08 November 2016

The Cyber Security Law is coming! Five things enterprises should know

This article was written by Jiang Ke (partner) and Yang Nan (associate).

On 7 November 2016, the PRC's Cyber Security Law (Cyber Security Law) was approved by the Standing Committee of the National People's Congress. The long-awaited Cyber Security Law will come into force on 1 June 2017, after three drafts spanning one and a half years.

The Cyber Security Law is applicable to both Chinese and foreign entities, i.e. it includes any entity that provides services via a network within the PRC territory, regardless of whether it is funded by domestic or foreign investors. However, certain provisions may cause more pronounced effects on foreign-funded enterprises operating in the PRC than on domestic enterprises.

In this article we discuss the five key things you need to know about the main provisions of the Cyber Security Law.

1. A wide range of "network service providers" will be regulated

The Cyber Security Law drew widespread attention from business, particularly internet-related businesses and foreign investors, due to the significant impact it would have on network security.

There are two key points in the Cyber Security Law regarding "network service providers" that businesses need to be aware of:

- Article 2 states that the Cyber Security Law will apply to the "construction, operation, maintenance and usage of networks within the territory of the People's Republic of China"; and
- Article 76(1) defines "networks" as "systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing."

Network infrastructure

"Networks" must exist in a physical form. Therefore, "relevant uses" (including 'business and usual' operations) applies to a network's physical infrastructure within the PRC. While this definition does not seem to capture entities outside the PRC who use overseas network infrastructure in the provision of online services - even when such services can be accessed from within the PRC - the Cyber Security Law does not completely ignore these entities' acts within the PRC. Article 50 stipulates that where the release or transmission of information is prohibited by laws and regulations, the State cyber administration (or other relevant departments discovering the information) shall notify the relevant entity. This entity may then adopt technical and other necessary measures to block the transmission of information.

Network operators

The Cyber Security Law establishes "network operators" as a core concept:

- "Network operators" are defined as "the owners and administrators of networks, as well as network service providers".
- "Network service providers" [1] are entities "providing services via networks" [2].

These are broad definitions[3] which encompass all entities who use a network as a medium to provide services ie the entire online service industry. Entities conducting online operations (such as app stores, e-commerce platforms and online ride-sharing platforms), and traditional bricks and mortar enterprises wishing to extend their business online, will all be affected.

2. Security requirements for network operators

Almost a quarter of the Cyber Security Law is dedicated to a series of requirements and obligations to protect "network operation security" for network operators, including network service providers. The two key requirements to note are:

- Article 20 which stipulates that the State must implement a "graded network security protection system" and requires network operators to comply with this system in exercising security requirements in network operations; and
- Article 31 which provides that the core protection on the "key information infrastructure" shall be based on such a graded network security protection system.

This is the first time Chinese law has defined a "graded network security protection system". However, the Cyber Security Law does not clarify the description of this "system", how it will be implemented or how a "network security grade" will be determined.

China's previously established cyber security systems

Prior to the release of the Cyber Security Law, China established two graded protection systems relating to cyber security:

1. the "graded computer information protection system" [4], relating to the computer

information system that contains the network, on which a five-graded protection system is exercised; and
2. the “graded security protection system for communications network elements” [5], relating to the public communications network and internet (collectively, the “communications network”), managed and operated by Chinese telecom business operators and internet domain name service providers.

In terms of the network and its security, these two systems overlap with the “graded network security protection system” established by the Cyber Security Law. But due to the ambiguity in the Cyber Security Law, the relationship between the “graded network security protection system” and these two systems remains unclear. It remains to be seen whether it is to be a substitution for these two systems, a combination or modification of them, or something else entirely.

The two existing systems use different grades with different requirements for operators of computer information systems and communications networks based. For example:

- only computer information systems above Grade II (and up to Grade V) must be filed with the public security department[6]; and
- only computer information systems above Grade III or communications networks above Grade II are subject to regular security self-examination, evaluation or inspection[7].

If the “graded network security protection system” follows the same regulatory approach, the two existing systems will be significant for the evaluation of network operation security obligations under the Cyber Security Law.

What are “operational” and “non-operational” enterprises?

An e-commerce platform is an example of an operational service, whereas a website established by an enterprise to provide its own information to the public, without any chargeable information is a non-operational service.

Fundamental differences exist between “operational” and “non-operational” services - the types of data being transferred, whether or not personal information is collected, the likelihood of website security issues, the level of risk of cyber-attack or data leakage, and the necessary security protection measures will differ between the two services[8].

It would be unreasonable to require a non-operational service to have the same network operation security as an operational service. For example, Article 21 of the Cyber Security Law requires the network operator to “adopt technical measures for monitoring and recording the status of network operations, and preserve network logs according to regulations for no less than six months”, and to “adopt measures such as data classification and back-up and encryption of important data”. While these measures are reasonable and necessary for an e-commerce platform, they are potentially unnecessary and impossible for an enterprise website. This may be why the condition of “according to the requirements of the graded network security protection system” was added to the requirements.

Providing personal identifiable information

Article 24 of the Cyber Security Law requires that network operators who “provide network access or domain name registration services, handle stationary or mobile phone network access, or provide information publication services or instant messaging services” to users, shall require users to provide real identity information when signing agreements or confirming the provision of services. If a user declines, services cannot be provided.

Cooperation with law enforcement

Article 28 requires telecom business operators, network service providers and network operators to provide technical support and assistance for public security body and state security body to safeguard national security and investigate crimes in accordance with law”. This broadly reaffirms a cooperative obligation stipulated in previous legislation[9].

3. “Key information infrastructure” defined

One of the biggest issues in the development of the Cyber Security Law was the proposed concept of “key information infrastructure”. The three main reasons that this concept was concerning are:

1. the current definition has a huge scope which would effect a large number of enterprises;
2. it sets a high threshold for the cyber security protection obligations of operators; and
3. it imposes special restrictions on the transfer of personal information and business data out of the PRC territory (see Part IV of this article).

The definition and scope of "key information infrastructure" was amended twice during the drafting process of the Cyber Security Law. The first draft limited its scope depending on industry, use, number of users and other factors[10]; the second draft removed its industry and use attributes emphasizing instead its special importance in the context of security[11]; and the third draft (and final text) combined industry attributes and security implications[12].

What industries fall under “key information infrastructure operators”?

Prior to the introduction of supporting measures, the Cyber Security Law had left enterprises in suspense about whether they will fall into the category of “key information infrastructure operators.” According to Article 31, we now know that “key information infrastructure” covers important industries and fields such as "public communications and information services, energy, transportation, water conservancy, finance, public services and e-government".

The State Council’s upcoming regulation on the “specific scope” and “security protection measures” will later clarify whether all the information infrastructure within the listed "important industries and fields" will automatically be "key", and if there are other unspecified "important industries and fields" in addition to those listed.

Corresponding legislation

Some obligations set by the Cyber Security Law for key information infrastructure operators may be found in other legislation. For example:

- Article 31 of the Cyber Security Law clearly establishes that security protection for key information infrastructure shall be based on the graded network security protection system;
- Article 38 requires key information infrastructure operators to conduct security risk assessment on their own or by entrusting professional agencies at least once a year.

4. Personal information protection: Restrictions on the storage and transfer of personal information

The Cyber Security Law also focuses on the protection of “network information security”, in particular the security of “personal information” collected and used by network operators [13].

The Cyber Security Law defines personal information as “various information, such as a natural person's name, birth date, identification card number, personal bio-metric data, profession, address, or telephone number, recorded electronically or by other means, from which a natural person's identity may be determined either by itself or combined with other information”[14].

In line with pre-promulgated laws relating to personal information protection[15], the Cyber Security Law emphasises the “identifiability” of personal information and aligns with pre-existing legislation in obliging the network operator to protect a user’s personal information. For example, it requires network operators to “abide by the principles of legality, legitimacy and necessity”, “explicitly state the purposes, means, and scope for collecting or using information”, “obtain the consent of the person whose information is collected”, “disclose the rules of information collection and use”, “not to disclose, distort or damage the personal information collected”, “not to provide personal information to others without the consent of the person whose information is collected”, “take technical measures and other necessary measures to ensure the security of collected personal information, and prevent information disclosure, distortion and damage” and so on [16].

Data storage

For the first time, there is a clear specification that certain personal information must be stored within the PRC territory. The word "certain" here does not refer to the content or type of personal information, but to the collectors and the channels of collection, that is “personal information collected and generated by the key information infrastructure operators in their operations within the PRC territory”[17]. In other words, not all personal information collected by network operators has to be stored within the PRC territory, only the personal information collected and generated by “key information infrastructure operators” during “their operations”. This requirement also applies to "critical data" meeting the above conditions, although the

Cyber Security Law does not define "critical".

Data transfer

Once an operator falls within the definition of a “key information infrastructure operator”, the Cyber Security Law will directly affect what it can and can’t do with its users’ personal information – ie whether it can transfer personal information and critical business data abroad. In today’s global economy, domestic and foreign markets are often integrated. The reality is that personal information and business data frequently flow across borders, particularly in businesses that provide "information services" via the internet. Therefore, substantial limitations and impediments may significantly affect the business operations of certain enterprises.

The Cyber Security Law does provide leeway for such restrictions though. If a key information infrastructure operator needs to transfer personal information or critical data out of the PRC territory for business purposes, the Cyber Security Law allows it to do so after "conducting a security assessment in accordance with the measure jointly formulated by the State cyber administration and other relevant departments of the State Council"[18]. However the threshold of this security assessment is not yet known and it appears that the language used (such as “for business purposes” and “needs to transfer out of the PRC territory") gives relevant authorities huge discretion.

5. Special requirements for “key network equipment and specialised cyber security products”

In addition to the regulation of network operators, the Cyber Security Law enacts special requirements for “key network equipment and specialised cyber security products”. Such equipment and products “shall only be sold or provided after being certified as secure by, or meeting the requirements of security inspection conducted by, qualified entities, in accordance with the compulsory requirements of relevant national standards”[19]. This means that any enterprise “selling” or “providing” such equipment or products must comply with the relevant provisions, even if it is not a network operator.

The State cyber administration and relevant departments of the State Council will determine the list of such equipment and products. Relevant enterprises should pay close attention to the publication of this list.

Cyber security: What’s next?

China’s Cyber Security Law is a significant piece of legislation for market participants. But while it provides rules and requirements, the Cyber Security Law still leaves a series of gaps to be filled, due to the complex and sensitive nature of the issue. These gaps will largely determine the implementation of the Cyber Security Law.

Domestic and foreign enterprises which appears to not be covered by the Cyber Security Law should thoroughly understand the provisions regardless, and pay close attention to how it is

implemented. Failure to do so may result in non-compliance caused by a lack of knowledge or misunderstanding of the relevant regulatory requirements.

Editor's note: this article was simultaneously published on Chinalawinsight.com

---

[1] See Article 76(3) of the Cyber Security Law.

[2] See Article 10 of the Cyber Security Law.

[3] We note that in the first draft version of the Cyber Security Law, "network operators" are used to be clarified as "including basic telecommunications operators, network information service providers, major information system operators and so on" (Article 65(3) of the first draft version). However, in the subsequent second and third draft versions and the official text, this paragraph does not appear any more. It seems that the legislator blurred this definition intentionally.

[4] See Article 9 of the Regulations of the People's Republic of China for Safety Protection of Computer Information Systems (revised version of 2011). Also see the Administrative Measures for the Graded Protection of Information Security, which was made according to the foregoing Article 9 and was jointly released by the Ministry of Public Security, the State Secrecy Bureau, the State Cryptography Administration and the Information Office of the State Council on June 22, 2007.

[5] See the Measures for the Administration of Communications Network Security, which was implemented from March 1, 2010 and was released by the Ministry of Industry and Information Technology.

[6] See Article 15 of the Administrative Measures for the Graded Protection of Information Security.

[7] See Articles 14 and 18 of the Administrative Measures for the Graded Protection of Information Security; Articles 11 and 12 of the Measures for the Administration of Communications Network Security.

[8] See Articles 3 and 4 of the Administrative Measures for Internet Information Services (revised version of 2011).

[9] See for instance: Articles 77 and 79 of the National Security Law (2015); Article 18 of the Anti-terrorism Law; Section X of the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection.

[10] See Article 25 of the first draft of the Cyber Security Law: "The State implements key protections for basic information networks providing services such as public correspondence and radio and television broadcast; important information systems for important industries such as energy, transportation, water conservation, and finance, and public service areas such as electricity, water and gas utilities, medical and sanitation service and social security; military networks and government affairs networks for state organs at the sub-districted city level and above; and networks and systems owned or managed by network service providers with massive numbers of users (hereinafter 'critical information infrastructure')".

[11] See Article 29 of the second draft of the Cyber Security Law: "The State implements key protections for critical information infrastructure, of which the destruction, loss of function or data leakage, may seriously endanger the national security, the people's livelihood, and the public interest, on the basis of the cyber

security protection classification system."

[12] See Article 31 of the third draft and the final text of the Cyber Security Law: "The State implements key protections for critical information infrastructure in the important industries and areas such as public communications and information services, energy, transportation, water conservation, finance public service and E-government, and other information infrastructure of which the destruction, loss of function or data leakage, may seriously endanger the national security, the people's livelihood, and the public interest, on the basis of the cyber security protection classification system."

[13] See Article 40-50, Chapter IV of the Cyber Security Law.

[14] See Article 76 (5) of the Cyber Security Law.

[15] See, e.g., the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection , the Consumer Protection Law (2013), the Provisions on Protecting the Personal Information of Telecommunications and Internet Users, etc.

[16] See Articles 41 and 42 of the Cyber Security Law.

[17] See Article 37 of the Cyber Security Law.

[18] See Article 37 of the Cyber Security Law.

[19] See Article 23 of the Cyber Security Law.

Categories: China Bulletin | Cybersecurity | Corporate, Private Equity, M&A and Commercial | Dispute Resolution & Litigation | Technology

Key contact

Jiang Ke
Partner
Beijing
T +86 10 5878 5588