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

RSIS COMMENTARIES

No. 060/2014 dated 1 April 2014

Cybered Conflict, Not Cyber War

By Peter Dombrowski

Synopsis

We have entered a period of cybered conflict. For militaries, governments and private firms mastering the demands of cybered conflict, it will be a long and painful process requiring strong cyber defences and organisational resilience.

Commentary

CYBER WAR is not coming, but cybered conflict is. For decades we have been warned of the possibility of digital Pearl Harbours where network attacks lead to cascading failures of critical military, public and private systems. Recently, there has been a backlash; contrarians now argue that cyber war not only hasn't occurred but is highly unlikely. They point to the absence of cyber "battle deaths" to date and the immense difficulty of using cyber weapons for political and military purposes.

Botnets and malware can disrupt service and lead to lost data, but these are expensive nuisances rather than acts of war. Truly dangerous attacks, targeting, for example, the supervisory control and data acquisition (SCADA) systems of military facilities or public utilities, while potentially destructive, require exquisite intelligence and dedicated teams of hackers. These are capacities beyond the means of most nation-states, much less terrorists or common criminals.

What's going on?

Yet worrying about cyber war and arguing about whether it can occur or not misses something important about the contemporary security environment much less the future. Communications and computer networks remain vulnerable. If we are not at war, therefore, what is going on?

We have entered a period of cybered conflict. Cybered conflict means simply that all adversarial and competitive relationships will have a cyberised dimension. Insofar as all modern systems from finance to transport require telecommunications and computers connected to the Internet or proprietary networks, adversaries of all sorts will seek to influence outcomes by accessing and altering both the systems themselves and the data that resides within.

For militaries, boots on the ground and ordinance on targets may be the ultimate determinants of victory but to deploying soldiers in the field or launching missiles on now requires the secure, accurate, and timely flow of information.

For most institutions, including nation-states, developing cyber defences and resiliency are key. With all the attention paid to high profile attacks like Stuxnet, it is sometimes difficult to remember that the most effort – in terms of time, manpower, technology and money – is put into developing defensive systems. Firewalls, anti-virus programs, cryptographic techniques and the like play important roles in maintaining functionality. Even more important, governments and firms are developing the training, tactics, and procedures necessary to protect data, software, and hardware. More needs to done and investments to date are inadequate, but progress is being made.

Defences of course are not enough. Given the stakes involved and motivations of hackers, it is inevitable that new malware will be developed, and internal threats from formerly trusted agents will emerge. But when telecommunications and computing systems are inevitably damaged they must be able to recover quickly; this might mean building in redundancy and avoiding single points of failure, but it also means having talented, well-trained personnel capable of responding quickly to repair, restore and rebuild.

The big picture

Beyond the importance of cyber defence and resilience, two big trends are emerging from this era of cybered conflict. Firstly, we are experiencing what Chris Demchak and I call the "Cyber Westphalia," that is, the reassertion of the nation-state into the ungoverned domain of cyberspace. States are slowly but surely dividing up cyberspace into national jurisdictions while establishing enforcement capabilities, such as the emergence of cyber commands, national and subnational computer emergency response teams (CERTS), domestic legislation codifying organisational responsibilities, and interstate bargaining over the future of global cyber governance.

Secondly, there are signs that the aerospace and defence sector is evolving into what might be called a cyber-military complex. When we think about war and preparations for war, we often think about the industrial giants that have traditionally supplied everything from tanks to ships to fighter aircraft: Lockheed Martin, Boeing, BAE Systems, and Airbus Group. Increasingly, these firms are tailoring themselves to meet the demands of defensive – and in some cases, offensive – cyber operations.

Yet, preparing for cybered conflicts demands a different set of industrial capabilities than preparing for traditional warfare. Of course, the old giants will play a role. Too much money is at stake and the old ways of doing business are too hard to break. Indeed, many companies in the aerospace and defence sector have created cyber divisions, advertise specialised cyber services, and have added the prefix "cyber" to many existing programs and products. But other, more non-traditional suppliers will also provide many of the technologies for militaries, government agencies, and private firms to cope with cybered conflicts.

In particular, firms in the information technology and communications sector are paying attention to government customers in ways not seen since the beginning of the information age. While at one time, many Silicon Valley firms were loathe to work closely with the government, more recently this is not the case. Of course, this attention is not an unalloyed good. Abuses have and will occur and the long-term implications for international competitiveness of firms closely associated with governments are uncertain.

But again Google, Huawei, and other telecommunications and computing conglomerates are working with government to provide the hardware, software, and services necessary to assert greater control over cyberspace. Further, highly specialised cyber security firms have become critical – not just for protecting home computers but also for providing network intelligence, digital forensics, and many other professional services.

Turbulent future

While in most countries defence and intelligence budgets are declining or stabilising, spending on cyber security remains a growth area. In the United States, for example, President Obama's 2015 budget includes roughly US$13 billion to improve cyber security and to mitigate network threats. Defence spending on cyber operations is projected to increase 21 percent over 2013 to $4.7 billion.

Even in a period of global austerity, other governments are increasing spending on cyber capabilities as well. If we add in spending on cyber security by private firms from banks to airlines and public utilities, investment analysts are positively bullish on any firms connected with the sector.

Mastering cybered conflict will be a long and likely painful process. Technologies evolve rapidly; developing defensive and resilient institutions remains a game of catch up. States will try to regulate and govern but will often fail or get things wrong. Gains to be made from cyber exploits – whether stealing intellectual property or disabling military equipment used for in a shooting war or deceiving publics with misinformation transmitted over social media – are simply too great for ambitious generals, corporate buccaneers, and criminals to resist.

Peter Dombrowski, a professor in Strategic Research at the US Naval War College, was until recently a Visiting Research Fellow with the Military Transformations Programme, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. This commentary draws from an earlier article he co-authored with Chris Demchak in the Naval War College Review*.*