly associated with many national leaders. It shows how offshore tax regimes can be manipulated to transfer and hide wealth.

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 analysis. 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, actual data.

A more accurate understanding of the challenges posed to authoritarian regimes by big data may provide us with a unique perspective on 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. This prospect has already generated a lively debate on the rise of China in the pages of this journal. 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.