INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IDSA
Backgrounder

China's First Cyber Security Law

Abhishek Pratap Singh

December 23, 2016

Summary

China has justified the passage of the new law as an 'objective need' for national security considering its large cyber infrastructure and its vulnerabilities .

The passage of China's first Cyber security law on November 7, 2016 marks another step in the direction of increased oversight over the use of the internet in China. The regulatory framework for the use of Internet and related services in China will now be subject to the provisions of new Cyber security law that will go into effect from June 2017.

The promulgation of the new Cyber security law is very much in line with President Xi Jinping's concept of an "overall national security outlook", which he enunciated in his address at the inaugural meeting of the National Security Commission in April 2014.[1] China has justified the passage of the new law as an 'objective need' for national security considering China's large cyber infrastructure and its vulnerabilities.

Background and Rationale

Cyber law is a recent phenomenon at the level of governance, both in China, and globally. The need for cyber laws to provide a regulatory legal framework has been felt in the last decade with the onset of the Internet revolution, and its deep penetration into all aspects of the economy, society and governance of China.

While it has caused an attitudinal change in the behavior and, activity of the people, at the same time it has promoted technological innovation, economic growth, developments in fundamental research and social progress as well. Cyber security is of critical concern to the Chinese leadership with regard to its impact on social stability, political control and national development in China. There are frequent complaints of network intrusions and cyber attacks in China posing threats to the domestic critical information infrastructure. A single Shanghai-based hacking organization reportedly compromised at least 141 companies across 20 industries.[2] Moreover, there are concerns also over the use of ICT (Information Communication Technology) for terror activities and anti establishment activities, particularly in the Xinjiang province of China.

Similarly, other important ICT areas like cloud computing, big data, new technology and application development are making the cyber security environment more complex in China. There is also concern over illegal acquisition and disclosure of personal information, concern over infringement of intellectual property rights and rights of legal person or entity.

In the given context, state efforts in China are more directed towards allowing 'regulated access' to technology subject to security review, and data storage with state agencies. To safeguard national security, China seeks to restrict absolute online freedom at large.

1 "Commentary: China to follow specific national security strategy", *Xinhuanet*, April 16, 2014.

2 Declan McCullagh, China's Cyberwar; Intrusions are new normal, 19 February, 2013. Available at https://www.cnet.com/news/chinas-cyberwar-intrusions-are-the-new-normal-faq/

Evolution of cybersecurity laws in China

The Chinese concept of cyber security was clearly articulated in a 2013 speech by Lu Wei, the then head of the Cyber Security Administration of China. He described it as encapsulating cyberspace sovereignty, security of Internet information, security of privacy in cyberspace, and security of information technology.[3]

The concern for cyber security in China owes its origin to the Government Online Project (GOP) launched on 22 January, 1999, the basic purpose of which was to promote e-government system in China. This led to a paradigm shift in China's state delivery model with increased use of ICT for the allocation of goods and services. In order to offer more clarity on the regulation of online services in China, the government issued Guidelines of National Electronic Government Construction (NEGC) in October, 2000 which laid down some rules regarding fund allocation, scope of operation and coverage areas about online services in China.[4]

Similarly, the revised version of China's Criminal Law in 2011 laid down some provisions under its Chapter VI on Crimes of Obstructing the Administration of Public Order on cyber security. Under article 286 of revised criminal law it was specified that,

> "Whoever, in violation of State regulations, cancels, alters, increases or jams the functions of the computer information system, thereby making it impossible for the system to operate normally, if the consequences are serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention".[5]

In addition, the law (Article 287) also prohibits use of computers to commit crimes such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of State secrets. In 2013, Article 13 of the revised version of China's Protection of Consumer Rights and Interests Law specified that;

> "When a business operator collects or uses the personal information of a consumer, it shall follow the principles of acting in a legal, justifiable and necessary way and shall expressly indicate the purpose, method and scope of the collection or use of the information and obtains the consent of the consumer".6

In 2015, Beijing adopted a sweeping national security law that aimed to make all key network infrastructure and information systems "secure and controllable".[7] Thus the new law is not a 'sudden development' but the outcome of considerable

3 Xinhua December 10, 2013. Available at http://news.xinhuanet.com/world/2013-12/10/c_125838121.htm
4 Hong Xue (2010), Cyber law in China, pp. 32-33. Kluwer Law International, Netherlands.
5 China's Criminal Law Revised 2011. Full version available at http://www.china.org.cn/china/LegislationsForm2001-2010/2011-02/11/content_21899017.htm
6 Protection of Consumer Rights and Interest law in China, Revised 2013. Available at www.chinalaw.org
7 http://www.reuters.com/article/us-china-parliament-cyber-idUSKBN132049 Reuters, 7 November, 2016.

reflection on how to control this medium by the Chinese leadership.

Legislation and Key Provisions of the new law:

The process towards the passage of new Cyber Security law in China started in mid 2015. The National People's Congress (NPC) released a first draft of a Cyber Security Law on July 6, 2015. Comments and observations were invited before the law was proposed for a second reading before NPC. After almost a year, in late June, 2016, the NPC held a 'second reading' of the Cyber Security Law.

Subsequently, it was submitted to legislators for its 'third reading' at the bimonthly session of the NPC Standing Committee, to be adopted finally on November 7, 2016.

A reading of the law suggests that it basically focuses on three specific themes for the evolving cyber security regulatory framework in China. This includes cyber attacks or intrusions, illegal acquisition or disclosure of personal information and dissemination of information promoting or supporting terrorism or extremism.

Moreover, the law also makes specific references to technology regulation, data localisation and cooperation with authorities. Article 19 of the law refers to the development of "national internet information department" in China as a nodal center for preparation of a catalogue on the likely list of equipment and products to be sold in China.

The law also defines 'key information infrastructure' noting any damage, malfunction or data leakage to it that would seriously jeopardize national security in China. It requires a security review for data and information technology equipment used in areas like ICT services, transport and finance. The law grants public security agencies in China power to take necessary measures, including the freezing of assets, against overseas individuals or organisations that "attack, intrude, interfere with or sabotage the nation's key information infrastructure".[8] The new law calls for 'better protective measures' for key industries including public communications and information service, energy, transportation, finance and e-government service.

Article 23 of the new law makes 'network operators' subject to strict monitoring and increases state control over flow of information and technology equipment in China, raising concerns among foreign companies operating in the mainland. Under 'data localisation' (Article 31) provisions, the law disallows storage of personal information abroad. Foreign business operatives must store within China their critical and personal data information which they collect in course of their stay and activity. Defining 'critical areas', the law incorporates data localisation provisions for firms operating in ICT services, energy, transport, water resources and finance.

In addition, the new cyber security law also brings within its ambit the domain of 'personal data information', which till now was more the subject to administrative

8 http://news.xinhuanet.com/english/2016-10/31/c_135794643.htm Xinhuanet, Beijing, October 31, 2016

rules and guidelines in China. Any and all personal data collection by the operators and service providers must be done in conformity with the principle of prior 'notice and consent' to the users. In addition, any case of breach in data privacy of users must be reported with the authorities. The new law also disapproves of disclosure of anyone's personal information to a third party by the network operator or any service provider in China. It also allows a data subject or user to request for deletion of personal information available with the service provider if its custody amounts to violation of law.

The provision for 'data privacy' seems necessary considering the compulsory provisions under the new law for prior 'user verification' by the operators when providing services. In other words, since the service provider collects personnel information of its users, the law bounds him to follow strict measures to ensure its data privacy as well.

The new law also makes necessary provisions for 'security certification' for important network equipment and software companies. It also makes clear that certain entities operating in 'key industries' like energy, transportation and finance will be subject to very specific requirements. They are required to keep a record of related web logs for at least six months.

The new law calls for service providers in 'key infrastructure facilities' to clear a security assessment test conducted by the government according to the rules issued by Cyberspace Administration in China (CAC). (The CAC was established in 2014 to ensure better state control over cyber security network and Internet services in China.) This basically applies to service operatives whose services may affect national security in China. CAC along with other governmental agencies may conduct tests on network products and services that involve national security, to be carried out on an annual basis.

Moreover, the law also calls for unspecified necessary "technical support" to security agencies by firms operating in China. Network operators must provide technical support and assistance to public or national security agencies in China if required.

Many foreign business organizations have raised deep concerns over the strict provisions of new cyber security law in China. They are particularly concerned with provisions related to data localisation and security review by state agencies subject to CAC rules. Similarly, lack of clarity in law on what exactly constitutes 'key information infrastructure' leaves larger scope for relating any service network to national security in China and mandating security tests for the same.

This might impede their commercial interests and possible loss of competitive advantage. The security test might involve disclosure of their source code and other business secrets to the Chinese state security agencies, which many foreign business operatives will not find acceptable. Similarly, provisions related to 'data localisation' disallow cross border data transfer for service providers in China even if it is commercially viable. All these issues create operational challenges for service providers in China in future. However, China has defended the law as being in consonance with international trade and practices.

Conclusion

In sum, the new cyber security law seeks to establish greater state oversight over the cyberspace architecture in China. While China maintains that the new rules are necessary for national security, there are valid concerns from trading groups and commercial enterprises over cross-border data flows, protection of user privacy and excessive control over the Internet in China.

While China has defended it as a 'basic law' which strikes a balance between privacy and security, the legal language has led to fears that it might increase protectionism in trade and tighten even more the already strict censorship. Nevertheless, the long 'grace period' till June 2017 for its implementation might provide time to facilitate some changes in response to the dissenting voices.

About the Authors

Abhishek Pratap Singh is a Doctoral Candidate at the Centre for East Asian Studies, School of International Studies, Jawaharlal Nehru University, New Delhi.

The Institute for Defence Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
contact.idsa@nic.in www.idsa.in
Twitter @IDSAIndia
www.facebook.com/InstituteforDefenceStudiesAnalyses