Linklaters

July 2016

China seeks to tighten cyber restrictions as its online economic evolution continues

Contents

On 6 July 2016, the Standing Committee of the National People's Congress (the "**NPCSC**") published the second draft of the Cyber Security Law (the "**Second Draft**") for public comment over a one-month consultation period. The Cyber Security Law is set to become the first legislation enacted by the NPCSC that specifically deals with cyber networks in China, and in particular the supervision of network security. This increased attention by China's regulators to the country's online ecosystem may not be surprising given reports such as that by analysts eMarketer, which predicts that the internet penetration rate among the Chinese population aged between 12 and 44 will grow to 90% by 2018.

The first draft of the Cyber Security Law was introduced exactly one year before in 2015 (the "**First Draft**"), six days after China's National Security Law came into force. The First Draft attracted broad comment from the market, although the majority of its provisions exist to varying degrees in current rules and regulations (such as real-name registration) or practices (such as the government's blocking of domestic network access when social disturbance endangers public security). By consolidating the scattered requirements and introducing new and more detailed ones, the Second Draft, if enacted, will begin an era of tighter regulation of cyber security in China.

The Cyber Security Law applies a hierarchical system to network security protection, a framework under which governmental authorities, educational institutions, industry associations and network operators will assume different responsibilities and obligations. In this alert, we will focus on the provisions of the Cyber Security Law that may most concern industry players, and those new changes that the Second Draft seeks to introduce compared to the First Draft.

Network security

Network operators

Under the Cyber Security Law, a "network" comprises systems of computers or other information terminals and related equipment which collect, store, transmit, exchange and process information in accordance with certain rules and procedures. Network operators is defined to include owners and

administrators of these networks and network service providers. This potentially broad range of enterprises and institutions will each assume the following obligations:

- Conducting real-name registration of users before providing services to them (including instant message services).
- Adopting measures for data categorisation, back-up and encryption.
- Storing logs of network activity for at least six months (an obligation introduced by the Second Draft although similar rules exist in lower level regulations).
- Formulating internal rules for security administration, and implementing technical measures to defend the network against cyber attacks.
- Drawing up contingency plans to deal with cyber security incidents and reporting threats to cyber security to the relevant regulator.
- Providing assistance to law enforcement and national security authorities.

Network operators are also required to assume additional responsibilities if they operate "critical information infrastructure" which involves national security, national welfare or public interests (see below).

Critical information infrastructure

The Cyber Security Law could be the first national legislation in China to dedicate a specific section to regulation of critical information infrastructure, setting out detailed requirements for its procurement, information storage, risk assessment and security protection measures. However, although the concept of "critical information infrastructure" itself is not entirely new since it has been used in previous regulations and policies (such as China's recent Thirteenth Five-Year Plan), like those regulations and policies, the Second Draft gives no clear definition of critical information infrastructure. Interestingly, the Second Draft omits the following scope of critical information infrastructure that was provided in the First Draft:

- Basic information networks such as those providing public communication and broadcasting/television transmission services.
- Critical information systems for key industries such as energy, transportation, water conservation and finance.
- Critical information systems for key public services, such as public utilities (electricity, water and gas), healthcare and social security.
- Military networks and networks for government agencies above municipal level.
- Networks and systems owned or administered by network operators with a significant number of users (although it was not clear in the First Draft what "a significant number" means in this regard; for example whether social media operators like WeChat and Weibo, which have hundreds of millions of users, would fall within its scope).

Instead, the Second Draft empowers the State Council to separately enact implementing rules as to the scope of critical information infrastructure. This move suggests that the authorities wanted more time to set the appropriate reach for the definition given its implications which we discuss below. Nevertheless, the parameters provided by the First Draft can be used as a reference in understanding the regulator's legislative intention.

In addition to the general responsibilities mentioned above that apply to all network operators, a network operator of critical information infrastructure must also fulfil the following key operational responsibilities and obligations:

- Ensuring that network products and services purchased by it have passed a national security review conducted by the Cyberspace Administration of China (the "CAC") and other government departments if those products and services may affect national security.
- Storing in China personal information collected from citizens and important business data collected or generated by the network operator during its operation within China. Any data that a network operator needs to transfer or store overseas must undergo a prior security assessment in accordance with procedures prescribed by the CAC and other departments. (The Second Draft adds important business data to the localisation requirement without specifying what may constitute this business data. This may cause ambiguity when enforcing the Cyber Security Law.)
- Designating an internal function and a person-in-charge to be responsible for security administration. This person-in-charge and other personnel serving in key positions must pass a security background check.
- Providing periodic training on network security to and conducting periodic assessments of its staff.
- Having a disaster recovery back-up for important systems and databases.
- Making contingency plans for cyber security incidents and periodically organising staff drills.

Information security

The Second Draft sets out a similar position to that under existing regulations and rules on the protection of personal information but with an intention to enhance protective measures. Under the Second Draft, "citizens' personal information" means information recorded electronically or in other ways which can reveal a citizen's personal identity by itself or in combination with other information, including but not limited to name, date of birth, ID number, biological identity information, address and phone number. The Second Draft requires that the collection and use of citizens' personal information must be legal, appropriate and necessary for its purpose. A network operator must notify a user of the purpose, method and scope of information to be collected and obtain the consent of the user to do so. Network operators will need to

establish a user information protection system and adopt measures to prevent the leak, destruction or loss of collected personal information.

The Cyber Security Law also requires a network operator that discovers information released or transmitted by a user which violates Chinese law or regulation to cease providing transmission services to that user, delete and prevent the dissemination of the information, keep adequate records of the incident and report the incident to the relevant authority.

Legal consequences

The Second Draft introduces a new provision that permits provincial level authorities or above to interview the legal representative or responsible person of a network operator when a significant security risk is discovered or a security incident occurs. The network operator must take measures to minimise these risks and occurrences.

Penalties for breach of the Cyber Security Law include imposition of a fine on the network operator and/or directly responsible person(s), and the suspension of the operator's business, closure of its website, and revocation of its relevant permits and/or business licence.

The Second Draft also provides that a person will be barred from taking on key roles including the administration of network security or network operation if he or she has received an administrative or criminal penalty for activities that endangered network security. In addition, any illegal conduct under the Cyber Security Law will be recorded and published publicly.

Conclusion

As the Chinese leadership looks to expand the nation's economy through digital initiatives such as Internet Plus and Made in China 2025, the growing connectivity of over 1.3 billion people presents a huge challenge in relation to managing China's cyberspace.

The Cyber Security Law attempts to establish a two-directional regulatory system where both government and network operators share important roles to ensure network stability and operational control. While we expect further rules to be released after the Cyber Security Law is enacted, containing national standards for network products and services and the definition of critical information infrastructure, it is already clear that network operators will likely need to incur higher costs to comply with the requirements under the Cyber Security Law. In particular, as the Chinese government seeks to emphasise the censorship duty of certain industry players, network operators may have to improve their security, monitoring and data storage systems and procurement processes.

If enacted in its current form, the widespread scope of application of the Cybersecurity Law will impact not only network operators themselves but also other enterprises and institutions which necessarily rely on online communication, data transfer and data storage. Forward planning by businesses that may be affected is recommended to efficiently mitigate the

additional time and monetary costs which are inevitable if the proposed new regime comes into force.

Reference

Second Draft of the Cyber Security Law (网络安全法（草案二次审议稿）全文) (the "**Second Draft**")

Issuing authority: Standing Committee of the National People's Congress

Authors: Eva Wang, Alex Roberts, Eric Cheng and Michael Gu

Contacts

For further information please contact:

Richard Gu

Senior Consultant

(+86) 21 2891 1839

richard.gu@linklaters.com

Annabella Fu van Bijnen

Partner

(+86) 10 6535 0660

annabella.fu@linklaters.com

Alex Roberts

Managing Associate

(+86) 21 2891 1842

alex.roberts@linklaters.com

Eric Cheng

Associate

(+86) 21 2891 1855

eric.cheng@linklaters.com

Linklaters LLP Shanghai Office
29th Floor
Mirae Asset Tower
166 Lu Jia Zui Ring Road
Shanghai 200120 China

Telephone +86 21 2891 1888
Facsimile +86 21 2891 1818

Linklaters LLP Beijing Office
25th Floor China World Office 1
No. 1 Jian Guo Men Wai Avenue
Beijing 100004 China
Telephone +86 10 6505 8590
Facsimile +86 10 6505 8582

Linklaters.com