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

RSIS COMMENTARIES

No. 114/2013 dated 21 June 2013

Tackling Cyber Threats: ASEAN Involvement in International Cooperation

By Caitríona H. Heinl

Synopsis

One of the primary challenges currently facing the international community is the recent marked increase in the role of state actors in the cyber domain. What is the state of ASEAN cooperation in tackling cross-border cyber threats?

Commentary

ASIA HAS become the locus of cyber conflict according to a 2013 Centre for Strategic and International Studies (CSIS) report. McAfee Labs *Threat Predictions Report for 2013* expects that states and armies will now increasingly become both more frequent sources as well as victims of cyber threats.

James Clapper, the United States Director of National Intelligence, also reports in the U.S Intelligence Community's *Worldwide Threat Assessment* of March 2013 that there has been a significant increase in state actors' use of cyber capabilities and this could possibly lead to an increase in the probabilities of miscalculations, misunderstandings, and unintended escalation. However, outside of a military conflict or crisis that threatens vital interests, he thinks it unlikely that other advanced cyber state actors will launch a "devastating attack".

Responsible state behaviour and international law

The CSIS report suggests that malicious activity in cyberspace, which could inflame existing tensions or increase misperception and miscalculation among governments of the intent and risk of cyber actions, poses the greatest cyber risk to security in Asia. Such activity includes "planning for military competition and asymmetric warfare, and engagement in economic espionage to gain long-term economic and trade advantages".

For instance, Australia, China, North Korea, India, Malaysia, Myanmar, Japan and South Korea are developing military cyber capabilities and doctrine, while Brunei and Singapore are developing defensive cyber capabilities, and capabilities of other Asian nations seem to range from "nominal to relatively sophisticated".

In this context, lack of international agreement on shared norms for responsible state behaviour and applicability of international law, plus the potential for mistake, raises probabilities of miscalculation and possibly conflict. Furthermore, there is no international or regional agreement on clear and harmonised definitions for

what constitutes “cybersecurity”, “cyber attack” or “cyber defence” - lines between cybercrime, cyber espionage and cyber attack are also ambiguous. According to the European Parliament Committee on Foreign Affairs Draft Report on Cybersecurity and Cyber Defence of 2012, even the very understanding of cybersecurity and other key terminology varies significantly between jurisdictions.

ASEAN and international cooperation

In light of these developments, and in addressing non-traditional security issues, the ASEAN Political-Security Community seeks to promote the renunciation of aggression and of the threat or use of force or other actions in any manner inconsistent with international law. Unlike nuclear weapons however, it is impossible to prevent the creation of advanced cyber capabilities and techniques.

Member States should therefore consider the feasibility of carving out a “no-use zone” by agreeing to not use advanced cyber capabilities in the region. Confidence building measures and preventive diplomacy such as exchanges among defence and military officials can also be enhanced to ensure escalation does not occur between ASEAN Member States or between ASEAN Member States and third countries. Such instruments should aim to prevent conflict and ensure that the chances of miscalculation and misinterpretation are reduced.

ASEAN should strengthen relations further with ASEAN Dialogue Partners and the international community by cooperating to tackle cross-border cyber challenges. It should also consider engaging other regional bodies and possibly establish joint working groups with the European Union and the East Asia Summit. A joint EU-US Working Group on Cybersecurity and Cybercrime was created in November 2010 and the European Parliament Committee on Foreign Affairs report of 2012 calls for accelerating cooperation and exchange of information on how to tackle cybersecurity issues with third countries, such as its proposals to engage BRICS.

Noticeably, the report does not mention ASEAN or the ASEAN Regional Forum. The 2013 Cybersecurity Strategy of the European Union does, however, outline the EU’s intention to seek closer cooperation with ASEAN in the future.

The Asia-Europe Meeting (ASEM), whose partners include the ASEAN Plus Three, 27 EU Member States and the European Commission, can also be engaged to explore these issues of common concern in an open and informal fashion in order to complement bilateral and multilateral cooperation efforts. Asian and European representatives can use this forum to discuss ways to enhance cooperation and host working groups to include the private sector and civil society.

Cooperation in tackling cross-border cyber threats should also be included within the ASEM 2012-2014 work programme and placed on the agenda of the 10th ASEM summit, which is due to be held in 2014.

Forging an ASEAN common position

Going forward, ASEAN Member States should agree a common position on shared norms for responsible state behaviour in cyberspace and the applicability of international law for the use of advanced cyber capabilities and techniques. For regional and international for a such as the coming G20 Summit in September 2013 and Seoul International Cyberspace Convention of October 2013, positions should be coordinated to promote ASEAN values and policies.

A common ASEAN position - or at a minimum, a common position paper - will reflect ASEAN’s views on what is emerging as a critical issue in international cooperation and international security.

Caitríona H. Heinl 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.