China's Cyber Security Strategy: Global Implications

GAUTAM SEN

Introduction

To understand the cyber security strategy of China and its implications, one has to accept that cyber space and Information Technology (IT) have enabled the economic, political, and cultural integration of China. However, IT raises new challenges for states by allowing actors to exploit networks, conduct cyber espionage, or compromise national security with greater ease. The purpose of this short exposition is to record how China, at the 36th Collective Study Session of the Communist Party of China (CPC), in October 2016, unfolded the theme of implementing the nation's strategic plans to emerge as a cyber superpower. General Secretary Xi Jinping stated, "China must work toward its goal of becoming a cyber power by accelerating reinforcement of security and defense capabilities in cyber space, accelerating the promotion of social governance using IT, and accelerating the advancement of China's right to speak internationally and right to set rules governing cyber space."[1] Subsequently, the Chinese government adopted the Cyber Security Law in November 2016 (which took effect in June 2017). This was followed by the declaration of the National Cyber Security Strategy in December 2016, and the International Strategy of Cooperation on Cyber Space in March 2017. These primary documents show China's aggressive and active pursuance in developing its cyber security doctrine to be at par with those of the most advanced nations of the world.[2]

The Narrative

As China continues to develop and grow in influence, it must also be prepared to confront challenges to Western dominant norms in policy areas such as cyber security. China has been actively promoting a counter-narrative: justifying stringent Internet controls through propaganda, denying involvement or accountability in cyber espionage, and accusing the United States of committing similar actions against China.[3] In the light of these challenges, how should we view China's strategic intentions? What is China trying to achieve? The Chinese government currently faces bureaucratic burdens and other domestic obstacles in implementing an optimal cyber strategy. However, it has, since 2012, dedicated significant efforts to remedy its shortcomings.

Normative Aspect

China's normative thinking about cyber security, and its cyber security strategy consists of three main component drivers: economic, political, and military. Important manifestations of those drivers are:

- Maintaining economic growth and stability, which involves industrial economic cyber espionage of the US and other foreign targets
- Protecting the governing power of the CPC through information control, propaganda, and targeting of domestic sources of potential unrest
- Using computer network operations to signal dissatisfaction with foreign powers over developments outside China (e.g. maritime territorial disputes, foreign allegations of Chinese hacking activity) that negatively affect China's reputation
- Preparing for military scenarios and ensuring military superiority in the event of cybered conflict with an adversary through military modernisation, computer network operations research, and human capital cultivation
- Studying and understanding potential adversaries' military infrastructures, motivations, objectives, capabilities, and limitations in the cyber domain
- Advancing alternative narratives of government control over/handling of cyber security internationally (e.g. the promoting sovereignty of states to control the Internet within a country's borders) and domestically (e.g. justifying domestic surveillance, information control).

The domestic policy and military modernisation over the past several years indicate that China has given cyber security the highest priority. Despite high-level guidance and strategic direction from President Xi Jinping and senior civilian and military officials, the implementation of China's cyber security

Chinese Cyber security definition encompasses intelligence activities during emergency and political warfare during peacetime.

strategy remains fragmented and its bureaucratic structure remains disorganised, characterised by competition for stakeholders, resources and influence on policy direction which includes:

- High-level decision-makers.
- Politburo Standing Committee.
- Central Military Commission (CMC).
- State Council Commission for Science, Technology and Industry for National Defence (COSTIND) [before it was dissolved in 2008, part of its duties went to the State Administration for Science and Technology and Industry for National Defence (SASTIND)].
- Civilian government agencies (e.g. Ministry of Industry and Information Technology (MIIT).
- Ministry of State Security (MSS), SASTIND.
- State Secrets Bureau.
- State Encryption Bureau.
- Party and state leading groups.

The Chinese cyber strategy has often been called the "network strategy,"[4] because in China, the term "cyber" is rarely used. Interestingly, semantic issues such as these reveal the deep gaps when one studies the issues, especially between China and the United States in respect of the two countries' security infrastructures. While the United States uses the term "cyber security"[5] to refer to the protection and defence of a wide array of electronic and communications information, China, according to Amy Chang, uses the term "network security" (网络安全, *wangluo anquan*) to refer more specifically to the protection of digital information networks. The term "information security" (信息安全, *xinxi anquan*) refers to a broader swath of information and communications systems.

Future Trends / Implications of China's Cyber Security Strategy

The following three points should be considered in terms of future trends in China's cyber security. First, cyber security in terms of China's military includes not only intelligence activities during an emergency, but also political warfare during peace-time. The Chinese government considers political warfare during peace-time to comprise the 'three warfares' of public opinion, psychology, and law. The problem is that China's approach to traditional political warfare and this manoeuvering has developed on the back of the country's vast economic might and new technologies. For example, the perpetrators of theft of confidential information and alteration of information in cyber space and cyber attacks inciting public opinion through false rumours are difficult to identify, and, in the case of smaller scale cyber attacks, it is difficult to even notice them. On a more strategic level, through cyber attacks, China attempts to incite public opinion and cause wavering of decision-making by leaders of countries that are locked in disputes with China. At the same time, keen China observers have noted that China isolates opposition internationally, legitimises its own responses, and deals with conflict in an advantageous matter without resorting to armed conflict. This type of political warfare in cyber space could cause various grey zone situations that blur the lines between peace-time and war-time. Further examination is needed concerning this point to make an empirical assessment of the behaviour of the Chinese and the development of their policy imperatives in this area.

Second, also relating to the above are the standards and thresholds for military attacks in cyber space. The *2013 Science of Military Strategy*, published by the PLA Academy of Military Science, states, "Cyber warfare is low cost and highly effective, so cyber warfare is easier to occur than other types of war." Conversely speaking, the psychological hurdle to cyber warfare, even in China, may be lower than conventional war.[6] For example, one can observe that with regard to soft skills such as cyber attacks (on information) that do not cause physical damage to the command systems of enemies, known as Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), there are some researchers who point out the possibility that China considers these as defensive measures to avoid escalation to war.[7] However, assuming that if a target country considers this as a military attack, there is a risk that the situation could escalate to warfare beyond merely a conflict situation and result in the use of conventional weapons.

Third is the difference between awareness of a deterrent in cyber space. In a speech in April 2016, General Secretary Xi stated, "China will reinforce its cyber security defense capabilities and coercive capabilities. The fundamental essence of cyber security is antagonism and the essence of antagonism is the competition between offensive and defensive capabilities." China's coercive capability is a concept close in meaning to deterrence. Analysing China's *2015 Science of Military Strategy* document, cyber deterrence can be categorised into: (i) strategic level deterrence where cyber attack capabilities against another military's C41SR system or core transportation and communications infrastructure deter the other party's cyber attacks; and (ii) tactical level deterrence that can hold in check dispersed,

Cyber warfare is low cost and effective and hence easier to occur than other forms of war.

small scale cyber attacks and cyber penetrations.[8] With regards to cyber deterrence, the basic conditions for forming a deterrent relationship of (i) intention; (ii) capability; and (iii) mutual understanding represent a fundamental problem because they are extremely vague in cyber space. In other words, costs are required to identify cyber attackers, and in addition to the difficulty of assessing China's attack and response capabilities, there is the problem of what exactly China considers to be a military attack in cyber space. For example, in terms of government criticism and the spread of misinformation, the Chinese government may determine this to be a cyber attack depending on the scale and situation. In such an instance, it is not clear how China would retaliate and against who. While keeping such difficulties in mind, if China seeks to reinforce its deterrence capabilities in cyber space in the future, the international community must deepen its understanding of China's intentions and capabilities as well as promote mutual understanding through communication.

Conclusion[9]

Taking into account the above, when considering Japan's cyber security, one must pay attention to both competing and cooperative aspects. As for the former, Japan's own initiatives and establishment of deterrence capabilities under the Japan-US alliance can be cited. For example, technological Research and Development (R&D) related to cyber defence, reinforcement of survivability of important cyber infrastructure, and development of highly advanced cyber personnel such as that currently being examined mainly by the National Centre of Incident Readiness and Strategy for Cyber Security (NISC) will contribute to Japan's deterrence by denial. With an eye on expanding the deterrent through the Japan-US alliance, deterrence capabilities through punitive measures in cyber space will also need to be examined. Therefore, Japan will need to closely discuss with the US about approaches to cyber security cooperation, including sharing of China's cyber attack risk and capability assessment information, and retaliatory measures for various situations, from peace-time to emergencies. This methodology will have to be adopted by countries like India, Nepal, Burma and even Pakistan in the South Asian context and those that share land borders with China. It is interesting that the countries mentioned do have an enunciated cyber security strategy in one form or the other but not as developed like those of Japan, the US and UK, as listed in the National Cyber Security Strategies Repository.[10]

In terms of collaborative responses, establishing a mechanism for a bilateral dialogue with China concerning cyber security can be cited. The US and China agreed to establish a dialogue mechanism on cyber space at the summit meeting held in September 2015, and already several ministerial level talks and working group discussions have taken place. These dialogues appear to be limited to cyber crimes and preventing theft of intellectual properties, but they also appear have had a certain effect.[11] The Chinese government considers itself a victim of cyber attacks and, at the same time, it is actively cracking down on cyber crimes that could inhibit the country's economic growth. Consequently, from this point at issue, through establishing information exchanges and a dialogue mechanism, it is possible to reduce the number of unnecessary cyber attacks and business espionage, and foster trust in the process. Already, cyber discussions have taken place among the diplomatic authorities of Japan, China and the Republic of Korea on three occasions. While utilising such mechanisms, higher level bilateral frameworks and cyber discussions between the defence authorities can be examined.

Also, from the standpoint of cooperation with the international community, it will be important to actively involve China in the formation of international rules on cyber security. Joseph S. Nye of Harvard University points out as one element for deterring cyber attacks the formation of international rules for sharing taboos on the scope of cyber attacks, and toward this end, the fostering of trust between countries.[12] While it may take a long period of time to conclude a new international treaty related to cyber security that China seeks, the results of strongly policy-inclined discussions such as the Tallinn Manual led by the North Atlantic Treaty Organisation (NATO) Cooperative Cyber Defence Centre of Excellence(CCDCOE) represent a relatively low political cost, which, while not legally binding, contribute to fostering international rules for deterring cyber attacks.

Prof **Gautam Sen** is a Distinguished Visiting Fellow, CLAWS.

Notes

1. "Xi Jinping: Accelerate the Indigenous Innovation Using IT; Making Continuous Efforts Toward the Goal of a Cyber Superpower," *CPC News,* October 10, 2016, http://cpc.people.com.cn/n1/2016/1010/c64094-28763907.html. Hereafter, final access for all sites occurred on May 11, 2017.
2. "National Cybersecurity Strategy", *Xinhuanet,* http://news.xinhuanet.com/politics/2016-12/27/c_1120196479.htm: "International Strategy of Cooperation on Cyberspace", *Xinhuanet,* http://news.xinhuanet.com/politics/2017-03/01/c_1120552767.htm.

3. Gerry Shih, "China's Internet Chief Accuses U.S. of Hacking but Says Talks 'Unhindered'," Reuters, October 30, 2014. http://www.reuters.com/article/2014/10/30/china-cybersecurity-idUSL4N0SP2QE20141030.
4. See for details, Amy Chang, "Warring State: China's Cybersecurity Strategy", where the various definition are as follows : ***NETWORK WARFARE***: The People's Liberation Army's (PLA's) military dictionary defines "network warfare" (网络战, *wangluo zhan*) as: "Also known as network confrontation. The destruction of the adversary's network of information systems and network information, the undermining of effectiveness of the adversary's use of its capabilities, while protecting one's own network of information systems and information in cyberspace".

   NETWORK PROTECTION: The PLA's military dictionary defines "network protection" (网络防护, *wangluo fanghu*) as: "To protect one's own information network system and data and taking preventative measures and actions to keep information safe, effective and functioning; includes network isolation, access control, intrusion detection, attack traceback, etc."

   INFORMATION DEFENCE: The PLA's military dictionary defines "information defence" (信息防御, *xinxi fangyu*) as: "Also known as information protection. Ensuring the stable operation of one's own information systems, information security and the correct decisions and measures taken. Information defense includes electronic defense and network protection."

   INFORMATION OFFENCE: The PLA's military terms dictionary defines "information offence" (息进攻, *xinxi jingong*) as: "Information attacks. The utilization of information warfare technology to interfere with, and sabotage, enemy information operations and information systems. Important tactics include electronic attack and network attack. The purpose is to affect and weaken the enemy's information acquisition, transmission, processing and utilization decisions."

   INFORMATION SECURITY: The PLA defines "information security" (信息安全, *xinxi anquan*) as: "The protection of information collection, processing, transport, and use from disruption, destruction or theft; the protection of normal use of information by its legitimate owners. Information security includes information content security, information systems security, information infrastructure security, information exchange security and information security awareness."
5. See "National Initiative for Cybersecurity Careers and Studies", glossary definition of "cybersecurity," http://niccs.uscert.gov/glossary#cybersecurity.
6. The Strategic Research Department of the Chinese Academy of Military Sciences, *The Science of Military Strategy* (Military Science Publishing House, 2013), p. 191.
7. Joe Mcreynolds, *China's Evolving Military Strategy* (Washington DC: The Jamestown Foundation, 2017), pp. 183-184.
8. Xiao Tianliang, *The Science of Military Strategy*, p. 147.
9. While composing this section, I have immensely used the deliberation published by Masaaki Yatsuzuka, *China's Basic Awareness of Cybersecurity* (National Institute for Defence Studies), at Website: http://www.nids.mod.go.jp/
10. See National Cybersecurity Strategies Repository, https://www.itu.int/en/ITU-D/Cyber security/Pages/National-Strategies-repository.aspx
11. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol 41, No 3, Winter 2016/17, pp. 60-62.
12. Ibid.