RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 045 – 4 March 2015

Decoding China's Cyber Warfare Strategies

By Michael Raska

Synopsis

While conventional, low-intensity, asymmetric, or non-linear conflict scenarios are plausible for East Asia's strategic flashpoints, the next major conflict involving China will likely start in cyberspace.

Commentary

EAST ASIA'S strategic assessments and debates currently focus on five key issues: the pace, character, and direction of China's military modernisation; the struggle for dominance by the region's two major powers (China and Japan); the future of the Korean Peninsula; intra-regional competition in territorial disputes in the East China Sea and South China Sea; and perhaps most importantly, the contours of long-term regional strategic competition and rivalry between China and the United States. In every major security issue facing East Asia, however, there is a major Chinese footprint, both direct and indirect.

Traditionally, China's primary strategic interests, influence, and military modernisation initiatives have aimed at prevailing in any future conflict over the status of Taiwan. While Taiwan scenarios remain the baseline for the PLA defence planning, China's military is gradually developing asymmetric warfare strategies and technologies designed to constrain US freedom of action in East Asia. Notwithstanding China's development of fifth-generation air platforms, standoff precision weapons, ballistic and cruise missiles, early warning, intelligence, surveillance and reconnaissance assets to naval assets, the key emphasis in PLA strategy is the applicability of computer network operations. Indeed, the next main conflict involving China will likely start in cyberspace.

PLA's Integrated Network Electronic Warfare

The PLA envisions future conflicts under the conceptual umbrella of Integrated Network Electronic Warfare (*wangdian yitizhan*) or INEW. China's strategic thought on cyber warfare closely emulates the Russian conceptions in a holistic representation that combines coordinated use of computer network operations (CNOs), electronic warfare (EW), and kinetic strikes designed to paralyse an enemy's networked information systems, and by creating "blind spots" against an adversary's C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems. These concepts are reflected in PLA's evolving doctrine of "Informationised Conditions" that envisions future campaigns conducted in all domains simultaneously: ground, air, sea, space, and cyberspace.

While specific operational aspects and capabilities are shrouded in secrecy, publically-available writings by PLA's semi-authoritative military sources such as the Academy of Military Sciences

indicate a simultaneous application of mutually-reinforcing and multiple force elements. These include (1) PLA's Electronic Warfare and Counter-Space Forces using electronic jamming, electronic deception and suppression to disrupt information acquisition and information transfer; (2) PLA's Computer Network Attack and Exploitation Units to disrupt, destroy, or subvert an adversary's data and networks using advanced virus attacks, hacking, deception, and sabotage information processing.

Information Dominance and Space-Based Information Asset Control

In such campaigns, PLA's INEW concepts of operations would be widely employed in the earliest phases of a conflict, and possibly preemptively with the objective to deny the enemy's access to information essential for continued combat operations. In particular, achieving information dominance (*zhi xinxi quan*) is a key prerequisite for seizing PLA's air and naval superiority, according to "*The Science of Military Strategy*" and "*The Science of Campaigns*" - two of the PLA's most authoritative public statements on its doctrine for military operations. Both documents identify an enemy's C4ISR and logistics systems networks as the highest priority for select INEW operations.

At the same time, the PLA recognises the importance of controlling space-based information assets as a means of achieving true information dominance, calling it the "new strategic high ground". In this context, the PLA is seeking to develop the capability to use space for military operations, while denying this same capability to an adversary. Specifically, PLA authors acknowledge that space dominance is essential for operating joint campaigns and for maintaining the initiative on the battlefield. Conversely, they view the denial of an adversary's space systems as an essential component of information warfare and a prerequisite for victory. To this end, the PLA maintains a strong R&D focus on counter-space weapons, both kinetic and cyber.

"Peacetime" Cyber Espionage

During conditions of peace time, China's cyber units are involved in a comprehensive cyber reconnaissance - probing the computer networks of foreign government agencies as well as private companies. These activities, which China denies, serve to identify weak points in the networks, understand how foreign leaders think, discover military-communication patterns, and attain valuable technical information stored throughout global networks. The scale, focus, and complexity of Chinese cyber espionage over the past decade strongly suggest that these operations are state-sponsored or supported with access to financial, personnel, and analytic resources that far exceed what organised cybercriminal operations or multiple hacker groups operating independently could likely access consistently over a long-duration.

What does it all mean for future strategic stability and defence planning for states in East Asia? On one hand, it is clear that China's information/cyber capabilities are continuously evolving parallel with PLA's ongoing military modernisation. With the increasing sophistication and integration of cyber concepts, technologies, and capabilities into PLA's doctrine, organisational force structure, training, and overall use of force, future cyber/kinetic interactions will increase in strategic significance. The essential problems, however, remain in the difficulties in identifying the direction and character of cyber threats, which increasingly blur both civil and military domains.

Accordingly, the development and diffusion of cyber capabilities, both offensive and defensive, will yield new types of hybrid conflicts that may lead to new balances of power between nation-states, and alter the contours of East Asia's future strategic environment.

Michael Raska is a Research Fellow at the Institute of Defence and Strategic Studies, a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.