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

RSIS COMMENTARIES

No. 024/2014 dated 5 February 2014

Enhancing Cybersecurity: Improving Technical and Analytical Expertise

By Damien D. Cheong

Synopsis

Singapore's recent initiatives to increase cybersecurity expertise through specialist training and education are timely and necessary. In addition to enhancing such skills, the strategic analytical skills of existing and potential cybersecurity practitioners must be honed as well.

Commentary

IT WAS reported in The Straits Times last year that Singapore, like many other countries such as the United States, United Kingdom and India, was experiencing a shortfall in the number of cybersecurity practitioners. Furthermore, graduates did not seem attracted to the IT security profession, which meant that the next generation of cybersecurity practitioners would be negatively impacted.

Expectedly, these trends are a cause for concern in light of the persistent and ever-increasing cyber threats facing the country. The government has embarked upon two major initiatives to address these issues.

Role of Strategic Analysis

Firstly, it has increased the number of scholarships for infocom security studies through the Infocom Development Authority (IDA). Secondly, it has announced two different training initiatives for potential and existing cybersecurity practitioners: (a) KPMG's Cyber Security Centre in collaboration with Singapore Polytechnic will conduct cybersecurity courses for 10 to 15 participants annually; (b) FireEye, a security company specialising in advanced cyber threat detection, will train existing cybersecurity practitioners to hone their skills in detection analytics, identification and monitoring of emerging threats as well as undertaking "defensive action".

These initiatives are both timely and necessary. In addition, they will need to be complemented with a corresponding increase in strategic analytical training. This is envisaged to significantly improve the quality of analytical products as better strategic insights can be generated.

The major challenge of data analysis in the "era of Big Data" is well-known; it is both time-consuming and involves a lot of manpower to make sense of it all. Even if technological advancements help minimise the time taken to filter useful data from non-useful data, the resultant data still lacks strategic insights. As a result, the value of the analytical product to decision-makers is somewhat reduced.

Enter the strategic analyst. His/her job, effectively, is to analyse data and convert it into useful information. This, according to Thomas Fingar, former chairman of the National Intelligence Council, is accomplished by "providing insight on trends". Such insight adds value to the information, and allows the decision-maker to "broaden the range of possible futures and thus better manage uncertainty".

Hence, effective data collection and functional analysis, while a major part of cybersecurity expertise, must be buttressed with "strategic analysis of threats and threat indicators".

Strategic analysis, according to the Software Engineering Institute (SEI) at the Carnegie Mellon University, "adds perspective, context, and depth to functional analysis, and incorporates modus operandi and trends to provide the 'who' and 'why' of cyber threats. It is ultimately rooted in technical data, but incorporates information outside traditional technical feeds – including internal resources such as physical security, business intelligence, and insider threat, and external feeds covering global cyber threat trends, geopolitical issues, and social networking.

The resulting strategic analysis can populate threat actor profiles, provide global situational awareness, and inform stakeholders of the strategic implications cyber threats pose to organisations, industries, economies, and countries".

Improving strategic analytical capabilities

Researchers at the SEI have proposed several measures to improve strategic analytical capabilities in their report Intelligence Analysis for Internet Security. These include:

Overall Threat Assessments: Pertains to the "analysis of vulnerabilities of critical missions (including levels of dependence), the kind of disruption and damage that could be caused to the implementation of these missions, the kinds of weapons/instruments that could be used to cause such disruptions and the likelihood of such attacks and intrusions taking place".

Sector Threat Assessments: Focuses on "vulnerabilities and threats either in particular areas such as national infrastructure, or in particular sectors of the economy such as banking or e-commerce…In effect, a strategic analysis of this kind has to take account of changes in what can be a very dynamic environment".

Trend Analysis: Relates to analysing "changing threats and vulnerabilities. These might include base-line assessments so as to better recognise departures from the baseline. Alternatively, they might focus on future threats and vulnerabilities in an effort to determine in what ways the problem is evolving – and what can be done to anticipate and contain future challenges. Trend analysis is likely to be most effective when it is linked with careful attention to drivers such as key trends in the political, economic, social and technological sectors that will shape the future threat and vulnerability environment of the future".

Potential Damage Assessments: Assesses the "potential cascade effects of intrusions. This would offer opportunities to develop both defensive and mitigation strategies. Crisis management, contingency planning, mitigation strategies, and disaster management would all be enhanced by strategic analysis of potential damage assessment. Indeed, the capacity for effective and rapid reconstitution might depend on such analysis".

Categorising and Differentiating Attacks and Attackers: Differentiating between intrusions/threats from various sources is critical. "This will be especially true as groups or individuals develop intrusion strategies that mimic other forms and thereby lessen their chances of identification or, in the case of nation states, provide plausible deniability of their actions. Also, by doing so, appropriate responses that might go beyond simply defensive or mitigation strategies can be determined".

Identification of Anomalies: This refers to detecting "anomalies that provide indicators of emerging threats and problems". Anomalies in this context can be understood as developments or events that do not fit typical or known patterns. The detection of anomalies or novel patterns can be a major element in anticipating new methods of intrusion, new targets, or even new classes of intruders. "It is a macro-level task that requires careful and systematic 'environmental scanning' as well as the coalescing of tactical and operational intelligence reports that identify and highlight specific aberrations from the norm".

Analysis of Future Net Environments: This provides "assessments of potential future environments on the Internet and the potential impact of malicious activity within those environments".

Some of these measures will most likely be taught in the new IT security courses. Nevertheless, it may be useful for public as well as private organisations to audit current capabilities to determine if their strategic

analytical expertise requires enhancement. In light of the inadequate regulatory/legal frameworks at the international level to deal with cyber threats, defence, through improving a country's cybersecurity capabilities, is the best approach to cyber threats at present.

Damien D. Cheong is a Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.