Cybersecurity under Xi Jinping

By Susanne Chan
Email: socicourse@gmail.com

> *"Cybersecurity and informatization are mutually constitutive. Security is the precondition of development, development is the guarantee for security, security and development must progress simultaneously."*
>
> *"Cybersecurity and informatization work constitute the key priorities under the '13th Five-Year Plan' period."*
>
> *Xi Jinping. April 19, 2016. "Speech at the Work Conference for Cybersecurity and Informatization."*

Xi Jinping declared a "new era" of Chinese socialism (新时代中国特色社会主义思想) as the 19th National Congress of the Communist Party of China (CPC) unveiled on October 18, 2017. At the Congress he officially elevated himself to the status of Deng Xiaoping and Mao by making "Xi Jinping Thought on Socialism with Chinese characteristics for a New Era" a guiding principle for the party.

Whether the rise of Xi signals the end of collective leadership is subject to debate, but the last five years did see his aggressive amassment of power. Xi's much touted anti-corruption campaign charged 300,000 officials in 2015 alone. "Tigers" at the top were taken down, with many perceiving that as a move to weed out rivals. Attempts were made to recentralize control organizationally and ideologically. Journalists, lawyers, academics, and activists have faced mounting pressure as the Party tightens its ideological grip. Much of this is done under the institutionalization of the "rule of law," or to be more accurate, the "rule *by* law." For the record, China was the world's worst jailer of journalists in 2014 and remained second worst in 2016 with 38 in prison.

In his video message to participants at the 3rd state-run World Internet Conference in November 2016, Xi reasserted the need to maintain national cyber sovereignty. "Internet and information security are matters of national security and social stability," he said. While some may reduce this to merely another call for media censorship, internet governance points to additional issues raised in the quoted statements at the beginning of this article. The following discussion attempts to contextualize these statements along two directions: 1) a quick overview of media governance in China and its ongoing attempts to recentralize media control (especially over the internet) since the 1990s, and 2) how cybersecurity and informatization must be understood in broader developmental and infrastructural light.

Media Governance in China

Ideological control has always been high on the state socialist agenda, encompassing elements as broad as "public opinion, morality, theoretical thought, political ideas, philosophy, religion, art, and literature." (Su 1994:75) Article 35 of the Constitution of the People's Republic of China

endows citizens with the right to "freedom of speech, of the press, of assembly, of association, of procession, and of demonstration." Unlike its liberal democratic counterparts, however, these rights are circumscribed by the principles of democratic centralism, hence the stipulation of the dual importance of rights and duties in Article 33: "Every citizen is entitled to the rights and at the same time must perform the duties prescribed by the Constitution and the law."

Democratic rights in China exist primarily for the advancement of the state and society's collective interests, with the Party acting as the final arbiter. While the role of the media has always been propagandistic, much has changed with marketization and the rising public expectations for accountability and information. News reporting, for instance, has morphed into a two-tier system where a market-oriented appropriation of public opinion supervision (*yulun jiandu* 舆论监督) exists alongside traditional propagandistic reporting. Investigative journalism and strategic/selective censorship that break the rule of positive reporting have been used increasingly since the 1990s to enhance its appeal to readers while maintaining Party hegemony under the guise of seeming liberalization.

Taming the net is nonetheless a challenging task. In 2013, Xi issued a call to arms against the country's unruly internet. He called for the revival of "ideological purification" and advocated the construction of "a strong army" to "seize the ground of new media." For those unfamiliar with the political system in China, understanding media governance there involves a broader appreciation of its organizational matrix. The current seven members in the Politburo Standing Committee represent the top leadership in the Party, whose duty is to deliberate over and decide on major policies when the Politburo is not in session. Next are the leading small groups (*lingdao xiaozu* 领导小组) that advise the Party Politburo on policies and coordinate the implementation of subsequent decisions. Two important new leadership groups were formed in the last several years: Comprehensive and Deepening Reform in 2013 and Internet Security and Informatization in 2014. Xi chairs them both, which speaks volumes to their priority. The whole Party-state apparatus is organized around broad functional areas (e.g., party affairs, organization affairs, propaganda and education, political and legal affairs, finance and economics, military, etc.) called systems **(***xitong* 系统). Each of these involves extensive vertical and horizontal nesting of related bureaucracies that crisscross ministry or industry boundaries.

For a quick reference to the list of Party and state agencies that regulate the media in China, please refer to "China's Media Governance System: A Partial Overview".

Control over traditional media (e.g., printed books and television) falls primarily under the area of propaganda and education. The internet arrived in China in 1994 and was initially categorized under telecommunications and managed under the finance and economics *xitong* during the 1990s. As we all know by now, the internet rapidly developed and expanded in its reach (e.g., the potential formation of trans-regional and trans-organizational networks) and function (e.g., as a public platform for dissent), exposing the regulatory limitations within a decentralized and fragmented system that lacked bureaucratic coordination.

Recentralization through organizational restructuring

As an attempt to recentralize control in various functional areas (e.g., taxation, media), a series of restructurings began in the mid-1990s (the late 1990s for the internet). The challenge for internet governance was to reduce overlaps in licensing and supervision procedures while consolidating management over different media (e.g., online and offline, print and audio-visual materials), the distinguishing lines of which were becoming blurrier by the day.

Organizationally, the State Council announced plans to downsize ministries and commissions in 1998. During the same year, the then Ministry of Posts and Communications (MPT), Ministry of the Electronics Industry (MEI), and parts of the Ministry of Radio, Film and Television (MRFT) were combined to form the Ministry of Information Industry (MII). In 2008, MII further merged with the (1) Commission of Science, Technology, and Industry for National Defense, the (2) State Council Informatization Office, and the (3) State Tobacco Monopoly Bureau to form the Ministry of Industry and Information Technology (MIIT). MIIT is not primarily responsible for the regulation of content in the media industry. Its key job is to regulate and develop China's telecommunication and software industries, and control the licensing and registration of all internet information services. The regulation of media content falls mainly upon the State Administration of Press, Publications, Radio, Film and Television (SAPPRFT), which was formed in 2013 through merging the General Administration of Press and Publication (GAPP) with State Administration of Radio, Film, and Television (SARFT).

The internet became incorporated under the propaganda *xitong* by the mid-1990s. The government began to maintain a list of banned sites and block access to external internet sites that supplied news and pornography. To further streamline the process of monitoring the internet industry and bringing it under one centralized regulatory body, the State Council Information Office (SCIO) announced the transfer of its offices that regulated the internet to the State Internet Information Office (SIIO) in 2011.

Conglomeration and mixed-ownership reform

Despite four decades of market reform, access to strategic industries like the media (especially regarding news production and broadcasting), energy, and banking has remained restricted. Telecommunication is no exception. The industry was protected by the state prior to its World Trade Organization (WTO) entry. International carriers were prohibited from entering the market and only equipment vendors could invest in China based on conditions of technology transfer. These rules did change after China's entry to WTO in 2001. Nonetheless, international carriers could only form joint ventures and invest up to 50% in internet services, up to 49% in the mobile sector in 17 cities, and up to 25% in fixed-line basic services in Guangzhou, Beijing, and Shanghai. Telecom operators in China remain exclusively local with the state acquiring majority ownership in the aforesaid telecom giants.

Restricted marketization was by no means the only strategy to recentralize control in an increasingly competitive and diverse field. In anticipation of increasing competition with global giants and the need to maintain political leverage, the Party-state began a series of corporate

conglomerations in the newspaper and television markets during the 1990s. The official rationale was to eliminate non-competitive organizations and allow for a more efficient allocation of resources even though these moves were both economically and politically motivated.

A similar process took place in the telecommunication industry in May 2008. The central government (MII, National Development and Reform Commissions, and Minister of Finance) merged six telecom companies into three state-owned giants, namely China Telecom, China Unicom, and China Mobile. The parent of China Telecom Corporation – China's biggest fixed-line company – bought a mobile-phone network from the parent of China Unicom, which then merged with the company that controlled China Netcom Corporation, the nation's second-largest fixed line company. China Mobile, the dominant player in the wireless market which took up two-thirds of the nation's mobile phone market at the time, would eventually take hold of the unlisted Tietong (i.e., railway telecom). This revamping boosted the resourcefulness of the fixed-line operators (i.e., China Telecom and China Netcom) so they could compete against China Mobile as China rolled out 3G high speed wireless services. These three state-owned companies remain the biggest player's in China's telecommunications industry. As of May 2016, China Mobile is the world's largest mobile phone operator with around 860 million subscribers.

As an effort to enhance the efficiency and competitiveness of state owned enterprises (SOE), the State-owned Assets Supervision and Administration Commission (SASAC) is now pushing mixed-ownership reform (*hungai* 混改). Announced in 2013, the mixed-ownership reform policy allows – pending SASAC's approval – foreign investors and non-state companies to invest in centrally owned SOEs. Telecommunications, along with equipment manufacturing, coal, electricity, and chemicals, have been identified as the target industries.

More recently, it was announced in August 2017 that China United Network Communications, the parent of China Unicom (Hong Kong) Ltd., would bring in four internet giants (Baidu, Alibaba, Tencent, and JD – collectively called BATJ) as its new shareholders. Whether these changes will "further optimize its corporate governance in accordance with the market-oriented principles" is subject to debate, but the cross-ownership of telecommunication (i.e., the hardware) with the largest players (i.e., BATJ) in the field of big data likely advances the goal of retaining state control.

Internet governance agencies and some important regulations

The previous sections present the basic architecture of media (more specifically the internet) governance from which various laws and regulations develop, and address some basic attempts at maintaining control during the course of reform. To recapitulate, at the top are two major leading groups that monitor the internet, namely the Central Leading Group for Propaganda and Ideological Work (CLGPIW) and Central Leading Group for Internet Security and Informatization (CLGISI). These provide guiding principles and policies to agencies like the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT), the Ministry of Industry and Information Technology (MIIT), the State Internet Information Office (SIIO), and the Cyberspace Administration of China (CAC) that regulate and coordinate the industry.

- *Leading group that provides guiding principles*
  - **CLGISI** – This leading group manages internet related issues, including the expansion of online services, internet security issues, jurisdiction over internet censorship policies.
  - **CAC** operates under **CLGISI**.

- *Regulation of news and publishing content*
  - **SAPPRFT** – This executive branch regulates the content of all news, publishing, and broadcasting content.

- *Internet censorship*
  - **SCIO** – This is the chief information office of the Chinese government.
  - **MIIT** – This Ministry regulates the internet service providers in China and is responsible for running the National Computer Emergency Response Team & Coordination Center (CNCERT/CC).
  - **CNNIC** operates under **MIIT**.

The Chinese government adopts a range of technologies and legislative actions to monitor the internet. The resulting censorship system has earned the name the "Great Firewall of China" (GFW). Two million internet police reportedly take part in internet surveillance operations and employ data-mining software to track down keywords on networking sites (e.g., Renren) and search engines (e.g., Baidu). URLs are filtered and there is blanking of keywords considered as harmful or anti-social. Online hosts will be warned or have their posts or even accounts deleted if they post anything considered detrimental to societal "harmony." A sizeable 50 cent army serves as online commentators who create favorable comments or censor negative postings on popular social media sites.

Internet sovereignty*:* Formal internet regulations date back to 1997, as the Ministry of Public Security took initial steps to issue regulations that governed internet usage. According to these regulations, "Individuals are prohibited from using the internet to harm national security; disclose state secrets; or injure the interests of the state or society." The first Chinese law (CL97) that criminalized cybercrime was passed during the same year. The concept "internet sovereignty" was first introduced in a 2010 white paper entitled "The Internet in China." It means that the internet is under the jurisdiction of Chinese sovereignty within Chinese territory and everyone – individuals and organizations – is expected to abide by the internet laws and regulations.

State authorization on the dissemination of news and information*:* There are numerous restrictions on who are allowed to publish/broadcast, as well as whom and what can be published/broadcasted in China. According to Article 8 of the "Measures on the Administration of Broadcasting Audio/Visual Programmes over the Internet or Other Information Networks" (互联网等信息网络传播视听节目管理办法 2003.01.07), anyone setting up an internet broadcast business for news-related audio/visual programs must be "approved by the State Council Information Office, and possess the qualifications to distribute news over the Internet." Article

10 further states that "An enterprise setting up an information network audio/visual program broadcasting business must have a radio/television, news, publishing, cultural, or propaganda unit at the local level or higher as its sponsoring agency."

State secrets*:* One must tread a fine line to avoid jail time in China, as there are numerous regulations that prohibit the divulgence of "state secrets" or the spread of "rumors" that "disrupt social order and stability." Definitions of state secrets and disruptive rumors remain blurry, not to mention the arbitrariness with which they are applied depending on who posts, where they post, and when they post. Strategically, media agencies and journalists have to "play edge ball" (擦边球) to test what it means to go "too far." These restrictive rules have been around for a long time. For example, according to Article 4 of the "Measures for the Implementation of the Law on the Protection of State Secret" (保守国家秘密法实施办法 1990.04.25), any divulgence of information that results in "jeopardizing the ability of the national government to maintain stability and defend itself," "affects the integrity of the nation's unity, solidarity among peoples, or social stability", "harms political or economic interests of the nation with respect to the outside world," "hinders important national safety or health work" – to name but a few – "shall be brought within the scope of a state secret and a specific secrecy grade." These wordings allow for an arrest of anyone who posts an article that allegedly could incite conflicts or undermine stability. This may include reports that expose food safety risks, epidemics, or various types of social unrest (e.g., protests against enterprises or governments, political tensions involving ethnic minorities).

Subversion of the regime*:* Article 105(2) of The Criminal Law (中华人民共和国刑法 1997.03.04) states that the **"**Use of rumor mongering or defamation or other means to incite subversion of the national regime or the overthrow of the socialist system shall be punished by a sentence of five years or less of imprisonment, criminal detention, supervision, or deprivation of political rights. Criminal leaders or those whose crimes are particularly severe shall be punished by a sentence of five years or more of imprisonment."

While this law had targeted a variety of behaviors deemed to be disruptions to social order, such as fighting, looting, throwing rocks or refuse at vehicles or buildings, or stirring up trouble in public spaces, an elaboration in 2013 has extended its application to the internet. The **"**Elaboration of Criminal Law Article 293" (中国刑法 第 293 条 寻衅滋事罪 2013.09) was jointly issued by the Supreme People's Court and Supreme People's Procuratorate. It states that the "use of information networks to berate or intimidate others," "to disseminate false information . . . that one has either invented or clearly knows to be fabricated," and "to organize or incite others to disseminate [such information]," should be punished under Article 293 of the Criminal Law for "creating a serious disturbance."

All these laws and regulations play a key role in muting dissent. Liu Yunshan, Politburo Standing Committee member and the leader of CLGPIW, stated clearly at the annual National Cybersecurity Publicity Week on September 16, 2016 that all Party and state agencies must seriously implement a cybersecurity responsibility system. Internet corporations have a duty to strengthen "social responsibility and moral responsibility," and netizens have to "go online legally" in order to maintain national cybersecurity.

Given the focus of this article, I would like to bring attention to some recent regulations that further restrict the freedom of speech online. The National Security Law and the country's first Anti-Terrorism Law were promulgated shortly after the 4th Plenary Session of the 18th CPC Central Committee meeting in 2014. The scope and ambiguity associated with these laws have triggered serious concerns among human rights activists as well as foreign corporations and governments. These new regulations authorize the Party-state's agencies to inspect what might be considered proprietary technological and intellectual property. There are also concerns regarding further state encroachment on the privacy of data. Here is a list of some regulations and laws passed under Xi:

Regulations	Controversial features
Counterespionage Law 反间谍法 (2014.11)	This law aims at tightening state security and building a "comprehensive" national security system. It will allow authorities to seal or seize any property linked to activities deemed harmful to the country. Authorities can ask organizations or individuals to stop or modify any behavior regarded as damaging China's interests. Possession of espionage equipment, as defined by the state security department, is also illegal. Enforcement agencies have the right to confiscate properties should the concerned refuse to comply.
National Security Law 国家安全法 (2015.7)	This law covers a wide range of state interests that many consider to be restrictive of people's freedom. Clause 1 states that the law aims to "safeguard national security, defend the people's democratic dictatorship and the socialist system with Chinese characteristics" as well as the "realization of the great rejuvenation of the nation." National security is defined as the protection of the political regime, sovereignty, national unification, territorial integrity, people's welfare, and the "sustainable and healthy development" of the economy and society. These and other "major national interests" should be "relatively free from danger and not be under internal and external threats." The importance of CPC's leadership in national security and its role in establishing "a centralized, efficient, and authoritative national security leadership system" is heavily emphasized. The law stipulates that there should be a "prevention of the infiltration of "harmful moral standards," that there should be an establishment of systems for the "protection of cyber and information security," "prevention of social conflicts," and "protection against terrorism, religious cults, interference of religious issues by 'overseas forces' and any forces that threaten ethnic harmony. " These ideas echo the spirit behind earlier laws and regulations, but effectively grant the National Security Commission – established in 2013 and headed by Xi – legal power to oversee China's national security across a range of domains, thereby centralizing Party control in security affairs.

Anti-Terrorism Law 反恐怖主义法 (2015.12)	In its call for a “secure and controllable” cyber infrastructure, this controversial law requires telecommunications and internet providers to "provide technical support and assistance including decryption" and will be made to "prevent dissemination of information" on extremism. Dissemination of information about terrorist activities is banned. The same applies to the fabrication of stories about fake terrorist events. Only pre-approved news outlets are allowed to report on a terror attacks or official responses. This applies to both online and offline reports. (Note: This is already a water-downed version of the original draft, which proposed the installation of security backdoors and required companies to keep servers and user data within China.)
Provisions on the Administration of Online Publishing Services 网络出版服务管理规定 (in effect from 2016.03.10)	These provisions were jointly issued by MIIT and SAPPRFT to replace the “Interim Provisions on Internet Publication Administration” promulgated in 2002. An online publishing service is an extension of traditional publishing, and should therefore conform to the guidelines under the latter. These provisions officially prohibit foreign companies or foreign joint ventures from “online publishing services,” meaning the public dissemination of online publications through an information network. “Online publications” include digital works with editing, production, processing, and other publishing features, including text, images, maps, games, animation, audio-visual books and other original digital works of literature, art, science, and any other digital works as identified by SAPPRFT. Foreign companies, joint ventures, or individuals are, however, allowed to generate online content through collaboration with a local company, pending approval from SAPPRFT, and only after they officially acquire an online publishing license. In addition, any publisher of online content, including “texts, pictures, maps, games, animations, audios, and videos” will be required to store their “necessary technical equipment, related servers, and storage devices” in China. The SAPPRFT and MIIT, as usual, will have the power to examine, approve, and supervise publishing services, allowing them to inspect and detain articles and business premises in contravention of the law.

Cybersecurity Law (CSL; 网络安全法) (In effect 2017.06.01)	This law was promulgated by the National People's Congress. It "regulates the construction, operation, maintenance and use of networks, as well as network security supervision and management" in China. (Xia 2017) This law grants the CNITSEC (affiliated with MSS) enormous power to request source code and other intellectual property of technological suppliers who operate in China. According to Article 28, network operators shall provide technical support and assistance to public security organs and state security organs and to lawful activities preserving national security and investigating crimes. National security, to recall, was defined in the National security law as "the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the welfare of the people…and the ability to ensure a continued state of security." In addition, Article 35 states that critical information infrastructure operators purchasing network products and services that might impact national security shall go through a national security review organized by the state network information departments and relevant departments of the State Council. Article 37 further specifies that personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China shall be stored within mainland China. All these rules are potentially very intrusive. Given the broad and vague definition of state security, firms are worried that this law would jeopardize the vendors' rights to their proprietary technology, with the risk of having that exploited for intelligence purposes. Foreign technological companies thus face a dilemma – should they comply or risk losing access to the Chinese market? As of September 2017, the CAC already accused the top three internet giants — Tencent, Baidu, and Sina — of violating Article 47 of the Cybersecurity Law. The companies were said to have failed to properly manage their social media platforms (Tencent's WeChat, Sina's Weibo, Baidu's Tieba) because some netizens "spread information of violence and terror, false rumors, pornography, and other information that jeopardize national security, public safety, and social order."

Regulation on the Management of Internet Forums and Communities (互联网论坛社区服务管理规定) and Regulation on the Management of Internet Posts and Comment Services (互联网跟帖评论服务管理规定) (in effect 2017.10.01)	These regulations took effect on October 1, 2017, just in time before the commencement of the 19th National Congress of the CPC. Promulgated by CAC (SIIO), they are designed to "properly implement the spirit of the Cybersecurity Law." These regulations require that internet chat service providers (e.g., Tencent's WeChat, QQ, Baidu's Tieba, Alibaba's Alipay chat) strengthen their regulatory functions. They are responsible for verifying the identities of their users and keeping a blog of group chats for no less than six months. Anyone who has not registered with valid identification should be barred from participating in online forums. When "services are provided for comments on news and information, a system of first-approve-then-post must be established." These measures effectively kill spontaneity online and further exhibit the Party's will to monitor the expression of online public opinion (*wangluo yulun* 网络舆论).

Cybersecurity and Informatization

This article centers on China's need to maintain Party legitimacy in the age of the internet. The previous discussion associates legitimization concerns with national security, as is reflected in how legislation over the latter is used to secure the former. The mainstream literature on media governance also tends to focus on these as concomitant concerns. A closer look at state (or in this case, Party) governance, however, shows a more multifaceted picture.

State strategizing involves the artful coordination of multiple institutions. Legitimation provides the foundation for compliance and order, but this is only one among a variety of concerns in Xi's agenda on cybersecurity and informatization. Effective governance also rests on a state's capacity to steer (i.e., ability to guide, define, and pursue goals that are in line with the nation's interests), extract (i.e., capability to mobilize resources to implement center goals), coerce (i.e., ability to use force to achieve core objectives), and administer/control the nation's territory. (Bernstein and Lu 2003:16) Without getting sidetracked into a discussion of the role that the military and police play, Xi's call to informatize has a lot to do with steering the country onto the next phase of economic development for future extractive potential.

Informatization and national security*:* What is informatization? This involves the connection of industries online and the utilization of technology to enhance efficiency and resolve economic developmental problems in China. The organizational restructuring addressed earlier was part of a greater move towards re-centralizing control as China reshapes its domestic architecture of information and communication technologies (ICTs) and positions itself in global strategic terms. As Creemers (2016) points out, this implies obtaining "effective control over all important ICT processes within its territory," with the first priority being "indigenization." In short, security and controllability of technology are both important. (Parasol 2017:14) Reducing the country's

dependence on foreign suppliers serves the dual functions of enhancing security while advancing China up the supply value chain.

Informatization and economic development*:* National security – both domestic (the need to censor dissent) and global (the need to prevent hacking and unauthorized breaching of big data) – is and has always been an underlying concern. Added to this is the need to develop economically in a sustainable fashion in the years to come. Despite its rapid rise to the world's second largest economy over the past few decades, the growth rate of China's economy has started slowing down. According to the Asian Development Bank Institute (ADBI), the annual average rate of real Chinese GDP expansion dropped from 10.54% between 2000 and 2007 to 9.7% in 2009. The figure further declined to an average of 7.84% from 2011 to 2015 and 6.5% in 2017, despite a temporary rebound as a result of the government's stimulus initiatives after the 2008 financial tsunami. This structural adjustment points to the need to shift its manufacturing orientation toward medium and high-end goods and services. For Xi, this implies a deeper integration of the internet, big data, and artificial intelligence with the economy. Innovation is one of the key principles identified in the 13th Five Year Plan (2016). In Xi's words, China's economy is stepping into the "new normal" (*xin changtai* 新常态), hence the need to ameliorate industrial over-capacity, and restructure and shift the economy into an innovative mode.

China is well placed to deploy the Internet of Things (IoT) for industrial use. To start with, it is already the leading manufacturer of global electronics that constitute the back bone for the IoT technology market. According to an IotIntl article, 95% of the IoT connected devices produced globally would be manufactured in China by 2020. The concentration of resources and the rapid industrial adoption of IoT in China provide grounds for benefiting from the economies of scale. More importantly, China is already quite connected. As Parasol (2017:3) pointed out, China has aggressively promoted the development of Smart Cities (*zhihui chengshi* 智慧城市). According to the Chinese National Development and Reform Commission, this strategy introduces modern science and technology to urban planning, construction, and operation, and could potentially integrate and offer a whole range of services (e.g., pollution control, transportation design, virtual finance) a city needs.

The adoption of such technologies has far-reaching implications. The interconnectivity associated with IoT raises security concerns, especially when there is an intersection between big data and IoT, big data collection/analytics/distributions, cloud computing intelligence, and cyber security. Xi's direct involvement in CLGISI, the establishment of CAC and the development of a series of internet regulations discussed earlier should be understood within this broader light of centralizing control over the internet governance regime. The priority is to build a cyber-superpower (*wangluo qiangguo* 网络强国), with the twin objectives of protecting critical information infrastructure while advancing indigenous innovation. As a recent article published by CAC emphasizes, "If our Party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term."

The utilization of technology is an irreversible trend. It is, however, a double-edged sword. Deployment of IoT significantly increases the Party-state's logistic reach. This sets up a surveillance system that empowers those who have control over such information capital, yet renders those subject to the gaze of the big brother increasingly vulnerable. This brings to mind

Mann's (1984) distinction between infrastructural and despotic power. In a regime where power is highly concentrated and accountability limited, this revolutionary increase in infrastructural power will likely amplify the despotic and coercive capacity of the Party-state in China.

Afternote

Although this is an article on China, at stake are some broader issues that apply worldwide. How have technological changes revolutionized the way information spreads and how people connect? How have these re-structured the relational and hierarchical dynamics in society, allowing for new configurations of alliances across space that could be experienced and perceived as simultaneously empowering and threatening? Traditional boundaries are getting blurrier and new rules have yet to be set to delineate one's jurisdiction over information and data. When do ownership of property and protection of rights start and end? Who will have the authority to arbitrate any disputes that arise from the process? These are but some age-old concerns since the internet revolution. As we brace ourselves for what some call the fourth industrial revolution, more questions remain to be answered. In an age where inequalities are widening and when there seems to be a worrisome retreat back to authoritarianism, it is important to reflect more critically upon the mechanisms that could ensure transparency, access, and equality. With that said, the scenario in China is far from rosy.

Cited references

Bernstein, T.P. and X. Lu. 2003. *Taxation without Representation in Rural China.* NY: Cambridge University Press.

Kania, Elsa B. September 27, 2017. "The Party's 'Hurdles': the Internet, Propaganda, and Power.." *The Diplomat.*

Lindsay, J.R. 2015. "Introduction – China and Cybersecurity: Controversy and Context." Ch. 1 in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by J.R. Lindsay, T.M. Cheung and D.S. Reveron. NY: Oxford University Press.

Miller, Alice. July 28, 2014. "More Already on the Central Committee's Leading Small Groups." *China Leadership Monitor* Issue 44. Stanford University: Hoover Institution.

Parasol, M. 2017. "The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and smart city dreams." *Computer Law and Security Review: The International Journal of Technology Law and Practice*, doi: 10.1016/j.clsr.2017.05.022

Su Shaozhi. 1994. "Chinese Communist Ideology and Media Control." Pp. 75-88 in *China's Media, Media's China,* edited by Chin-Chuan Lee. Colorado: Western Press Inc.

Xi Jinping. April 19, 2016. "Speech at the Work Conference for Cybersecurity and Informatization." (在网络安全和信息化工作座谈会上的讲话) *Xinhuanet.com*

Xia, Sara. June 24, 2017. "China's New Cybersecurity Law: The 101." *China Law Blog.*