RSiS Nanyang Technological University | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

RSIS COMMENTARY

www.rsis.edu.sg No. 136 – 11 July 2014

Emerging Cyber Capabilities in the Asia Pacific: Potential Military Impact

By Caitríona H. Heinl

Synopsis

The Asia Pacific comprises diverse countries with conflicting ideologies and different states of development. Given the variety of challenges and tensions over territorial disputes and geopolitical uncertainties across the region, a careful analysis of cyber capabilities and their possible impact would be valuable.

Commentary

The Asia Pacific is a diverse region comprising countries with conflicting ideologies that are at very different stages in terms of cyber technologies and both strategy development and implementation. Capabilities considered as new and emerging technologies in one state or a number of states are not always new throughout the region; although the current speed of technological change means most countries are still challenged.

This often means that timely and effective implementation of policy and legislation is made more difficult, especially when it can be difficult to fully and quickly understand the implications of these new technologies.

Implications for the Asia Pacific

There are four implications for the Asia Pacific. First, acquiring offensive cyber capabilities can often seem financially attractive, in particular for less wealthy states in the region, relative to the higher costs of other weapons. Moreover, by contrast, bolstering defences might be considered more difficult, more expensive and take longer to implement. In many cases, strong defence infrastructures are not even in place within these countries.

This is particularly significant for this region where many states are spending increasing amounts on arms capabilities and the military compared to the U.S. and EU where military budgets are being considerably reduced. Although, in relative terms, the overall U.S. budget still far outweighs that of other countries and the U.S. has not decreased the cyber defence budget to the same extent as other fields, this balance could eventually shift over the medium term. If defence reports are correct in their analysis, China's defence spending may be three times as much as the U.S within 20 years if China maintains its current levels of defence spending as its economy continues to grow.

Second, accurately attributing responsibility for cyber incidents can be difficult. This means that misunderstandings could arise between states, tensions could possibly escalate, or it might be harder to ensure effective deterrence. These apparent difficulties in appropriating blame on top of the advantages of once-off or lower costs are therefore attractive, particularly for states with limited financial resources, capabilities and expertise. This is especially relevant where weaker entities might avoid open confrontation and instead exploit vulnerabilities. Although in light of more recent statements claiming that anonymity is not necessarily guaranteed, they could seriously risk reputation damage and physical retaliation if found responsible.

Third, most countries in the region are challenged in the near term by a skills shortage in this domain. Although China and India are exceptional since they not only have excellent ICT sectors and financial resources, they also have large growing pools of manpower. For now, they are continuing to invest in this domain as well as cultivating indigenous ICT to reduce supply chain security concerns and reliance on imports. Likewise, defence reports suggest that the scale and pace of their innovative and industrial capacity will outpace many Western nations in a matter of years and China is likely to attain and sustain global leadership in a number of technical areas including computer science.

Fourth, non-state actors further complicate this space. Cyber criminals, terrorists, hackers, hacktivists, and proxy actors must equally be considered. Moreover, some argue that growing cybercrime in this region could cause further instability because of connections to espionage and military activities. These points align with projections that the character of war is likely to continue to be shaped not only by a system of rival states but by forces outside the state-centric systems.

This is important given that there is a large and active “Internet militia” comprising hacker communities and information security experts in this region. The majority of these, according to defence reports, are likely to be part of government structures or programmes while others, although operating independently, are under the influence of or tolerated by national authorities. Where such actors are active on state instructions, or under its direction or control in carrying out conduct, experts’ findings conclude that this may then be attributable to the state and give rise to its international legal responsibility. Further, reports assert that countries are likely to mobilise these groups as part of coordinated national efforts during periods of conflict.

Future Projections

Military structures are still adapting to these emerging technologies and future warfare will most likely comprise a cyber component. These technologies will support or substitute conventional war and might be used to destroy a nation’s ability to wage war. Nevertheless, at this juncture, it seems most state and non-state actors do not have the operational sophistication for devastating attacks although unexpected outcomes could arise accidentally. Instead activities will likely include espionage, interference with information and networks, restricting situational awareness, and disrupting infrastructure, financial systems and social networks.

Policy reports argue that increased military developments are expected in cyber within the region. Defence analyses equally predict that many South Asian states will undertake state-sponsored programmes facilitated by low barriers of entry, large pools of skilled manpower, and extensive IT infrastructures in order to project influence that would otherwise be limited using conventional instruments. The U.S, China, Australia, Singapore, and South Korea lead in military aspects of cyber capabilities according to a recent ASPI report. Significantly, this report highlights North Korea’s increased use of cyber capabilities over the period 2013-2014 as especially concerning since it places the South Korean government under further pressure to ensure incidents do not escalate.

Nevertheless, given current sensitivities surrounding cybersecurity, in particular cyber capabilities, it is difficult to precisely ascertain the extent to which states in the Asia Pacific have developed or acquired capabilities, especially advanced cyber capabilities.

Transparency and Confidence Building Measures

Although threat assessments calculate that advanced state actors are unlikely to launch a devastating cyber attack, this is based on the premise that there is no military conflict or crisis threatening vital interests.

Maintaining stability in this region is of primary importance. Although it is unlikely that cyber capabilities will significantly change the power balance for the near term, there is still a need for improved confidence building and transparency measures like military-to-military engagements, increased dialogue, information sharing, joint exercises, official contact points, and crisis communication procedures or hotlines to prevent misunderstandings, false attribution, or further escalation in already terse relations. The proposal for a direct communications link between ASEAN Defence Ministers by 2015 to handle crisis situations, in particular for maritime security, therefore presents a timely opportunity to include cyber-related emergency situations.

Caitriona H Heinl is a Research Fellow with the Centre for Excellence in National Security, a component of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.

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