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

RSIS COMMENTARIES

"Cyber War" in the 21st Century: The Emerging Security Challenge

Commodore (retd) Ashok Sawhney

18 February 2010

The recent "Google spat" between China and the United States has brought to fore the possibilities of subverting the 'cyber commons'. Cyber attacks have the possibility of unleashing great havoc on the very functioning of a networked, modern state.

Extent of the Problem

THE RECENT unexpected blow-up between the United States and China over Google's accusation of Chinese hacking into its sites for what Google deems as clandestine purposes has exposed a new but larger security challenge.

Many critical infrastructures in most countries have been built for reliability and round-the-clock operation, but not for security. They have had little or no cyber protection as the traditional concept revolved around physical security. Today however, infrastructure is interconnected with computer networks, accessible from anywhere in the world. It is, therefore, imperative that critical infrastructure like power, water, and essential services like hospitals, transportation and communication, prepare for the havoc that cyber attacks can cause. Even militarily, a war could be won or lost without a shot being fired. However, cyber-war must not be confused with cyber-crime, which is also prevalent and growing, but for purely monetary gains.

Evolution of Cyber War

Nation states or non-state actors who have chosen the asymmetric warfare route to bridge the technology/capability gap find 'cyber war' tools effective. Cyber-space research and monitoring companies have detected efforts from at least 15 countries -- including China, Russia, Taiwan and the United States -- trying to get inside industrial control systems clandestinely. However, having pin-

pointed the country of origin, it was almost impossible to determine whether the exact source was a military organisation, an intelligence agency, terrorist group, criminal or an individual.

Cyber attacks, as a prelude to confrontation between nations, first emerged in the Russia-Estonia conflict of 2007, when the computer screens of Estonians trying to do business with their government online were frozen. In 2008, when Russia invaded Georgia, the cyber attacks grew more widespread and the Georgian government had to move its online activity to servers in Ukraine. More recently, in December 2009, South Korea reported an attack in which North Korean hackers may have stolen secret defence plans, outlining the South Korean and US strategy in the event of war on the Korean peninsula.

The US is a leading source of "hacktivists", who use digital tools to attack government websites, computer systems and censoring tools in Iran and China. These efforts are known to be supported by US foundations, universities and even the federal government. The Bush administration had reportedly used cyber attacks on insurgent cell phones and computers in Iraq, and on computers related to Iran's nuclear weapons programme. In other words, the same tools are being used today to serve different ends, ranging from stealing intellectual property, fighting for and against democracy, to controlling nuclear proliferation.

The Dilemma and Possible Solutions

The cyber arms race is ongoing. It has been determined that it is simply not enough to build defensive systems to restrict access to computers. "Mutually Assured Destruction" deterrence lessons from the Cold War are not applicable, since it is almost impossible to determine the identity of the attacker in the case of a cyber attack. This has led to the pre-emption doctrine, which advocates going into foreign computers to destroy malicious software before it can do any harm. However, this would amount to an act of war, and since each nation is today as much, if not more, dependent on the cyber domain as any other, it would also suffer damage in a counterattack.

Solutions to overcome the 'cyber war' threat are necessary at the national as well as the international level. Some of the possible solutions at the national level would be greater security consciousness of all users; putting organisational structures in place to overcome lapses; and regulatory frameworks by governments, which tend to vary. India, China and Germany are reported to have the highest levels of regulation, while the US has the lowest. Critical systems should be stand-alone, as far as possible, and not linked to the Internet.

A comprehensive approach involving all sectors -- government, industry, business and academia -- is essential. In addition, because of the widespread use of personal computers and the Internet, active participation of the cyber citizenry as a whole is necessary. The importance of adequate budgetary allocation is highlighted by the fact that banks and financial institutions have fallen shy of implementing the necessary stricter security measures due to cost constraints. Since cyber space has no boundaries, international cooperation is essential. However, this presents severe challenges.

Everyone talks of creating norms of network behaviour between states. There has also been talk of 'international laws specific to cyber security' as also 'rules for cyber engagement'. But before all this can be attempted in a meaningful manner, governments need to bring cyber activities, normally clouded in secrecy, out in the open for a debate leading to innovative solutions. The International Institute for Strategic Studies, in its annual report for 2010, highlights the problem: "Despite evidence of cyber attacks in recent political conflicts, there is little appreciation internationally of how to assess cyber-conflict. We are now, in relation to the problem of cyber-warfare, at the same stage of intellectual development as we were in the 1950s in relation to possible nuclear war."

Urgent International Cooperation Needed

The modern, inter-connected world, created in large measure by gainful utilisation of the ‘cyber commons’, is under threat due to dubious utilisation of the same commons by some. It is essential to not only overcome this threat by taking security measures at the national level, but to also find innovative means through international cooperation. This is probably even more essential than safeguarding the nuclear threat, as the trigger for a cyber war is not only held by responsible nation states, but also by individuals who could be terrorists or just irresponsible teenagers. It would be better to act now towards international cooperation through transparency, rather than waiting for a major disaster.

Commodore Ashok Sawhney (retd) is Visiting Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. He retired from the Indian Navy in December 2008. He has served as Director Naval Operations, Naval Attache in Washington DC and in command of Indian naval ships Rajput, Hosdurg and Vijaydurg.