RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 176 – 20 August 2015

China's New Cyber Security Policy: An Exercise in Control

By Eugene EG Tan

Synopsis

In recent months, China has become more assertive in its cyber security policies, asserting its right on its own "cyberspace sovereignty". The motivations over the move towards more stringent cyber policies are examined in this commentary.

Commentary

CHINA, THROUGH its official newspaper, China Daily, announced on 28 May 2015 that it will prepare a five-year cyber security plan to protect state secrets and data. Earlier in May, China also included cyber security into its draft national security law to tighten the legal framework governing its cyberspace.

Although China's approach to cyberspace governance has been somewhat heavy handed, there have been marked developments and heightened intervention in China's cyberspace policy in the past year. The details of this policy change have yet to be fleshed out, but bigger question marks loom over the motivations and the timing of this policy change.

National Security Posture

This change *prima facie* is to further improve China's national security posture in cyberspace, amid allegations that software codes designed by American firms allow for the United States to gain access to data from Chinese users. According to the Chinese government, the new plan would focus on improving the security for software used by government departments, state-owned enterprises and financial institutions.

China has also been trying to move away from foreign providers of software after Windows ended support for its XP operating system in mid-2014, rendering the majority of Chinese government computers, which mainly still run XP, at risk to security breaches. In retaliation, the Chinese government chose to exclude the Windows 8 operating system from its procurement lists, and supported the organic local development of Linux-based operating systems.

However, this is not the first time China has taken action on foreign software providers. In a move to bolster its cyber security in January 2015, the Chinese government forced United States companies selling software to state-run Chinese finance firms to hand over the source codes and use Chinese-

designed security algorithms instead. Heightened security checks have also been placed by the Chinese government on United States-based vendors before these products can be used by state-owned financial institutions.

The refusal of United States government agencies to allow Chinese hardware manufacturers to sell equipment, on suspicion that backdoor mechanisms are written into the code and hardware to conduct surveillance, has also fuelled the national security debate in China. Chinese authorities have argued that the degree of control that its government is exerting on technology companies is similar to that of the United States government, and it is well within its rights to do so.

Nationalism and party survival

Amid the bluster over national security issues, the desire to protect the legacy and legitimacy of hegemonic ideological control by the Chinese Communist Party (CCP) cannot be overlooked in this cyber security policy change. In a draft national security law in June 2015, there was renewed emphasis on safeguarding against "harmful moral standards" – suggesting that dissent against the values of the party and the state will be clamped down.

While this stance on dissent and the absolutist nature of state control is not new, the timing of the announcement does highlight the preoccupation of the party with the control of information dissemination, especially in cyberspace where party rhetoric and persecution of activists have been ratcheted up. The Cyberspace Administration of China released Cyberspace Spirit in February 2015, a song that extolls the virtues of internet control. The lyrics further reveal the desire of China to be a strong nation in cyberspace, and the use of the internet to propagate positive messages about China.

With positive messaging in cyberspace the goal of the Chinese government, criticism has been brutally suppressed. In late-May 2015, a prominent activist-blogger against government abuse, Wu Gan, was arrested in Jiangxi on charges of defamation, "inciting the subversion of state power", and "picking quarrels and provoking trouble". The arrest of the high-profile Wu was trumpeted across all state media, and showed the state was changing gears in response to well-received online dissidents for fear of losing control in cyberspace.

Implications of tighter control

Cyber security in China thus is not solely a one-dimensioned effort to keep intruders out of China's cyberspace, but also is an attempt to control voices bounded by the great firewall. The abrupt tightening of cyber security measures seem to suggest that China is increasingly wary of the impact that voices and activities in cyberspace can cause in the physical realm.

It is also because of this insecurity that China will be more assertive in its posture with regard to its foreign partners, be it governments or private vendors. Lu Wei, Director of China's State Information Office, put it bluntly in December 2014, that the current multilateral international state system, and not a multi stakeholder model, is China's solution to cyberspace management. The ownership of the internet in China belongs to the state alone, which control will only strengthen.

Hence, it can be seen that cyber security is of paramount importance to the Chinese government, not just because of the security of its systems, but also the political implications of maintaining control over the monopoly of information which is too great for the Chinese government to ignore. The nationalist and party-centric leanings of the new National Security policy need to be further unpacked with regard to issues that involve the Chinese national interest, like territorial claims and terrorism, as well as party interests such as corruption and abuses of power.

Eugene EG Tan is an Associate Research Fellow with the Centre of Excellence for National Security (CENS), a component of the S Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.