Focus Asia
Perspective & Analysis
May 2020

China's Cybersecurity Legislation:

A Paper Tiger or an Institutionalized Theft?

Maud Descamps

China's digitalization drive has become a key force for the country's economic growth and transformation, opening new opportunities for Chinese companies internationally. The booming digital economy, which has increased the reliance on information technology for business operations, has however exposed Chinese companies to new threats and vulnerabilities, mandating the need for reinforced cybersecurity legislation to protect data and sensitive information.

Introduction

The Cybersecurity Law enacted by the Chinese government in 2016 - and put into force on June 01, 2017 - partly sought to address the existing deficiencies in data protection and online vulnerabilities. Nevertheless, the stringent measures implemented as part of this digital reform introduced new challenges – especially in terms of data control and intellectual property protection - for the many foreign companies who had been incentivized to invest in China through the "Open Door Policy", but also for those collaborating with Chinese investors venturing overseas as part of the "Going Out policy".[1]

Beijing is currently in the process of implementing a new set of reforms deriving from the 2016 Cyber Security Law, the latest being; the Cybersecurity Multi-level Protection Scheme (CMLPS 2.0).[2] Although it is touted as an effort to protect the interests of Chinese citizens, this new cybersecurity legislation has raised important concerns in terms of data protection, in particular, regarding sensitive business information and trade secrets. In other words, foreign firms' intellectual property could now be at risk of being leaked to Chinese-based competitors. The basic law governing cybersecurity is experiencing an evolution which could also lead to private information being leaked and used by the Chinese government for malicious purposes.

Beijing into the Cyberspace

The government of the People's Republic of China (PRC) established full connection to the global internet in 1994 under Jiang Zemin's presidency. However, it was not until 2010 that the government released its first white paper on the topic. The document entitled; "The Internet in China", established an early guideline on the use of the internet and represented a first attempt by the government to tackle information security.

President Xi Jinping is following in the footsteps of Jiang Zemin by leading the country deeper into cyberspace, making digital development a central feature of his second mandate. In line with Xi's vision of "socialism with Chinese characteristics for a new era", the digitalization of the economy and the development of ICT (Information and Communication Technologies) industries are set to be integral parts of the restructuring of China's economic model and the Belt and Road Initiative (BRI).

The aforementioned objectives resulted in the development of China's data regime. The Chinese government has long kept reins on the domestic cyberspace, applying strict online censorship rules in order to oversee and influence its content through the deployment of the Golden Shield Project (better known as the "Great Firewall"), which prevents non-approved services such as Google and Facebook from operating.[3] However, to enable China's ascension as a competitive actor in the digital era, additional legal instruments were to be set. In order to do so, cyberspace regulations needed to be redesigned to better safeguard information technology so as to mitigate risks of data being bought, stolen or traded. Nevertheless, the Chinese government took an approach unlike anything that had been done before.

"China's Way"

President Xi envisions cyberspace legislation as a way to protect national security and ensure economic and social stability. Those objectives set the need to make cyberspace more easily manageable and, in particular, build up China's digital resilience to support the country's transition from an industrial age to an information era.[4] This means that China has the goal to produce higher-end products as established by the 2015 strategic plan: "Made in China 2025".[5] As the legitimacy of the Communist Party of China (CPC) mainly rests upon its ability to deliver economic growth, the development of the digital economy entails interlinked political and economic objectives at the domestic level. At the international level, China seeks to catch up with Western nations and ultimately present itself as the digital leader in the global economy. The growing international footprint of high-tech companies such as Chinese telecommunication giant Huawei, which has made major advances in 5G technology is a good example in that regard.

Despite the high potential it carries in terms of generating new opportunities, this new environment represents both a space for innovation in which the country can excel (e.g. 5G network technology) but also raises concerns regarding data protection in such a large nation. In this case, opportunities and risks are two sides of the same coin. It is a chance for firms to establish a major economic presence online through

*The **Institute for Security and Development Policy** is an independent, non-partisan research and policy organization based in Stockholm dedicated to expanding understanding of international affairs. With its extensive contact network with partner institutes in Asia, each year ISDP invites a number of visiting researchers as well as guest authors from the region to participate in research, discussion, and exchange with European scholars and policy officials. ISDP's Focus Asia series serves as a forum for these researchers as well as guest authors to provide and clarify their viewpoints on the contemporary issues and challenges concerning their countries, adding a much-needed Asian perspective to the policy and research debate.*

For enquiries, please contact: info@isdp.eu

the development of the digital economy in such sectors as e-commerce, insurance, banking, IT, tourism, etc. Nevertheless, the protection of the flow of information being transferred and used is a key challenge. The danger of private data leaks is most typically linked to inadequate resources and capabilities to counter cyber-attacks.

> ***The cybersecurity law is, therefore, a tool to create more control and represents another step on top of the content limitation measures set out by the Great Firewall.***

China's move to implement a cybersecurity law, was loaded with a desire to enforce scrutiny over digital data and content as part as an effort to protect national security and private data.[6] While the 2016 cybersecurity law imposed regulations on the public and private sectors in order to secure data and sensitive information, the new cybersecurity regulation will provide Chinese authorities open access to all types of data beyond the current scope. The broad legislation is set to issue regulations and strict directives on how firms should ensure data security and privacy in China and but also with Chinese stakeholders overseas. The regulation not only requires Critical Information Infrastructure (CII) operators to allow the government full access to their data, but also make the storage of said data within Mainland China mandatory. CII operators are enterprises running in key sectors such as finance, transportation, energy, and water conservation.

While digital regulations typically serve the primary purpose of improving personal data protection, for China the priority lies elsewhere. The key differentiating element is the strong focus placed by the Chinese government on modernizing national security and safeguarding social stability. The threat of data and private information being leaked presents the Chinese party-state with the opportunity to use technology as a tool to control information flows that have the potential to undermine its authority over the country's politics and economy, which is even more relevant in the context of the pro-democracy movements in Hong Kong. In that sense, China's cybersecurity regime is unique in its agenda: bolstering Communist party resilience in the face of potential disruption.

The cybersecurity law is, therefore, a tool to create more control and represents another step on top of the content limitation measures set out by the Great Firewall. Beijing's vision towards cyberspace was to prevent the use of anonymous services on the internet. This is one of the reasons that explains why the mobile application "Whatsapp" is banned, as the messages are encrypted. However, the ban of such encrypted applications or services has facilitated data breaches, multiplying the risks of data being stolen and shared on publicly accessible hacking chat groups or forums. Unlike in many Western countries, Chinese cybersecurity protection had a slow start to ensure cyber-crime prevention. The criminal law with the support of the cybersecurity law provides additional tools for data protection and law enforcement on the internet, which was poorly enforced before. An overhaul of cybersecurity regulations was therefore needed to ensure that illegal acts occurring in cyberspace are to be properly dealt with.

Against this backdrop, the cybersecurity law and its 2019 amendment aim at increasing the protection of sensitive data produced and transmitted on China's territory against cyber-theft. The PRC has released an updated version of its cybersecurity legislation with the CMLPS 2.0, which was enacted on December 01, 2019. The upgraded legislation strengthens the state's capacities to enforce its control in areas beyond traditional national security concerns, such as energy issues. Businesses partaking in what are considered "critical sectors" by the Chinese government are now monitored under this new legislation. Naturally, the Chinese party-state's strong involvement in shaping economic policies, coupled with its eagerness to support China's rise as a global e-tech leader raises important questions in terms of intellectual property protection

for foreign enterprises. Existing collaborations and new partnerships could see the rules being reset, therefore, bringing many uncertainties.

The situation has evolved from limited cyber monitoring of the state to a barrierless data gathering and surveillance program. The CMLPS 2.0 requires all firms and individuals to comply for the purpose of security. It impacts the use of ICT systems, which consist of hardware (e.g. computer), software, data and also the individuals who use them. In other words, all forms of network activity are impacted from the internet, mobile phones and social networks to cloud systems and email services, that are either domestically or internationally operated.

> ***Any cyber framework that conceals data or information from the Ministry of Public Security will be deemed illegal.***

While the focus of the cybersecurity law enacted in 2017 was more centered upon establishing a broad security apparatus, the CMLPS 2.0 is set out to ensure absolute state surveillance by allowing the Chinese authorities a borderless control over all data and information at their disposal. This new requirement will fully expose foreign companies and individuals in China to the monitoring of the Chinese State. The way entities and individuals (both foreign and Chinese) have attempted to bypass the Great Firewall will need to be rethought. All platforms, apps, and other technologies that cannot be accessed by the Ministry of Public Security will be outlawed and no longer tolerated, including VPNs (Virtual Private Networks), encryption, and private servers.

In short, any cyber framework that conceals data or information from the Ministry of Public Security will be deemed illegal. It is understandable that the government wishes to know which digital infrastructure in its own national systems can be trusted, nevertheless, the strategy chosen by the CPC means that these rules will apply to every company doing business in China. This differentiation in approach is a fundamental change in the corporate information technology landscape in China but also for firms engaged with Chinese partners anywhere in the world.

IP at Risk?

The new legislation is evolving towards the reduction of users' privacy in favor of increased state control over information in cyberspace. The digital network that is being developed along with the BRI - the "Digital Silk Road"[7] - could have major consequences for foreign firms in the private sector. "China's Open Door policy," set in 1978 under Deng Xiaoping's mandate, allowed foreign enterprises to enter the Chinese market but under the requirements of forming joint ventures with Chinese firms (fully or partially state-owned) and making mandatory technology transfers to them. Under these circumstances, the security of Intellectual Property (IP) is already difficult to manage. However, with China's investors going abroad, in line with the "Going Out Policy", foreign and Chinese businesses are becoming more connected. The cybersecurity regulation aimed at providing a framework for those relations.

The problematic aspect of the regulation is not limited to operations of Chinese firms within the PRC. In line with Article 5 of the 2017 Cybersecurity Law, entities operating in "critical sectors", as both suppliers or collaborators, are required to store all data on Chinese territory and to allow the authorities full scrutiny over them. The development of the BRI and its digital counterpart, which both involve a multiplicity of stakeholders operating across borders, will likely make the digital market much more intertwined with China, further exposing foreign companies to the monitoring of the Chinese party-state.

Although the protection of data and IP is a key issue that the PRC is legitimately concerned about - as per its commitment to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Beijing remains weak in the enforcement of IP rights rules.[8] The lack of clarity in the provision of data

regime regulations, including the vague concepts of national security and public interest embedded in the law, opens the door for the government to access and store data following its own interpretation with little room for dispute. There is also an increasing risk of this information being lost, passed on to local competitors or kept and used by the government itself.

As the Chinese cyberspace is steadily moving toward further CPC control, where trade secrets and intellectual property do not exist/are not permitted to exist, foreign companies operating in China have to assume that any "secret" they seek to maintain on a server or network in China will automatically become available to the Chinese government and also to all of their government-controlled competitors in China, including the Chinese military. Phone calls, emails, WeChat messages and any other form of electronic communication will no longer (if they ever really were) be kept private in the eyes of Chinese authorities.

Conflicting Interests

It has become clear that China has chosen to shift from the scrutiny of targeted information to full data accessibility. However, a key unanswered question is how rigorously the strategy will be enforced and which level of authority will partake in the enforcement of regulations. As with China, many governments have issued bills to implement backdoor strategies (e.g. Australia, the U.S., the UK) as a way to test the vulnerabilities of firms to hacking. This is a good practice as long as the targeted firms are informed of such activities and notified of which data are copied by the government. If no communication is made to them, then it is simply hacking under a legal name.

Investigation can be initiated by Chinese authorities but also by a trade association, meaning domestic competitors can request spot checks on foreign firms, raising the question of biases and abuses.[9] The capacity of accessing information from firms for security purposes and other reasons exists in other countries - such as in the U.S. for counterterrorism. However, in the U.S. targeted firms can go to court to defend their rights without the risk of seeing politics interfering with the judiciary, which is not perceived as guaranteed in China.

Despite the large scope of the legal framework, the Chinese government is increasingly inclined to leverage new media and advanced technologies to its advantage. It also relies heavily on private companies to carry out government directives on a daily basis and that also holds true for the implementation of MLPS 2.0 and China's Cybersecurity Law.

> ***Xi Jinping's efforts are now shifting towards new digital space tools such as cryptocurrencies.***

Tensions related to IP protection[10] (e.g. EU framework for the screening of foreign direct investment) and trade surplus (e.g. U.S.-China trade war[11]) could lead China to rethink its approach as a show of goodwill. However, this is unlikely given the steps that China has already taken. The result is that trade operations in China could be more difficult than they already are.

Despite China's progresses in improving the protection of trade secrets and decreasing the level of IP theft, from the perspective of outside states Beijing remains a risky partner when it comes to IP safety. Forced technology transfers are a systemic issue that discourage foreign operators to engage, as they fear losing their competitive edge. In June 2018, the EU filed a case against China on technology transfer at the WTO.[12]

Xi Jinping's efforts are now shifting towards new digital space tools such as cryptocurrencies. Blockchain technologies in China are now seen as a way to relaunch China's economic growth. In light of the global Covid-19 pandemic, digital platforms have represented key opportunities that have soared worldwide.

However, Beijing's obsession with state security is reflected in the modernization of the Chinese legal environment and enforcement tools. Instead of opening the market for Bitcoin or Libra (Facebook's cryptocurrency), Beijing is working to develop a national cryptocurrency which would not need to compete with digital foreign currencies.[13] The rules for what exactly foreign firms are required to do with regard to incorporating encryption into their products, as well as using encryption in their own communications is now undergoing changes that will be set within the protection of the CPC's leadership.

> ***The party-state leadership is also using digital tools to strengthen authoritarianism, especially in regard to information flows that could jeopardize its authority.***

Cyberspace regulations are designed to allow the Party the ability to examine and authenticate digital encryption and information. The Cybersecurity Law, the Cryptography Law and the CMLPS 2.0 are relatively vague and provide the party-state with an arbitrary power to approve, safeguard, or oppose the digital frameworks of companies. Ultimately, Beijing seeks a control that goes beyond the simple regulation and safety of users. This state of uncertainty increases at a time when foreign firms already face the impacts of the U.S.-China trade war.

Besides the risks for foreign IP, concerns are also being raised - in the European Parliament for instance - about the growing use of digital authoritarian tools by the Chinese party-state that facilitate pervasive cyber control over Chinese citizens and repression on political dissidents and ethnic minorities. In terms of values and technologies, the EU is intimidated by China's growing share as an e-power. The number of Chinese companies active in the EU remains negligible compared to the number of European firms operating in the PRC.

For foreign firms, best practice would be to segment their operations and separate data needed for businesses in China or operating with Chinese actors and data used on their global network. This will help prevent Chinese IP addresses from accessing computers. This example highlights the difficulties that awaits firms, as the digital transformation of China and its legal reforms are set to create a more restrictive environment for the digital economy.

Conclusion

China has worked to establish a more resilient system for the protection of personal information and the securitization of sensitive business sectors in the digital sphere. Nevertheless, under the guise of protecting national security and intellectual property, the party-state leadership is also using digital tools to strengthen authoritarianism, especially in regard to information flows that could jeopardize its authority.

China's Great Firewall controls external information flows into China, but the cybersecurity law is designed to protect the data outflow through an original approach. Until recently, the cybersecurity law tackled private data and state security in the face of criminality, however, China has now introduced an additional distinction between "personal information" and "important data". Yet, ultimately both types of data produced by CII operators are to be copied and stored onto a data center based in Mainland China as set by the 2016 law.

The government authorities have acquired a legal basis to exert further monitoring and enforce control, but this also raises concerns over the protection of intellectual property in a now uncertain global order. MLPS 2.0 will cover any industry with ICT infrastructure, as it encompasses the vague category of "network operators", which can include any entity that uses an ICT system.

The unlimited availability of information for the authorities is a strategy diverging from the approach taken by other governments, such as the EU which

is much more focused on the protection of data in terms of misuses. The Chinese answer to cyberspace management is a new road that could inspire other nations to take up similar policies and force businesses to rethink how they operate in those countries. However, this might not be what is needed to efficiently tackle property rights theft in cyberspace and could lead to more challenges to engage in the Chinese digital economy. ■

Author Bio

Ms. Maud Descamps has worked as a trainee in the foreign policy team of the Political Section of the EU Delegation to China and an intern at ISDP's China Center. Ms. Descamps has a bachelor in political Science from Saint-Louis University – Brussels (Belgium). She holds a MA from Katholieke Universiteit Leuven (Belgium) in European Studies and a MSc in China in Comparative Perspective from the London School of Economics and Political Science (UK).

Endnotes

1. Hongying, Wang, "A Deeper Look at China's 'Going Out' Policy"," CIGI, March 2016. Accessed November 30, 2019, https://www.cigionline.org/sites/default/files/hongying_wang_mar2016_web.pdf
2. "China seeks Public Comments for Draft Regulations on Cybersecurity Multi-level Protection Scheme to Implement the Cybersecurity Law," Covington, July 05, 2018. Accessed November 15, 2019, https://www.cov.com/-/media/files/corporate/publications/2018/07/china-seeks-public-comments-for-draft-regulations-on-cybersecurity-multilevel-protection-scheme-to-implement-the-cybersecurity-law.pdf
3. Rajeck, Jeff, "The Great Firewall of China 2017 Update: The Good and the Bad," E-consultancy, April 02, 2017. Accessed on November 16, 2019, https://econsultancy.com/the-great-firewall-of-china-2017-update-the-good-and-the-bad/
4. Cao, Siqi, and Leng, Shumei, "Cybersecurity week kicks off in China, "Global Times, September 16, 2019. Accessed November 16, 2019, http://www.globaltimes.cn/content/1164607.shtml
5. "Made in China 2025," ISDP, June 2018. Available at: https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf
6. "Overview of China's Cybersecurity Law," KPMG China, February, 2017. Accessed November 16, 2019, https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf
7. "Beijing's Silk Road Goes Digital,"Council on Foreign Relations, June 06,2017. Accessed November 16, 2019, https://www.neweurope.eu/article/european-parliament-agrees-to-keep-eye-on-chinas-takeovers-and-investments/
8. New, William, "After 15 Years in WTO, China Still Weak on Many IP Rights Rules, US Says," Intellectual Property Watch, January,10, 2017. Accessed November 16, 2019, https://www.ip-watch.org/2017/01/10/15-years-wto-china-still-weak-many-ip-rights-rules-us-says/
9. Wagner, Daniel, "China's cybersecurity law is biased and open to abuse, but it may not stop others copying it, "South China Morning Post, June 25, 2018. Accessed November 16, 2019, https://www.scmp.com/comment/insight-opinion/china/article/2152347/chinas-cybersecurity-law-biased-and-open-abuse-it-may
10. Berkofsky, Axel, "China and the EU: 'Strategic Partners' No More," ISDP, Issue Brief, December 04, 2019. Accessed December 05, 2019, http://isdp.eu/content/uploads/2019/12/China-and-the-EU-04.12.19.pdf
11. "Screening of Foreign Direct Investment," European Commission, last update June 24, 2019. Accessed November 17, 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=2006
12. "Commission Staff Working Document: Report on the protection and enforcement of intellectual property rights in third countries," European Commission, SWD (2019) 452 final/2. Accessed on January 12, 2020, https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158561.pdf
13. Clark, Grant, and Ying, Lulu, "How China is stifling Bitcoin and Cryptocurrencies: Quick Take," Bloomberg, January 09, 2018. Accessed December 01, https://www.bloomberg.com/news/articles/2018-01-09/how-china-s-stifling-bitcoin-and-cryptocurrencies-quicktake-q-a