RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 236 – 26 November 2014

Securing ASEAN's Cyber Domain: Need for Partnership in Strategic Cybersecurity

By Elina Noor

Synopsis

The ASEAN region cannot afford a security lapse as the digital domain is supposed to propel its development. ASEAN should lead in forging partnership in strategic cybersecurity.

Commentary

THE NAYPYIDAW Declaration on the ASEAN Community's Post-2015 Vision positions ASEAN as a rules-based and resilient community that is capable of upholding its centrality in the evolving regional architecture. Equally, an integrated ASEAN in the years to come should preserve its continued relevance by contributing and responding to global issues of common concern.

Ensuring that the region remains free of weapons of mass destruction is one way of achieving this vision. So, too, is strengthening maritime security and cooperation. But where ASEAN can really start to make a difference - to be proactive - to lead in partnership and to boldly underscore its bearing, is in the emergent area of strategic cybersecurity.

Urgency to secure cyberspace

As a developing region, Southeast Asia has the most advanced implementation of harmonised e-commerce laws. Nine of the 10 ASEAN countries have laws related to electronic transactions, while eight have those concerned with cybercrime. All but one have a national cybersecurity programme. This is, perhaps, of little surprise, given that economic prosperity (and the regulatory framework to secure that) as the basis for peace and security has been an ASEAN priority from the beginning.

Since the World Trade Centre attacks in the United States, as well, issues of terrorism related to cyberspace and cybercrime have featured in numerous ASEAN declarations and communiques. This growing recognition of the urgency to secure cyberspace has permeated discussions in the ASEAN Regional Forum with tentative initiatives, such as a work plan aimed at promoting confidence-building measures.

Where discussion has lagged in the ASEAN framework has been how state interactions with each other and non-state actors should be governed in cyberspace. Specifically, and, rather shockingly, for a grouping of relatively and mostly small states with a constellation of powerful dialogue partners, there has been little consideration about the role and applicability of international law in the conduct of relations in the virtual realm.

Duality of cyberspace: civilian, military or both?

A region that aspires to connectivity must underwrite its own security. This goes beyond technical resilience — crucial in its own right — to a framing set of cross-border laws and principles that will guide state conduct online, as well as offline. A conversation about rules must be conducted by a community to be based on rules.

It is not just diplomats who should be talking, however. The duality of cyberspace means that the usual parameters that define civilian and military spaces are mutable. How should militaries in the region be guided in cyberspace, when infrastructure, network grids and software are shared with the civilian world? What rules of engagement apply if cyber or other operations are warranted?

Southeast Asia's militaries should also be talking with each other to clarify intentions, promote some predictability of conduct and advance interoperability in cyberspace. The ASEAN Defence Ministers Meeting (ADMM) does not yet discuss cybersecurity as a separate working group. It would do well to do so. It would do better to explore the matter with its dialogue partners, many of which have superior cyber technologies and much to share.

Even accounting for the inevitable natural security sensitivities in this new domain, there is plenty of scope at this stage for doctrinal development, technical exchanges and joint exercises. At the very least, militaries in the region should be establishing rules of engagement in cyberspace in accordance with prevailing international law.

Rising East, Shining West?

The irony is that even as the East is rising, the sun appears to be still shining in the West, at least in cyberspace. ASEAN cannot afford a security lag or lapse in this space, especially not when the digital domain — a recognised force leveller — is supposed to leapfrog the region's development.

To capitalise on technology, even the smallest and least developed member state must be an active and participatory stakeholder, if not in capability, then at least in voice.

As geopolitical dynamics evolve and states jostle with each other for power and dominance online, it will be absolutely in this region's interest to shape and advocate a cyber domain based on an international legal framework. As chair of ASEAN next year, Malaysia should lead this charge and set the tone for, and in line with, the the ASEAN Community's Post-2015 Vision.

Elina Noor is Assistant Director, Foreign Policy and Security Studies at the Institute of Strategic and International Studies (ISIS), Malaysia where this article was first published.

**See also article by RSIS Research Fellow Caitriona H Heinl on Regional Cybersecurity: Moving towards a resilient ASEAN cybersecurity regime in Asia Policy Number 18, July 2014, pages 131-159). http://nbr.org/publications/element.aspx?id=751 It describes the predominant cybersecurity issues confronting ASEAN and outlines policy options to create a more resilient cybersecurity regime across the region.*
