Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
01/17

CHINA'S NEW CYBERSECURITY LAW AND TAKEAWAYS FOR INDIA

E.Dilipraj
Associate Fellow, CAPS

On November 07, 2016, the 24th Session of the Standing Committee of the 12th National People's Congress of China passed the country's Cybersecurity Law. The law has received widespread criticism from foreign companies and foreign network providers and internet service providers operating in China calling it as an act of 'protectionism'[1]. Moreover, the critics of the law term it as a vaguely drafted document which could be exploited by the Chinese authorities in the future to impose their will on the foreign companies. China, on the other hand, has justified the need for this new law to bolster data security at a time of multiple threats.[2]

From an external observer's point of view, knowing China's nature of authoritarianism in its domestic policies, this new cybersecurity law should not come as a surprise. In fact, with the release of this new law, China has now legalised its already existing practices of controlling its domestic cyberspace.

The new law has seventy nine articles divided into 7 different chapters. Some of the highlights of the law are:

- The network operators are to adopt technological measures for monitoring and recording network operational statuses, security incidents, and follow relevant provisions to store network logs for at least six months.

  Such measures would require enormous investments from the network operators and hence small firms such as start-ups would suffer a setback as a result of financial crunch.
- The network operators are required to provide technical support and assistance to public and state security organs to preserve national security and investigate crimes.

  This clause again could be exploited by the Chinese authorities to extract the foreign companies' technologies on the pretext of gathering evidence for investigating crime.

Although it is believed that the authorities would not go to the extent of requesting the disclosure of source code, the vaguely worded clause makes it uncertain.

- According to the law a plethora of infrastructures such as public communication and information services, power, traffic, water, finance, public service, electronic governance, and more fall under the category of Critical Information Infrastructure(CII). And in order to avoid any data leak from these CIIs, the Security Council would formulate specific scope and security protection measures.

  The categorisation of almost all public infrastructures in CIIs clearly exhibits the protectionist attitude of the state. Also, the law has not defined what constitutes a CII, it keeps open the possibility for any infrastructure in China to be termed as one by the state authorities in the future if need arises.

- An important aspect of the law is that it also favours localisation of data. According to the law, any personal information or other data gathered or produced by the CII operators inside China must be stored in servers physically located inside the country. But if the operators require the data to be transferred outside the country's territory, then they are required to attain prior permission from the authorities, i.e. from relevant departments in the State Council.

  This clause in the law is a direct blow to the western promoted global cyber governance model, which promotes global free flow of data that is currently in existence around the world. It also restricts the operations of foreign operators associated with China's CIIs and puts their operations at the behest of China's State authorities.

- The law also prohibits persons or organizations from subverting national sovereignty or overthrowing the socialist system which is also a very important aspect of China's 2015 National Security Law. Also the law gives authority to State Council and other government entities to temporarily restrict internet access in a particular region as required by national security or to preserve social order.

  This clause in particular could be used to virtually cut off communications in parts of controversial Xinjiang province or any other region inside China in case of crisis or whenever the state authorities feel the need for it.

- The law also details the list of punishments for the violators and the list of punishments range from fines to prison term for individuals and hefty fines to freezing of assets for organisations.

- One of the highlighting positive aspects of the law is the provisions to restrict the amount of personally identifiable information that can be collected, limit how

it can be treated, and give an individual the right to request that information be deleted if mishandled.[3]

This aspect of the law is well received among the Chinese community especially the privacy advocates.

Takeaways for India

Understanding from an Indian perspective, the new cybersecurity law of China has few takeaways for India in terms of regulating the country's cyberspace.

First, being the country with the largest number of internet subscribers [more than 721 million], China has ably utilised the business it gives to the network and internet operators to its advantage and has legally asserted its will over these operators from around the world through this new law to establish its sovereignty over the country's cyberspace. In fact China's National Security Law, which came into effect in July 2015, also mandates that the Chinese government must take measures to protect national sovereignty, security and development interests in cyberspace.[4]

India is now ranked second in the list of countries with the largest number of internet subscribers with a count of more than 462 million and a penetration rate of around 34.8%. The country's growth rate is expected to be phenomenal in the future. India could thus utilize this aspect to its advantage while regulating the country's cyberspace and can establish its sovereignty over the country's cyberspace.

Second, India could take a cue from China by restricting the access and utilization of users' personal data by random organizations for their business gains in order to enhance privacy while the country is pushing hard for digitalization. Such an assurance of privacy in the form of a government policy could be an encouraging factor for people to accept digitalization in the desired format.

Third, like China, India has also got a considerable number of CIIs and being a country with the second largest population and with the push for digitalization, the country is going to generate humongous volumes of data in the coming years. Therefore, considering the amount of data, the sensitivity of it and the importance of having control over one's own data, it would not be unwise for India to look for options of localization of the country's data– at least from CIIs.

Fourth, by legally making the network operators to provide technical support and assistance to the public and state security organs for preserving national security and investigating crimes, China has entrusted more responsibility on the network and internet companies operating in its territorythrough the new law. Such an effort from the Indian side could also be favourable for the country as it would increase the responsibility on these foreign business

ventures in case of a crisis involving their product. Moreover, it can help reduce Indian security agencies' hassles in collection of evidence and other information for their investigations, and more importantly, can be a bypass for the time consuming MLAT[5] process.

Fifth, as a result of the country's regulation over cyberspace, the network and internet operators' responsibilities also increase. This might result in more investments from these companies not only to abide by the laws but also to not lose out the huge market potential and business existing in the country. Such investments would considerably help the growth of the country's economy on a longer run.

One aspect that India could avoid is the aspect of vagueness in the law. The Chinese new law is highly criticised for its vaguely worded articles which create a sense of suspicion among the operators in understanding the real intentions of the Chinese policy makers. Therefore, any policy regulation related to cyberspace from India should be a precisely worded document with definitions and clarifications at appropriate places.

India's cyberspace is a rapidly developing sphere which would need proper regulatory frameworks in the very near future. In this scenario, the unveiling of the Chinese new cybersecurity law and more importantly its implementation from June 01, 2017 needs a closer look as this would help India understand the reactions of the network and internet operators to such a stringent law and also the Chinese response to it. This would ultimately aid India to formulate more meaningful, precise and moderate policies for the country's cyberspace.

(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] Josh chin and Eva Dou, "China's New Cybersecurity Law Rattles Foreign Tech Firms", *Wall Street Journal,* November 07, 2016, http://www.wsj.com/articles/china-approves-cybersecurity-law-1478491064, accessed on December 27, 2016.

[2] Lotus Ruan, "What Does China's New Cybersecurity Law Mean for Chinese Internet Companies", *The Diplomat*, November 10, 2016, http://thediplomat.com/2016/11/whatdoeschinasnewcybersecuritylawmeanforchineseinternetcompanies/, accessed on December 27, 2016.

[3] Chris Mirasola, "Understanding China's Cybersecurity Law", *Lawfare*, November 08, 2016, https://www.lawfareblog.com/understanding-chinas-cybersecurity-law, accessed on December 29, 2016.

[4] Tang Lan, "National Sovereignty applies to cyberspace", *China Daily*, April 20, 2016, http://www.chinadaily.com.cn/opinion/201604/20/content_24681612.htm, accessed on December 31, 2016.

[5] A mutual legal assistance treaty (MLAT) is an agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.