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

RSIS COMMENTARIES

No. 138/2012 dated 30 July 2012

Negotiating the World's Cyber Frontier

By Benjamin Ho and Jennifer Yang Hui

Synopsis

The increasingly networked nature of the world has given rise to concerns over the use of cyberspace for global conflict. More and more countries are shoring up their cyber defenses against would-be aggressors. But with modern international relations largely defined by Westphalian rules of engagement, negotiating cyber frontiers will prove challenging.

Commentary

IN THE PAST MONTH security experts have uncovered the existence of a Mahdi trojan, a new Persian-language cyber spy network targeting Iran and diplomatic missions of several Middle Eastern nations. The campaign, which is believed to have started some eight months ago allow remote attackers to steal files from infected PCs, monitor emails and record key strokes, among others.

This latest discovery comes on the heels of an attack on Iranian network infrastructure in May by a computer virus known as Flame, a similar software said to be 20 to 40 times more powerful than Stuxnet, a worm which infiltrated Iranian uranium infrastructure in 2010. Notwithstanding Tehran's charge that these attacks were the work of US and Israeli spy agencies, both countries have not publicly admitted responsibility for these actions.

With the multiplication of computer viruses that could reach transnational targets, governments have begun to ponder the feasibility of moving the governance of the cyberspace to a post-Westphalian model. Named after the Treaty of Westphalia that was signed in 1648, the existing system has guaranteed the principle of the sovereignty of states and the fundamental right of political self-determination, the principle of legal equality between states as well as the principle of non-intervention of one state in the internal affairs of another state. Moving forward, this may not be tenable.

Whither the 'Nation State'?

One of the key challenges in cyberspace today is the problem of attribution. The nature of cyber attacks and cyberinfrastructure often spans several political jurisdictions, making it difficult to accurately pinpoint the national identity of a hostile agent. The multiple denial-of-service attacks carried out against Estonia in April and May 2007 highlighted the complicated nature of cyber warfare and the ambiguity surrounding international regulation.

Unlike armed conflict which is covered under the United Nations Charter (UNC) and customary international law, there is at present no clear or comprehensive framework within which states are able to shape policy responses to the threat of hostile cyber operations. The emphasis on preserving the state's territorial integrity means that anything other than an armed attack is not expressly prohibited by international law.

The conduct of war in an age of cyberspace can be equally problematic. The provisions of the Geneva Convention necessitate a distinction between combatants and noncombatants in a battle. With cyberspace, however, this distinction becomes increasingly blurred. As Sun Tzu pointed out, the adept in warfare are able to subdue the army of the enemy without having resort to battles. In this respect, the ability to strike at the plans and strategies of the enemy, without attacking his cities is viewed as the supreme objective in war. Accordingly cyberspace opens up an entirely new battlefield as far as national security is concerned. The offensive player is now able to utilize greater means by which to wage war against his enemy. These include: intelligence gathering (open source or signals), information piracy, superimposition fraud, and perception management (sometimes known as psychological operations).

Furthermore, the increasing interconnectedness of information systems vital to a country's critical infrastructure and the dual usage of such systems render discrimination far more complex in cyberspace than physical space. It may be extremely difficult to distinguish, for instance, the code in a computer that governs delivery of power to an early warning radar system (which may be a lawful target of a cyber attack) from the code that controls power to a hospital's intensive care unit. The risk of unintended consequences and the possibility of collateral damage further complicate the targeting picture.

The Human Factor

While the Stuxnet attack demonstrated the possibility of remote control of a nation's technological apparatus, this capacity would not have been possible without the meticulous reconnaissance of Iranian physical and technological architecture. According to a Stuxnet dossier released by Symantec, the attackers, among others, would have to (i) gain access to the schematics of the industrial control systems (ICS); (ii) set up a mirrored environment that include the necessary ICS hardware; (iii) obtain the digital certificates to avoid detection; and finally, (iv) introduce Stuxnet into the target environment, most likely by removable drive. All these suggest that substantial human effort is required.

Cyberspace has allowed the human factor to be amplified many times; a security breach from a single employee can potentially affect the entire system. Ironically, this results in a situation where a technologically advanced country has more to lose than a less endowed adversary. Existing vulnerabilities become more pronounced and state secrets can be easily broken as a result of individual negligence. Indeed, the usual categories related to national security - imposed by the Westphalian markers of geography and territory – becomes less salient in an age of cyberspace as state borders become increasingly porous.

Commanding Cyberspace

In July 2011, the US Department of Defense announced that it was developing strategies for operating in cyberspace, thus highlighting the importance of cyberspace as an operational domain in matters of national security. Other technologically advanced countries such as South Korea, the United Kingdom and Singapore have all invested substantial efforts in boosting their cyberspace capabilities.

Indeed, the past two decades have witnessed the unprecedented – and ubiquitous - influence of cyberspace on political and diplomatic affairs. From the development of net-centric concepts and defense transformation in the military to the use of technology in myriad facets of national policy (counterterrorism, financial systems, provision of energy), cyberspace has become an indispensable medium for achieving national objectives. The future will witness a more challenging cyber-environment for states to operate within; rethinking Westphalian norms of command and control is urgently needed.

Benjamin Ho Tze Ern is an Associate Research Fellow in the Centre for Multilateralism Studies and Jennifer Yang Hui is an Associate Research Fellow in the Centre of Excellence for National Security, both at the S. Rajaratnam School of International Studies (RSIS).