RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 166 – 11 October 2018

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the author(s) and RSIS. Please email to Mr Yang Razali Kassim, Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Evolving Nature of Cyber Conflict

By Eugene EG Tan

Synopsis

The understanding of the nature of cyber conflict is evolving and expanding, even as Singapore recognises the threat of deliberate online falsehoods. States need to develop holistic responses to keep up with these changes, and to protect the resilience of their systems and society.

Commentary

FOR DECADES cyber conflict has been understood by western governments, practitioners and scholars, to include protection of critical infrastructure and computer networks from breaches of confidentiality, integrity, and availability – otherwise known as 'hacking'. This understanding has been the basis of international discussions on the applicability of international law to cyber conflict, cyber norms of behaviour, and deterrence of cyberattacks. The focus has been on the technology – networks, hardware and software – instead of on the information carried by the technology.

There is however an alternative view, led by Russia and China, that traditionally has seen information as an inalienable part of cyber conflict. Russia introduced a draft resolution on information security in the First Committee of the United Nations General Assembly 20 years ago in 1998, and has continued to press for information security to be part of the international conversation on cyber conflict, including submitting a letter in January 2015 (together with China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan) to the UN calling for an international code of conduct for information security.

Focus on Technology

While the letter was noted by the 2015 UN Group of Governmental Experts (UNGGE), the recommendations proposed by the group squarely focused on the protection on critical information and communications technology (ICT) infrastructure, which was reflected in the norms proposed in the consensus report.

One reason for this focus on technology instead of information has been the philosophy of many western democracies that any controls over the flow of information would infringe the fundamental right to freedom of expression. Incidentally, respect for the freedom of expression, right to privacy, and other human rights was one of the norms proposed by the 2015 UNGGE.

This position appears to have shifted ever since the alleged Russian interference in the US presidential Elections in 2016. At various international conferences this year, including the landmark Conference on Cyber Conflict (CyCon) organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), keynote speeches addressed how the use of information operations through cyber means is now an important part of cyber conflict.

Keynotes at CyCon by Alex Stamos (then Chief Security officer of Facebook) and Camille Francoise (Principal Researcher at Google Jigsaw) highlighted how social media is used in state-sponsored information operations, citing numerous examples of how states have used tools to influence elections and promote questionable content to destabilise incumbent governments.

Protection For Social Media Platforms?

They also called for cooperation and a common approach to misinformation and manipulation of social media. This leads to the conclusion that social media platforms need protection as much as critical infrastructure like power plants and airports. However, including information operations in the discussion of cyber conflict is not straightforward, because the threats faced by social media platforms are different from those faced by traditional cyber targets.

First, in information operations, the networks of social media platforms are not being breached, but are being used for their built purpose: spreading information. The challenge is to curb the spread of misinformation without hindering freedom of expression.

Second, information operations are designed to exploit vulnerabilities not in the technology but in the society being targeted. Tackling them requires expertise in socio-political issues, psychology, communications, and other humanities.

Third, states can build resilience to cyberattacks through building strong technical defences and conducting exercises and drills. But resilience to information operations is built through institutional trust-building, media literacy education, independent fact-checking, and transparency in communication.

Fourth, while the international community has already found it difficult to develop international norms of behaviour in cyber operations, where those norms only considered technology, it will be even more complex if information is included in the discussion, because of different states' differing philosophies on the control of information versus freedom of expression.

Need for New Policies, New Organisations

Singapore has also recognised the national security threat that information operations, or deliberate online falsehoods, can pose to society. The Report of the Select Committee on Deliberate Online Falsehoods has provided 22 recommendations for responding to them. Many of the recommendations reflect the multi-faceted nature of information operations as explained in the foregoing paragraphs.

As the international community begins to recognise information operations as part of cyber conflict, states like Singapore will have to develop new policies and possibly even new organisations to respond to information operations alongside the more traditional cyber security challenges.

These new policies and organisations will need expertise in a range of areas such as public education, fact checking, and international relations. Cyber conflict will continue to evolve at a rapid rate, and states will need to produce timely and effective measures to prevent these conflicts.

Eugene EG Tan is Associate 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, Singapore.