RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 172 – 17 August 2015

Cyber-Enabled Hybrid Conflicts in East Asia

By Michael Raska

Synopsis

As new strategic realities create new powers, new types of future conflicts emerge. In East Asia, these will include new forms of cyber-enabled conflicts defined through a convergence of 'cyber-kinetic-information domains' and their strategic interactions.

Commentary

EAST ASIA'S current strategic template hinges on a convergence of unresolved historical legacies and emerging security challenges, characterised by a mix of asymmetric threats, low-probability / high-impact risks, and a range of non-traditional security challenges. These are amplified through a perennial strategic distrust, which propels a regional "arms competition" and diffusion of advanced military technologies in nearly every combat domain.

At the same time, however, regional powers acknowledge the interlocking economic interdependencies and consequences of potential conflict escalation. Therefore, their strategic choices point toward a long-term competitive strategies, including novel ways and means of asymmetric negation short of major wars.

Netwars and information spheres of influence

One of the quintessential aspects of the cyber-enabled hybrid conflict spectrum is strategic ambiguity - in terms of effects, sources, and motives. The cyber domain amplifies the use of ambiguity - neither confirming nor denying the use of force vis-à-vis existing or potential adversaries and their selective proxy targets. Direct, and to a lesser degree, indirect results of cyber-attacks are often invisible, which creates uncertainties about the sources of the intrusion, attack, or malfunction.

Even if the source is known or detected, the purpose of the cyber-attack might be less clear. Accordingly, cyber-attacks may be used as a response to a limited kinetic attack or aggression with a lesser risk of escalation than a physical retaliation. At the same time, however, strategic ambiguity in the use of cyber may increase the propensity for offensive and unrestricted cyber warfare given the prevailing perceptions of lesser risks of detection, the lack of accountability, and the resulting low probability of successful deterrence.

The development of ambiguous cyber warfare strategies, however, transcends the cyber domain. Cyber-enabled conflicts are embedded in the broader context of information conflicts – political, economic, information, technological, media, and ideological struggles for influence. In the 1990s,

John Arquilla and David Ronfeldt introduced the concept of 'netwars' – information-related conflicts between nations or societies, in which opponents are trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it. Traditionally, netwars have been conducted through public diplomacy, propaganda, psychological campaigns, intelligence operations, as well as through traditional print media and television.

Social media and strategic vulnerabilities

Today, social media have brought netwars or information conflicts to a new level. In essence, social media enable protagonists to seed ideas, deliver information campaigns, and shape narratives for specific target groups in real time and with no geographic limitations. The diffusion and sharing of selective information generates 'certainty' which creates, to varying levels of influence, 'conversion' of target groups.

This is done by exploiting existing tensions or identifying new fracture points within target groups, and conveying selective information to select audiences to influence their emotions, motives, objective reasoning, and ultimately their behaviour to favour 'friendly' objectives. In doing so, social media campaigns may target a national will, regional or group audiences to gain support and weaken opposition, to individual targets to enhance particular narrative at a local level. At the same time, they provide defensive aspects – preventing opponents from using or manipulating information to gain an advantage.

Sceptics may argue that there are serious limitations with regard to the use of cyberspace for political purposes. However, the continuously evolving character and reliance on cyberspace in both civil-military domains provides a new arena for strategic competition, increases uncertainty, and enables a spectrum of operations other than war. Accordingly, traditional regional security flashpoints in the East and South China seas, the Korean Peninsula, the Taiwan Strait will likely have parallel and continuous confrontations in and out of cyberspace, with potential cyber-attacks on physical systems and processes controlling critical information infrastructure, information operations, and various forms of cyber espionage.

The progressive complexity in strategic interactions and interdependencies between cyber, information, cognitive, and physical domains will likely challenge traditional kinetic uses of force in future conflicts. For example, in ensuring operational access in the East or South China seas, the US military will have to ensure the security, reliability, and integrity of its mission-critical command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems as well as combat support and logistics systems.

Shifting centres of gravity

These will become increasingly vulnerable to cyber threats as well as other emerging forms of electronic warfare, including threats from electromagnetic pulse and high-powered microwave weapons. A sophisticated cyberattack on these systems would likely result in cascading effects on the individual services with ramifications on their abilities to carry out operational missions.

As conflicts move into the cyber and information domains, the centres of gravity are going to shift. The value and more importantly, the accuracy and reliability of strategic information relevant for the situational awareness and function of the nation state as a system will become even more important with the increased dependence on cyberspace.

Cyber-enabled conflicts will evolve in parallel with technological changes – e.g. the introduction of the next generation of robots and remotely controlled systems that will continue to alter the character of future warfare. Ultimately, however, both cyber and information domains – whether civil or military - may become simultaneously targets as well as weapons.

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, Singapore.

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg