Cyber conflicts and Singapore's 'Total Defence' strategy

Raska, Michael

2016

Raska, M. (2016). Cyber conflicts and Singapore's 'Total Defence' strategy. (RSIS Commentaries, No. 156). RSIS Commentaries. Singapore: Nanyang Technological University.

https://hdl.handle.net/10356/81437

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 156 – 23 June 2016

Cyber Conflicts and Singapore's 'Total Defence' Strategy

By Michael Raska

Synopsis

The progressive complexity of cyber-enabled conflicts are likely to challenge Singapore's traditional conceptions of 'Total Defence' strategy.

Commentary

FOR MORE than 30 years, the principal strategy underlying Singapore's security has been embedded in the concept of "Total Defence" – a form of national security strategy aimed at strengthening and mobilising resources in five mutually-supportive defence domains: military, civil, economic, social, and psychological. Singapore has applied its 'Total Defence' to an array of potential security predicaments, as a comprehensive defence framework amplifying resilience in both civil and military domains.

However, as conflicts transcend into the cyber and information domains, the centres of gravity – the sources of state power that provide moral or physical strength, freedom of action, or will to act - are going to shift. The principal challenge for Singapore's Total Defence strategy is identifying these shifts, while managing, and responding to potentially more severe, cascading, multi-level crises – whether internal or external – emanating from cyber space.

Changing Character of Cyber Conflicts

Indeed, in every major security issue facing Singapore today and even more in the future, cyber-enabled threats have an extensive footprint.

Cyber conflicts transcend the cyber domain. Cyber conflicts are embedded in the

broader context of information conflicts – political, economic, information, technological, media, and ideological struggles for influence in which information may simultaneously serve as a target and weapon. In doing so, cyber-enabled conflicts are increasingly challenging traditional boundaries between peacetime and wartime, geography and distance, state and non-state actors, civil and military domains.

These cross-domain civil-military interactions therefore provide a new arena for strategic competition, which increases uncertainty, and enables new forms of conflicts other than war.

As Singapore is preparing its first comprehensive cyber strategy, while allocating substantial resources to strengthen cyber security, national resiliency, Singapore's leaders must be clear about their long-term national cyber priorities. In particular, they must define what constitutes Singapore's cyber power in relation to its means, national security aims and objectives.

Implications on 'Total Defence'

Singapore's Total Defence envisions mobilisation of population and resources to strengthen the readiness, resolve, and resilience of every sector of society as well as government departments - each playing a role in ensuring Singapore's security against all forms of security challenges.

The progressive complexity of cyber-enabled conflicts, however, challenges each pillar of Singapore's 'Total Defence' simultaneously, while increasing the risks and costs of potential failure.

(1) Cyber-enabled conflicts may challenge *Psychological Defence* or the collective will and commitment among Singapore's citizens to defend the country. Singapore's multi-cultural society is increasingly affected by global information conflicts through social media. Social media campaigns may target national will, regional or group audiences to gain support and weaken opposition, to individual targets to enhance particular narrative at a local level.

(2) In cyber-enabled conflicts, the main battlefield is consciousness, perception, and strategic calculus of the targeted adversary. As such, a false picture of reality may threaten through the manipulation of the information sphere. It may also threaten the mutual co-existence, cohesion, and harmony based on multicultural consensus and community-building regardless of race, language and religion – *Social Defence*.

(3) Cyber-enabled conflicts increasingly target processes controlling critical information infrastructure – strategic industries such as energy, transportation, communications, water distribution, and others. An advanced persistent cyber-attack may disrupt, deny, destroy, or subvert these critical systems, which provide distribution of essential items and resources such as food, water, fuel, and in doing so, undermine the foundations of the *Civil Defence*.

(4) *Economic Defence* has both strategic and operational significance for Singapore: on one hand, it refers to the contingency planning for the conversion of civilian

human resources, technological skills, and capital investments for the military during wartime. At the same time, it also recognises that military power depends on economic strength.

In the absence of a strong economy, the costs of creating and maintaining an effective military capability would be too high. In cyber-enabled conflicts, cyber criminals may seek to attack Singapore's financial system primarily for monetary gain, using relatively low-cost means but sufficient subject-matter knowledge. At the same time, there are substantial risks of various economic cyber-espionage.

(5) Ultimately, computer network operations in the military domain may challenge Singapore's *Military Defence*, undermining the operational readiness of the SAF as well as indigenous defence industrial base that meets the SAF's military-technological requirements. For example, cyber-enabled attacks that may disrupt, deny, degrade SAF's situational awareness - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

Rethinking Strategy

The key question for Singapore's Total Defence is this: should Cyber Defence become a separate pillar in the strategy or serve as an integrated part in each of the existing domains?

For example, in the military domain, the SAF is currently studying cyber as a new domain of warfare together with its strategic and operational ramifications in the context of the Fourth-Generation SAF 2030 Force. In the process, the SAF is likely to conceptualise both offensive and defensive components of cyber power and its utility in achieving strategic and political outcomes. In this context, should the SAF be tasked to defend Singapore's strategic industries from advanced persistent cyber-threats?

Notwithstanding the seemingly symbiotic relationship between Singapore's defence spending, economic development, educational system, civil service, media information sphere and the public in tackling emerging cyber threats, the Singapore government must continue to revamp its interagency policy processes, while encouraging a broader understanding of cyber-enabled conflicts, including debates on future cyber threats that might differ from what is seen today.

Ultimately, government agencies, academia and think tanks, and the private sector must work together to facilitate strategic and operational adaptability that leads to innovative concepts, technologies, and organisations in tackling existing and more importantly, future cyber threats.

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