Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
126/16

CHINA'S NEW CYBERSECURITY LAW: A REACTIONARY SOLUTION OR PROGRESSIVE CONSOLIDATION

Gp Capt Ashish Kumar Gupta
Senior Fellow, CAPS

On November 7, 2016 the Standing Committee of China's National People's Congress ("NPC") passed China's first Cybersecurity Law, which will come into force from 01 June 2017 onwards.[1] Christened by enthusiastic supporters as China's 'fundamental law' in the cybersecurity realm, the new law is being projected as an attempt to protect China's "cyberspace sovereignty" in line with the governments articulated priorities. The new law is also being viewed as an attempt to bring Internet related issues within legal framework and to consolidate overall network-security. Not surprising, once the law is effectuated, the Chinese government agencies will have greater enforcement and regulatory powers to control cyber activities. The law's effects are intended to be far broader than any previous regulatory initiatives and will have long-lasting implications for cyber ecosystem structure and function in China.

The Communist Party of China, while being weary of implications of unrestricted online access to information to its legitimacy, has enthusiastically promoted the use of Internet as an inalienable part of its quest for global hegemony, economic growth and orchestration of its technical prowess. With an estimated 688million people using Internet, China holds the distinction of having world's largest number of Internet users outnumbering the entire U.S. population two to one.[2] China views Internet as a fertile ecosystem that germinates, fosters, nurtures, and engenders political dissent, detrimental social activities and societal unrests. Chinese leadership since long has had an ambivalent relationship with the Internet. During Arab Spring in early 2011, China bolstered its censorship bureaucracy, reportedly creating a new office under State Council Information Office to "regulate every corner of the nation's vast Internet Community,"[3]

The new Cybersecurity Law, in part, is manifestation of objectives underpinned by President Xi Jinping on October 9, 2016, during CPC Central Committee on the implementation of cyber power strategy.[4]President Jinping, during his speech called for the development of secure and controllable technologies to enhance cybersecurity. The law has come under severe criticism from various quarters, including from within China, albeit not vociferously enough due to fears of a government crackdown. Foreign entities argue that the law threatens to force the foreign technology companies to shut shops in China and under the garb of security reviews is putting contentious regulations for data to be stored only in China. The proponents of Internet freedom argue that the law will *exacerbate the obstructive* conditions for accessing the Internet in China, already reeling under restrictive regime facilitated by the world's most sophisticated online censorship program 'the Great Firewall'. Some of the key features of the law are as follows:

- ***Obligatory Compliance with law by Network Operators***[5]

The new law mandatorily requires compliance with certain Chinese "national standards" by the providers of network products and services. Those products deemed "Critical Network Equipment and Network Security Products" would undergo testing by accredited evaluation centres before making a foray into the Chinese market. The Chinese government is contemplating issuing a comprehensive catalogue of approved products.

- ***Protection of Personal Information***

The new Law prohibit network operators to disclose, tamper with, or damage citizens' personal information that they have collected and are under obligation to delete unlawfully collected information and to amend incorrect information. Moreover, they can't share the collected personal information of citizens with others without consent.

- ***Protection of Critical Information Infrastructure (CII)***

The new Law has set the most stringent cybersecurity rules for the operators of Critical Information Infrastructure (CII) and their suppliers. The list of sectors that are defined as part of China's CIIs is expansive, making sectors such as telecommunications, energy, transportation, information services and finance subject to rigorous cyber security checks. China's lawmakers describe such provisions as mandatory to ensure protection of its CIIs from severe and multitudinous cyber threats.[6]

- ***Prevention of Cross-Border Data Transfer*** [7]

The data on citizens' personal information and important business data, collected or generated by the operators of CII must be stored

within the precincts of Chinese territorial borders. In case, the data is required to be transferred offshore for operational reasons, the associated process will be scrutinized and assessed by designated agencies for cyber security, compliance and risk.

- ***Penalisation of offenders of foreign origin***

The penalties for non-compliance by foreign organizations and individuals have been made more strict and have gone to extent to include freezing of assets or other sanctions in case found to be guilty of facilitating, perpetuating or attempting to attack any of the Chinese CIIs.[8]

- ***Protecting Minors in Cyberspace***

China's top internet regulator, the Cyberspace Administration of China (CAC), continues to set rules for the protection of minors in the context of online activities and data privacy. In October, CAC released for a new draft regulations '***Regulations on the Protection of Minors in Cyberspace'***, aimed at protecting minors on the Internet.[9] In line to efforts by CAC, the new Law sets forth general principles for the online protection of minors, intended to provide a basis for developing ancillary laws and regulations on the subject.

The offshore and home-grown companies operating in China are trying to quantify the impacts of potential enforcement and enactment of new regulatory law on their operations. In August 2016, 40 global business groups petitioned the Chinese premier, Li Keqiang, to amend controversial sections of the law. However, Chinese officials maintain that the new law will not interfere with or impede foreign business interests.[10] Foreign companies fear that the mandatory requirement for "critical information infrastructure operators" to store personal information and important business data in China would provide Chinese security agencies an excuse to open back doors within products or to hand over intellectual property. Human Rights Watch is concerned that some provisions of the law are draconian and run contrary to the principle of 'freedom of expression'. For example, the use of internet for activities which "damage national unity" would be criminal offence and would further tighten the noose on online freedom in China. .

However, in spite of global criticism, Chinese officials view the enactment and enforcement of the law as inalienable right and an indispensable defence against growing cyber threats and safeguarding its version of 'cyber sovereignty'. The full impact of the law on Chine cyber ecosystem can only be gauged once it is implemented and how the post implementation outcomes direct and shape the Chinese cyber 'Zeitgeist".

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] Charles Clover and Sherry FeiJu, China cyber security law sparks foreign fears, *Financial Times*, November 7, 2016 , https://www.ft.com/content/c330a482-a4cb-11e6-8b69-02899e8bd9d1, accessed November 28, 2016.

[2] Euan McKirdy, "China's online users more than double entire U.S. population," *CNN*, October 4, 2016, http://edition.cnn.com/2015/02/03/world/china-internet-growth-2014/, accessed November 28, 2016.

[3] Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Serach of Cyber Peace,* (Cambridge University Press, New York, 2014).

[4]United States Information Technology Office, "Xi Gives Speech on Cyber Power Strategy", http://www.usito.org/news/xi-gives-speech-cyber-power-strategy, accessed November 28, 2016.

[5] Covington & BurlingLLP China office, "China Passes New Cybersecurity Law", November 8, 2016, https://www.cov.com/en/news-and-insights/insights/2016/11/china-passes-new-cybersecurity-law, accessed November 28, 2016.

[6]Josh Chin and Eva Dou, China's New Cybersecurity Law Rattles Foreign Tech Firms, *The Wall Street Journal*, November 7, 2016, http://www.wsj.com/articles/china-approves-cybersecurity-law-1478491064

[7] Covington, n. 5, accessed November 28, 2016.

[8]Ibid.

[9]Grace Chen, Yan Luo and Ashwin Kaja, "China Issues Draft Regulations on Protecting Minors in Cyberspace", Covington & Burling LLP China office, October 21, 2016, https://www.insideprivacy.com/international/china/new-regulations-in-china-regulate-internet-privacy-of-minors/, accessed November 28, 2016.

[10] Reuters, China's new cybersecurity law sparks fresh censorship and espionage fears, *The Guardian*, November 7, 2016, https://www.theguardian.com/world/2016/nov/07/chinas-new-cybersecurity-law-sparks-fresh-censorship-and-espionage-fears, accessed November 28, 2016.