S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 95/2011 dated 28 June 2011

Framing Cyber Warfare: Between Offence and Defence

By Alan Chong and Nah Liang Tuang

Synopsis

The increasing frequency of cyber attacks purportedly mounted by state and non-state actors is causing worry worldwide. However policymakers need to steer carefully between their offensive and defensive dimensions in discussing options for cyber defence.

Commentary

THE RECENT reported hacking into Google's Gmail accounts in China purportedly by actors with links to the Chinese authorities through a dedicated Cyber Warfare unit are – if proved true - worrying developments for international IT security. The US administration has suggested that the alleged Chinese-sponsored infiltration into Google's Gmail database might constitute an act of war requiring military action. Such a reaction, however, may be disproportionate considering that it was unclear if the hackers had provable links to the Chinese government. Nonetheless, the uproar highlights the growing possibility of a slide towards Cyber Warfare conflicts.

Cyber Warfare (CW) can include operations conducted in cyberspace to attack an adversary's critical Information Technology (IT) infrastructure. The goal would be to disrupt military command and control systems, sabotage operations and logistics networks, cripple corporate IT services and remotely steal sensitive data. This could involve online infiltration of the target's information systems via hacking attacks, the planting of computer viruses into the systems' networks and co-ordinated attempts to overwhelm enemy servers via denial of service attacks.

Clarifying the Threat

As successful CW operations could cripple military operational readiness and result in severe economic disruption, the importance of CW defence for holistic national security cannot be gainsaid. However, it is often difficult to distinguish between corporate and juvenile mischief on the one hand, and an outright act of war on the other. An act of war requires the clear identification of a source. Consequently, the victim has to politically determine that a cyber attack would be crippling to its national life to the extent that it constitutes paralysis on a nation-wide scale of the order of the World War II attack on Pearl Harbour.

In 2007, Estonia suffered a massive cyber attack which was ostensibly routed through a number of servers based in Russia. While this attack coincided with offline tensions between ethnic Russians and Estonians, it could not be conclusively proven that the Russian government was behind it. More recently Malaysian government portals were hit in mid-June 2011 by an unknown group named Anonymous. And serial attacks

were mounted against corporations such as Sony and Nintendo, as well as at the International Monetary Fund. Do these attacks on non-state actors and intergovernmental organisations amount to acts of 'war'?

Offence, Conquest and Fending Off Intrusions

Most defence industry professionals and government experts suggest that militaries should invest in cyber defences simply because the Internet generates cyberspace as a fourth dimension of war. However, "cyber warfare" is rooted in old fashioned thinking. The Internet invites interdependence upon common software frames and its derivatives. Consider how Internet Explorer and Java programmes work with APPLE and Microsoft operating systems while Google search engines work in tandem with myriad book publishers and information agencies.

The Internet works for anyone who travels the information superhighway only if the 'vendors' of various services online collaborate and accept niche dominance in certain services. Indeed, the vast majority of the world's corporations rely on software compatibility over the Internet so that virtual meetings can be conducted and work allocation efficiently coordinated. Accordingly an expert like Martin Libicki rightly claims that friendly 'conquests' of cyberspace have occurred through firms that have spearheaded software enhancements to the Internet or to services offered online.

These conquests are not territorial but are virtual conquering of Internet space akin to the capturing of uncontested market share. When these services appear online, they advertise themselves to attract clients and in turn, their competitors desire to learn, or steal, the secrets of their success.

Institutionalising Cyber Warfare 'Defence'?

Therefore, one cannot speak of CW preparedness in the way one might seek to counter the latest conventional weapons. Defence in CW means fending off intrusions through vigilance in monitoring traffic and intent. One might even consider 'cyberdeterrence' a possibility. But it is one that is supported by law enforcement agencies skilled in electronic monitoring and coordinating prosecution of cyber malefactors through international collaboration. Interpol can be involved in these efforts because a crime online can be legislated to be a crime offline.

Aside from litigable cases, there are many intrusions that are mounted for vanity and thrill-seeking reasons. Finally, if one considers deterring state-sponsored cyber attacks, then the usual threats of suspending international online commerce apply. Interestingly, both China and Iran have insulated parts of their information infrastructure from the World Wide Web as a form of prophylactic.

Can Singapore afford to follow the containment approach to sanitising national virtual space? The answer is no. It has a globalised economy that relies on the Internet to augment its maritime and aviation connections, ports, airports and border checkpoints. Despite the fact that Singapore does not have overt state enemies and has not suffered any serious CW attacks to its critical infrastructure, its corporate IT infrastructure has experienced significant attacks over the past three years. A 2010 Symantec State of Enterprise Security Study reported that 67% of companies in Singapore have been subjected to cyberattacks between 2009 and 2010. It noted that the top three attacks featured theft of intellectual property (100 per cent), work environment downtime (67 per cent) and theft of other corporate data (33 per cent).

Respond and Recover

Hence, a clear case can be made for the institutionalisation and development of strong Cyber Warfare defence capability. The Singapore Infocomm Technology Security Agency (SITSA) is working with private sector professionals to foster a 'respond and recover' culture among companies and other vulnerable agencies.

Such an approach, while low-keyed, assures the global business community that cyber defence here is being treated with a clinical approach without going to the extreme of threatening forceful retaliation. The point is to practise vigilance, early detection, and round-the-clock monitoring, which is what cyber protection is all about. It supplements the protection of critical civil infrastructure functions like power and water supply, telecommunications, e-banking, the Monetary Authority of Singapore and the Singapore Stock Exchange.

'Respond and recover' is not just a mantra for an Internet-reliant nation-state. It is also about clarifying the principles of framing cyber warfare without venturing into the military template of offence and defence.

Alan Chong is an Associate Professor of International Relations at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. Nah Liang Tuang is an Associate Research Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.