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

RSIS Working Paper

No. 263

Regional Cyber Security:
Moving Towards a Resilient ASEAN Cyber Security Regime

Caitríona H. Heinl

S. Rajaratnam School of International Studies
Singapore

09 September 2013

About RSIS

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous School within the Nanyang Technological University. Known earlier as the Institute of Defence and Strategic Studies when it was established in July 1996, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education with a strong practical emphasis,
- Conduct policy-relevant research in defence, national security, international relations, strategic studies and diplomacy,
- Foster a global network of like-minded professional schools.

GRADUATE EDUCATION IN INTERNATIONAL AFFAIRS

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science (M.Sc.) degree programmes in Strategic Studies, International Relations and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Thus far, students from more than 50 countries have successfully completed one of these programmes. In 2010, a Double Masters Programme with Warwick University was also launched, with students required to spend the first year at Warwick and the second year at RSIS.

A small but select Ph.D. programme caters to advanced students who are supervised by faculty members with matching interests.

RESEARCH

Research takes place within RSIS' six components: the Institute of Defence and Strategic Studies (IDSS, 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2004), the Centre of Excellence for National Security (CENS, 2006), the Centre for Non-Traditional Security Studies (Centre for NTS Studies, 2008); the Temasek Foundation Centre for Trade & Negotiations (TFCTN, 2008); and the Centre for Multilateralism Studies (CMS, 2011). The focus of research is on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region.

The school has four professorships that bring distinguished scholars and practitioners to teach and to conduct research at the school. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, the NTUC Professorship in International Economic Relations and the Bakrie Professorship in Southeast Asia Policy.

INTERNATIONAL COLLABORATION

Collaboration with other professional schools of international affairs to form a global network of excellence is a RSIS priority. RSIS maintains links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

ABSTRACT

This paper outlines regional level cooperation efforts of the Association for Southeast Asian Nations (ASEAN) to counter serious cross-border cyber threats and identifies where gaps might exist, which require further and urgent consideration. It considers whether more might be done to create a comprehensive approach to cyber security in the ASEAN region. Finally, it aims to fill identified gaps by providing several recommendations for possible future development and implementation to create a resilient regional cyber security regime.

****

Caitríona H. Heinl is a Research Fellow at the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). She is responsible for research related to the CENS Homeland Defence Programme, primarily with regard to issues pertaining to cyber security.

She is a UK trained Solicitor (non-practising) and admitted as an Attorney-at-Law in New York. She holds an M.Phil in International Relations from the University of Cambridge.

Prior to joining CENS, Caitríona was the lead researcher responsible for Justice and Home Affairs policy and the Justice Steering Committee at the Institute of International and European Affairs (IIEA), Ireland.

Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime

I. Introduction

Cyber threats are causing increasingly serious risks to the economy as well as to national and international security. They are now widely accepted in the international community as a top-tier risk, if not the most pertinent risk, to national and international security. The EU considers cyber threats as a major risk to the security, stability and competitiveness of its Member States and the private sector,[1] while the United States Intelligence Community's *Worldwide Threat Assessment* for 2013 ranks cyber threats first ahead of terrorism, transnational organised crime, weapons of mass destruction proliferation, counter-intelligence, counter-space, natural resources insecurity and competition, health and pandemic threats and mass atrocities.[2] Furthermore, it should be noted that, for the first time since the 11 September 2001 attacks, international terrorism does not rank first in the U.S. Intelligence Community's assessment of global threats to national security.[3]

A number of international and regional organisations, bodies and fora are working on cyber security[4] issues, albeit to largely varying extents. *Inter alia* these include the OECD,

[1] European Parliament, Committee on Foreign Affairs, *Draft Report on Cyber Security and Cyber Defence (2012/2096(INI),* p.4, 22 June 2012.

[2] James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*, Senate Select Committee on Intelligence, 12 March 2013.

[3] Mark Mazzetti and David E. Sanger, The New York Times, *Security Leader Says U.S. Would Retaliate Against Cyberattacks*, http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all, 12 March 2013, last accessed 03 April 2013.

[4] The concept of cyber security is defined within the Cybersecurity Strategy of the European Union (07 February 2013) as commonly referring to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of information contained therein.

the OSCE, the EU, the Council of Europe, BRICS, the OAS, AU, APEC, the Shanghai Cooperation Organisation, the G8/G20, the UN, the Internet Governance Forum, ICANN, NATO, and the World Economic Forum. Since international and regional cooperation on cyber security are required in order to deal effectively with the cross-border nature of cyber related threats, this paper therefore examines regional level efforts in the Association for Southeast Asian Nations (ASEAN) region to counter these threats.

To date, national and regional efforts to adopt comprehensive cyber security strategies have been somewhat slow and fragmented. Similarly, ASEAN Member States' efforts to adopt a regional comprehensive framework for cyber security are so far piecemeal and fragmented (as are national level efforts). An ASEAN-wide comprehensive cyber security framework has not yet been developed, official public documents are vague, the 2013 schedule for official meetings does not include cyber security,[5] and the precise extent of discussions and proposed initiatives is difficult to fully ascertain,[6] and lacks full transparency.

While still a developing area, this lack of region-wide cohesiveness detracts from security of the region and a proper functioning market. This paper finds that it is essential for ASEAN as a region to develop a comprehensive approach to deal with cyber security issues so as to enhance its overall resilience to serious cyber threats. Resilience[7] is taken

[5] ASEAN, *Official Meetings 2013*, as of April & July 2013.

[6] Unattributable, May 2013.

[7] Note: Council of the European Union conclusions on the wider EU understanding of resilience were issued on 28 May 2013 (Council of the European Union, *Council conclusions on EU approach to resilience*, 3241st Foreign Affairs Council Meeting, Brussels, 28 May 2013.)

The study focuses on building a resilient cyber security regime in the ASEAN region. The term "Cyber Resilience" is therefore not incorporated within the document since the focus lies rather on the term "cybersecurity".

to mean the ability of the ASEAN region, its Member States and its citizens to be prepared, to be able to adapt, and to make quick progress post-incidents. The following sections outline why ASEAN is important to the global cyber security order, the primary global cyber security challenges of common interest to ASEAN Member States, ASEAN cyber security related official documents and measures as well as how the region currently lacks a resilient cyber security regime, and finally several recommendations relevant to the ASEAN context on a way forward to create a resilient regional cyber security regime.

II. Why ASEAN

ASEAN is a particularly significant region in terms of international cyber security issues. First, ASEAN's centrality in the regional architecture of the wider Asia Pacific region and its potential role as a neutral broker is significant in terms of international cyber security cooperation. In the context of U.S.-China relations and recent political focus on the impact of state and economic cyber espionage, a 2012 Council on Foreign Relations working paper's[8] references to ASEAN's history of working together with the United States and China and to how ASEAN is seen as a neutral broker by most major powers, is particularly important. Furthermore, ASEAN's potential role as neutral broker is even more pertinent in mitigating possible tensions and misunderstanding between these two state actors if, as a 2013 Centre for Strategic and International Studies report[9] states, China's use of cyberspace to gain military and economic advantage is one of the primary forces shaping a new Asian strategic environment and China's activities have created "an implicit

---

[8] Joshua Kurlantzick, Council on Foreign Relations, *ASEAN's Future and Asian Integration*, International Institutions and Global Governance Program, November 2012.

[9] James Lewis, CSIS, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia,* Prepared for the Lowy Institute MacArthur Asia Security Project, 07 March 2013.

commonality of interests" among other regional powers. It should also be noted that China is similarly concerned about targeted cyber threats.[10]

Second, while citizens in many areas of the region still do not have access to Information and Communications Technology (ICT), numbers are set to increase. According to the 2013 Impact Assessment report[11] accompanying the European Commission's Proposal for a Directive on network and information security, of the 2.1 billion Internet users worldwide, most are located in Asia (922.2 million). The next most significant region in terms of numbers of Internet users is Europe with 476.2 million users.[12] China alone has 485 million Internet users - more than any other country *or region* (including Europe and the rest of Asia) - and an Internet penetration of only 36.3 per cent.

ASEAN, comprising ten Member States,[13] has a total population of slightly over 600 million.[14] Recent indicators forecast that the population growth rate is higher in most of the ASEAN countries than the Asian average for the period 2010-2015,[15] which should

[10] James Lewis, CSIS, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia,* Prepared for the Lowy Institute MacArthur Asia Security Project, 07 March 2013.

[11] European Commission, *Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union SWD(2013) 32 final*, 07 February 2013.

[12] European Commission, Commission Staff Working Document*, Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union SWD(2013) 32 final*, Annex 12: Internet 2011 in Numbers, 07 February 2013.

[13] ASEAN Member States: Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam.

[14] ASEAN Statistics, *Selected basic ASEAN indicators Table 1*, as of January 2013.

[15] Credit Suisse Research and Analytics, *ASEAN's positive demographics underpins stable growth*, 31 October

raise the probabilities of increased demands for ICT usage. Within the region, Internet users have almost doubled during the period 2008 to 2011 and mobile phone density is close to 967.5 units per 1,000 persons.[16] It is estimated that mobile broadband subscriptions will be close to 70 per cent of the world's total population by 2017. Globally, there are twice as many mobile broadband subscriptions vis-à-vis fixed line broadband subscriptions and furthermore, GSM/EDGE mobile technology will cover more than 90 per cent of the world's population with 85 per cent accessing WCDMA/HSPA mobile technology at speeds of up to 2Mb per second by 2017.[17]

Region targets for ASEAN are set for "exponential growth" in ICT adoption and a ramping up of infrastructure and human capital development is intended to achieve these targets.[18] It is intended that fixed and mobile broadband access be improved in rural and remote areas, more affordable IT access be provided, and prioritised projects include an ASEAN Broadband Corridor.[19] Furthermore, in order to improve speed as well as to lower interconnectivity costs, the region is currently assessing the feasibility of developing an ASEAN Internet-Exchange Network - a platform to facilitate intra-ASEAN Internet traffic "to facilitate peering among ASEAN Internet access providers".[20] Finally, critical infrastructure protection will be essential, particularly in consideration of plans for the region which include establishing "an integrated and regional connectivity"[21] through:

2012, http://www.credit-suisse.com/researchandanalytics, last accessed 08 May 2013.

[16] ASEAN Secretariat, *ASEAN Community in Figures 2012*, March 2013.

[17] UNODC (United Nations Office on Drugs and Crime), *Comprehensive Study on Cybercrime*, Draft – February 2013.

GSM/EDGE: Global System for Mobile Communications/Enhanced Data rates for GSM Evolution

WCDMA/HSPA: Wideband Code Division Multiple Access/High Speed Packet Access

[18] ASEAN Secretariat, *ASEAN ICT Masterplan 2015*, 2011.

[19] ASEAN Secretariat, Master Plan on ASEAN Connectivity, January 2011.

[20] ASEAN, *Mactan Cebu Declaration Connected ASEAN: Enabling Aspirations*, 19 November 2012.

[21] ASEAN Secretariat, *Master Plan on ASEAN Connectivity*, January 2011.

i) A multi-modal transport system (i.e. an integrated transport network such as air (harmonising air navigation systems), road, rail (the Singapore-Kunming Rail Link project targeted for completion in 2015), and maritime;
ii) Enhanced ICT infrastructure such as the optical fibre network; and
iii) A regional energy security framework (i.e. the ASEAN Power Grid, Trans-ASEAN Gas Pipeline, and planned grid interconnection projects such as the regional gas grid).

Closer Connectivity: Higher Probabilities of Cross-border Cyber Threats

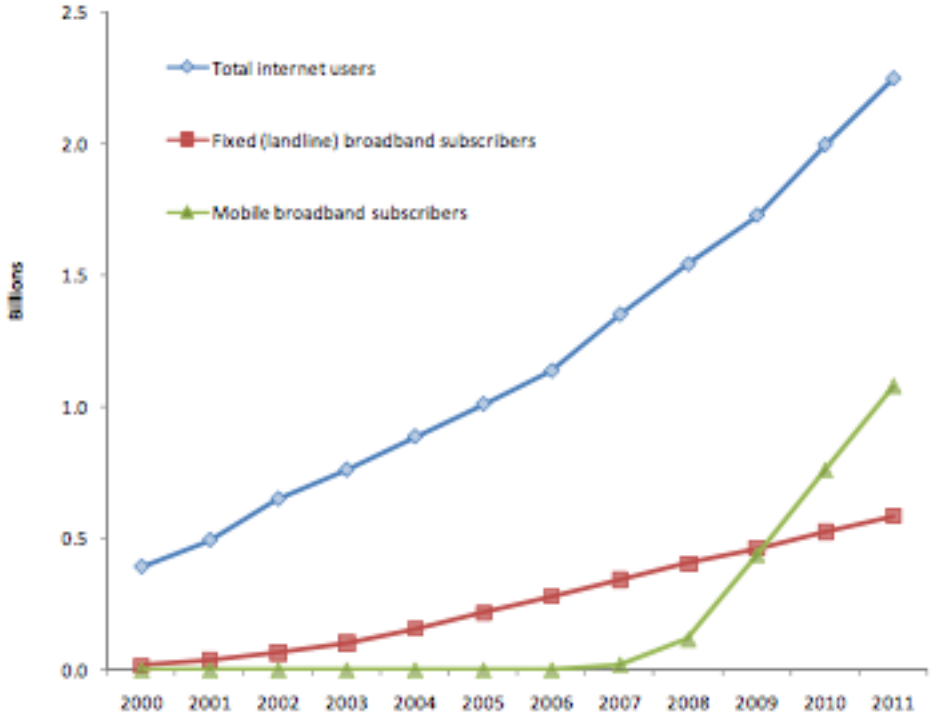
Closer connectivity however raises the probabilities of trans-national crime and cross-border cyber related challenges such as serious cyber threats and cyber incidents. Akin to the "global connectivity revolution"[22] (depicted in the graph below), these levels of increasing connectivity in the ASEAN region significantly raise the threat spectre for cross-border cyber incidents. With increasing access to high-speed networks, levels of low-level cybercrime have already increased in the region[23] (Appendix 1 below provides an overview of some cyber related incidents in the ASEAN region for the period January 2012 to present). It is also suggested that as the level of cybercrime is likely to grow in Asia, this could possibly increase instability because of its links to espionage and military activities.[24]

[22] UNODC (United Nations Office on Drugs and Crime), *Comprehensive Study on Cybercrime*, Draft – February 2013.

[23] James Lewis, CSIS, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia,* Prepared for the Lowy Institute MacArthur Asia Security Project, 07 March 2013.

[24] James Lewis, CSIS, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia,* Prepared for the Lowy Institute MacArthur Asia Security Project, 07 March 2013: (language was a barrier but this seems to be changing).

Figure 1.2: Global internet connectivity 2000 - 2011



Source: ITU World Telecommunication ICT Indicators 2012

The ICT Development Divide: Cyber Security Advantage

As it stands, there are varying levels of ICT development and adoption across the region and efforts are under way to "bridge the digital divide" to promote greater adoption of ICT. The three ASEAN Community blueprints are aligned with the Initiative for ASEAN Integration (IAI) and the Hanoi Declaration on Narrowing the Development Gap for Closer ASEAN Integration, which aim to narrow the development divide and provide assistance to Cambodia, Lao PDR, Myanmar and Vietnam (CLMV) to meet ASEAN-wide targets and commitments to realise the ASEAN Community. Furthermore, according to the 2011 Master Plan on ASEAN Connectivity,[25] the extent of the digital divide across the region (highlighted by way of example in the below graph of Internet subscriptions and mobile phone density[26]) and how it can be overcome is regarded as the most important challenge to developing ASEAN ICT infrastructure.

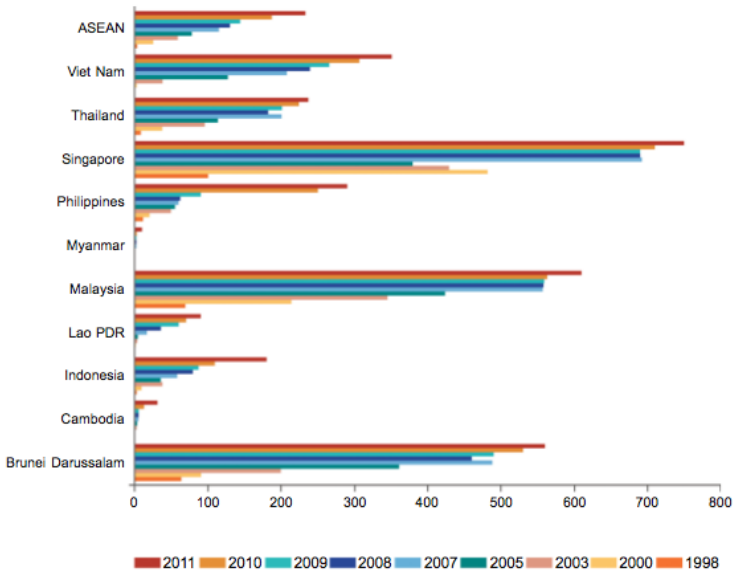
[25] ASEAN Secretariat, Master Plan on ASEAN Connectivity, January 2011.

[26] ASEAN Secretariat, *ASEAN Community in Figures 2012*, March 2013.

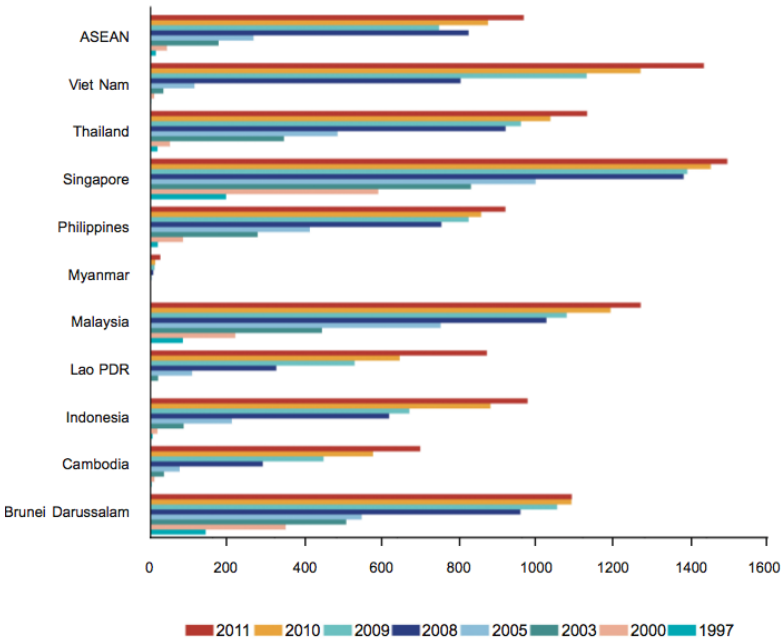
08 ASEAN telecommunications

Chart 3

ASEAN: Internet subscribers/users per 1000 persons
for periods indicated



ASEAN: Cellular/mobile phone density (number of units per 1000 persons)
for periods indicated



First, in this regard, while developed countries globally have higher levels of Internet access (70 per cent) than developing countries (24 per cent), it should be noted that in fact the absolute number of Internet users in developing countries already far outweighs the number in developed countries,[27] and it seems that "the digital divide is larger when measured in terms of subscribed capacity than in terms of subscriptions".[28] In 2011, approximately 62 per cent of all Internet users were in developing countries.[29] Vietnam is a particularly significant case in point since it was globally ranked in June 2012 as 18th in terms of Internet use (eighth in Asia and third in ASEAN behind Indonesia and the Philippines), an estimated 31 million people (35 per cent of the population) are connected to the Internet, and usage is expected to reach 45-50 per cent of the population by 2020.[30] In Cambodia for example, in March 2013 there was an increase of 60 per cent in Internet users since 2012 and a figure of 2.7 million citizens were reported as online by December 2012.[31]

Furthermore, in analysing the ASEAN Secretariat's March 2013 *Community in Figures* report for 2012,[32] figures for mobile phone density[33] across the region show that Member

[27] UNODC (United Nations Office on Drugs and Crime), *Comprehensive Study on Cybercrime*, Draft – February 2013.

[28] International Telecommunication Union (ITU) Annual Report, Measuring the Information Society – Executive Summary, 2012.

[29] UNODC (United Nations Office on Drugs and Crime), *Comprehensive Study on Cybercrime*, Draft – February 2013.

[30] The Citizen Lab, Southeast Asia CyberWatch – August 2012, *Vietnam ranks among the top 20 nations by Internet use*, https://citizenlab.org/2012/08/southeast-asia-cyberwatch-august-2012/#vietnam, last accessed 20 August 2013.

[31] The Citizen Lab, Southeast Asia CyberWatch – March 2013, *Cambodia reports increased Internet penetration*, March 2013.

[32] ASEAN Secretariat, *ASEAN Community in Figures 2012*, March 2013.

States are close to saturation in terms of number of units per 1,000 persons marking a narrowing digital divide. The average mobile phone density for the region is close to 967.5 units per 1,000 persons – as compared to an average of 232.8 Internet subscribers/Users per 1,000 persons. There is a marked contrast in the lower variance of mobile phone density as between ASEAN Member States across the region compared to the higher gaps in numbers of Internet users/subscriptions. Vietnam, for instance, now ranks next to Singapore in terms of cellular/mobile phone density with 1,434 units per 1,000 persons compared to the highest regional average of 1,495 in Singapore. Myanmar is the exception with by far the lowest mobile phone density of 25.7 units per 1,000 persons, although these figures are set to change with the awarding of two telecommunications licences in June 2013. In liberalising communications networks, Myanmar intends to increase mobile penetration by 50 per cent (from one million users for a population of 60 million) by 2015 to increase Internet access.[34] Indonesia has nearly 63 million Internet users of which the majority accesses the Internet through mobile devices.[35]

Second, such digital divides and differing levels of ICT development and adoption should not necessarily impinge upon prospects of regional cyber security cooperation nor should they deter efforts in seriously tackling cross-border cyber related threats, in ASEAN or elsewhere. Rather, regional cooperation efforts can stimulate progress, fuelling collective security and the further enhancement of national cyber security measures no matter where a state is on the spectrum of ICT development. In fact, such disparity in ICT development can advantage countries with a less developed ICT infrastructure and less connected critical infrastructure. As less digitally developed countries become more connected, lessons may be applied from other states' experiences in countering cyber related threats, best practice policies and measures may be implemented, and both security and data privacy by design may be incorporated from inception in the

[33] The smart phone proportion of mobile phone density was not published under these figures in March 2013.

[34] The Citizen Lab, Southeast Asia CyberWatch, July 2012.

[35] The Citizen Lab, Southeast Asia CyberWatch, *Internet access on the rise*, January 2013.

development of ICT and connected critical infrastructures. Furthermore, higher levels of ICT development and adoption as well as connected critical infrastructures have not necessarily been synonymous in the past with equally high levels of development and implementation of cyber security measures. Rather, more often than not, it has instead meant higher exposure to vulnerabilities and possible cyber threats. This has been described as "the combination of a blessing and a curse" so that while the previous technology cycle has been lost and the new technology cycle needs to be built, it means that in doing so it is free of legacy and lessons may be learned from the mistakes of others.[36]

Therefore, where countries are developing (or further developing) their ICT and critical infrastructure, and are in the process of awarding contracts for example (as in the case of Myanmar's issuance of licences for telecommunications in 2013), terms and conditions requiring the implementation of at least minimum standards and best practice measures can now be negotiated. It is contended[37] that "baking in cyber security" from the beginning is perhaps easier for developing countries rather than developed countries where there is less ability to affect things such as basic "cyber hygiene" and "hardening" and the private sector is already more independent. If market incentives are leveraged and if more can be done from the beginning to build a market standard of care (without being too directive so that the private sector can still develop more efficient ways of mitigating threats), it is felt that this could be more effective and more efficient in the long run. In the United States, for example, sectors vary quite a bit in their levels of cyber security capabilities and there is no base-line standard of care so that the U.S. is now challenged with recreating or even breaking some paradigms in order to come up with that base line. Furthermore, it is argued that no matter how wealthy the country, it cannot protect against everything, and therefore, developing countries with lower budgets and less resources or manpower for cyber activities, and developed countries

[36] CENS Cybersecurity Workshop, *Effective and Credible Cyber Deterrence*, 27 May 2013.

[37] Chris Finan, former Director for Cybersecurity Legislation and Policy, U.S. National Security Staff at the White House, CENS Cybersecurity Workshop, *Effective and Credible Cyber Deterrence*, 27 May 2013.

alike, should look for efficiencies where they can by pursuing a risk-based approach. In other words, with a finite amount of resources, a decision must be made regarding the highest risks for which these resources should be used based on data and a constant reviewing of the risks and how they evolve.

It is in the interest of ASEAN states as well as the international community that measures be put in place to mitigate possible "weak links" and havens of vulnerable architectures. In particular, measures should be incorporated from the outset if the CLMV grouping is to participate in the ASEAN energy schemes delineated under the Initiative for ASEAN Integration Strategic Framework and Work Plan 2, such as the ASEAN Power Grid, segments of the Singapore-Kunming Rail Link, and possible CLMV ICT manufacturing bases/clusters (with expected connection to other IT parks in ASEAN).[38]

From the outset, agreements may be entered for technical assistance as well as training and expertise (both technical and non-technical) in order to assist in building a resilient cyber security architecture. Such assistance could be provided by another ASEAN member or grouping thereof with established expertise, by bilateral engagements with non-ASEAN states, or by third parties such as the ITU-IMPACT alliance and the EU. ITU-IMPACT, for instance, completed a Computer Incident Response Team (CIRT) readiness assessment and cyber drill simulation for the CLMV grouping in December 2011 and the EU proposes in its February 2013 *Cybersecurity Strategy of the European Union*[39] to work towards

[38] ASEAN, *Initiative for ASEAN Integration (IAI) Strategic Framework and IAI Work Plan 2 (2009-2015).*

[39] European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final),* 07 February 2013.

It is worth noting that in the EU, previous efforts by the European Commission and EU Member States have also been too fragmented to deal effectively with the growing challenges of cyber issues.[39] In June 2012,

closing the digital divide and to actively participate in international efforts to build cyber security capacity. Regarding bilateral engagements, it is worth noting that Indonesia and Australia partnered in 2011 to establish the Cyber Crime Investigation Center in Jakarta and in May 2013 a second joint cyber crime office was opened for information-sharing,

---

the European Parliament Committee on Foreign Affairs issued a *Draft Report on Cyber Security and Cyber Defence*[39] underlining the need for a global and coordinated approach to these challenges at the EU level with the development of a comprehensive EU cybersecurity strategy (only ten of then 27 EU Member States had by that time officially adopted a national cybersecurity strategy). By April 2013, this number increased to 14 EU Member States.[39] Consequently, with a view to outlining the EU's "vision" in this area, the European Commission and High Representative of the Union for Foreign Affairs and Security Policy released the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* in February 2013, and the European Commission further issued as part of its overall strategy, the *Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union.*

References:

- European Commission/EEAS – Press Releases, *EU Cybersecurity plan to protect open internet and online freedom and opportunity*, 07 February 2013, http://europa.eu/rapid/press-release_IP-13-94_en.htm, last accessed 21 May 2013.
- European Parliament, Committee on Foreign Affairs, *Draft Report on Cyber Security and Cyber Defence (2012/2096(INI),* 22 June 2012.
- ENISA, *National Cyber Security Strategies in the World,* http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world, last accessed 21 August 2013.
- European Commission, *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (2012/0027 (COD),* 07 February 2013.

coordinating of investigations, and tackling cybercrime originating in Indonesia.[40] Lastly, an announcement was made in June 2013 of India's intention to build the Indira Gandhi Hi-Tech Cyber Laboratory in Vietnam.[41]

In this regard, it is now widely accepted that countries, which have not yet developed or implemented a comprehensive cyber security strategy, should publish and implement a framework as soon as possible (including national contingency and cyber crisis management plans).[42] To assist in the building of understanding and capacity to develop national cyber security strategies (particularly for those countries under budgetary constraints or lacking the necessary expertise and capabilities), the National Cyber Security Framework Manual[43] of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), which was published in 2012 to serve as a guide to develop and improve national policies, laws and regulations, decision-making processes and other aspects relevant to national cyber security since the "implementation, maintenance and improvement of national cyber security comprises a range of elements",[44] may be consulted. The European Network and Information Security Agency's (ENISA) Guidebook on National Cyber Security Strategies may also be consulted as a guide for actions and steps which can be implemented to develop and maintain a national cyber security strategy (it includes a national cyber security strategy lifecycle and a list of key

[40] The Citizen Lab, Southeast Asia CyberWatch, *Indonesia and Australia open joint cybercrime office*, May 2013.

[41] The Citizen Lab, Southeast Asia CyberWatch, *India to build a "Cyber Forensics Laboratory" in Vietnam*, June 2013.

[42] Delineating recommended guidelines for developing, implementing and maintaining a national cyber security strategy is beyond the scope of this paper.

[43] Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012.

[44] Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012.

performance indicators).[45] The European Commission has also been called upon to assist non-EU countries, if needed, in their efforts to build cyber security and cyber defence capabilities,[46] and the 2013 EU Cybersecurity Strategy proposes engaging with international partners and organisations, the private sector and civil society to support global capacity building in third countries and to develop "donor coordination for steering" capacity building efforts. It is proposed that EU aid instruments will be used for cyber security capacity building, including assisting the training of law enforcement, judicial and technical personnel and to support the creation of national policies, strategies and institutions in third countries.

Finally, the Council for Security Cooperation in the Asia Pacific (CSCAP) concludes that common collective measures include "cooperative arrangements" for capacity development and technical assistance and recommends that at the level of regional cooperation, the ASEAN Regional Forum (ARF) should implement capacity building and technical assistance measures by developing a programme of advice, training and technical assistance that strengthens the cyber security capacity and capability of crisis management in all states.[47]

Inherent Constraints

Like other regional blocs however, ASEAN faces obstacles of its own. Frequently cited limitations include structural and organisational limitations, a small staff at the Secretariat, decision-making by consensus, disparity in development among Member

[45] Resilience and CIIP Unit ENISA, *ENISA Guidebook on National Cyber Security Strategies*, available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide, 19 December 2012.

[46] European Parliament, Committee on Foreign Affairs, *Draft Report on Cyber Security and Cyber Defence (2012/2096(INI),* p.4, 22 June 2012.

[47] CSCAP Memorandum No. 20, *Ensuring a Safer Cyber Security Environment – A Memorandum from the Council for Security Cooperation in the Asia Pacific (CSCAP),* May 2012.

States, divisions within Member States, an aversion to intervening in the affairs of other Member States, and little capability in handling traditional or non-traditional security challenges, and little capacity has developed to combat drug-trafficking, human trafficking, terrorism and other high priority non-traditional security threats.[48] The aforementioned CFR Working Paper[49] outlines how, until now, ASEAN has been more successful in promoting trade integration and creating regional forums for discussing security issues than it has been in promoting more concrete security or economic integration.

III. Primary Global Cyber Security Challenges of Common Interest to ASEAN Members: Recent Status & Emerging Trends

In dealing with cyber threats, some of the most significant global challenges of common interest to ASEAN Member States include:

- The increasing volume and complexity of threats
- The dilemma of accurate attribution
- An increasing number of state and non-state actors
- The lack of harmonised definitions and understanding of "cyber" terminology
- Achieving effective public-private sector cooperation
- Insufficient levels of R&D
- The inadequacy and unavailability of expertise
- Insufficient public awareness, and
- The protection of civil liberties.

[48] Joshua Kurlantzick, Council on Foreign Relations, *ASEAN's Future and Asian Integration*, International Institutions and Global Governance Program, November 2012.

[49] Joshua Kurlantzick, Council on Foreign Relations, *ASEAN's Future and Asian Integration*, International Institutions and Global Governance Program, November 2012.

Increasing Volume and Complexity of Cyber Threats

First, the alarming and continually increasing volume and complexity of threats is a serious global challenge common to the wider international community including ASEAN Member States. The increased frequency at which attacks are occurring is becoming unwieldy and posing a serious challenge to effective and timely implementation of policy and legislation. In some instances, according to James R. Clapper, the United States Director of National Intelligence, these technologies are being applied faster than the policy community's ability to understand the security implications and mitigate the potential risks.[50] In addition, the time between an attack and systems compromise can take a matter of minutes yet it can often take months for the breach to be discovered.[51] Multi-national computer security firms assessing the global threat landscape continually highlight changes in the frequency and complexity of evolving or new threats by way of quarterly and annual reports. In 2012 at least two new viruses were discovered every second and one in fourteen Internet downloads contained malware.[52] Mobile malware samples discovered by McAfee Labs were 44 times that discovered in 2011,[53] and it is estimated that 150,000 computer viruses are in circulation daily with 148,000 computers compromised per day.[54] Furthermore, according to the World Economic Forum, there is a

[50] James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*, Senate Select Committee on Intelligence, 12 March 2013.

[51] Costin Raiu, Director, Global Research and Analysis Team, Kaspersky Labs, *Cyber Terrorism – An Industry Outlook*, Speaking at Cyber Security Forum Asia, 03 December 2012.

[52] Costin Raiu, Director, Global Research and Analysis Team, Kaspersky Labs, *Cyber Terrorism – An Industry Outlook*, Speaking at Cyber Security Forum Asia, 03 December 2012.

[53] McAfee Labs, *McAfee Threats Report: Fourth Quarter 2012 – Executive Summary*, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012-summary.pdf, last accessed 04 April 2013.

[54] European Commission/EEAS – Press Releases, *EU Cybersecurity plan to protect an open internet and online freedom and opportunity*, 07 February 2013, http://europa.eu/rapid/press-release_IP-13-94_en.htm, last accessed 21 May 2013.

10 per cent likelihood of a major critical information infrastructure breakdown in the coming decade, which could cause estimated damages of USD250 billion.[55]

The increasing complexity and sophistication of these attacks is creating an environment of uncertainty and unpredictability. Technologies and techniques are both strengthening and evolving at an extremely fast rate and new, more dangerous, cyber threats are introduced on a continual basis. In 2012 alone,[56] new advanced persistent threats (APTs)[57] accelerated, new malware sample discoveries increased by 50 per cent, and ransomware[58] saw material growth (more than triple on Windows PCs). In addition, the

---

[55] European Commission/EEAS – Press Releases, *EU Cybersecurity plan to protect an open internet and online freedom and opportunity*, 07 February 2013, http://europa.eu/rapid/press-release_IP-13-94_en.htm, last accessed 21 May 2013.

[56] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

See also McAfee Labs, *McAfee Threats Report: Fourth Quarter 2012 – Executive Summary*, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012-summary.pdf, last accessed 04 April 2013.

[57] Dmitri Alperovitch, Vice-President, Threat Research, McAfee, *Revealed: Operation Shady RAT*, White Paper, 2011:

APTs: Advanced Persistent Threats: Targeted compromises that occur largely without public disclosures. They present a far greater threat to government and to companies, as the adversary is tenaciously persistent in achieving their objectives. The key to these intrusions is that the adversary is motivated by a massive hunger for secrets and IP – this is different to the immediate financial gratification that drives much of cybercrime.

[58] McAfee Labs, *McAfee Threats Report: Fourth Quarter 2012 – Executive Summary*, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012-summary.pdf, p.4, last accessed 04 April 2013.

first ransomware "kits", which enable criminals without programming skills to extort financial payments, were introduced for sale on the black market.[59]

According to McAfee's Threats Report for 2012,[60] predictive assessments suggest that a variant of a new APT development called Operation High Roller designed to target financial services infrastructure and attack the Automated Transfer Systems in Europe and new High Roller-based attacks aimed at manufacturing and import/export firms will target the Automated Clearing House infrastructure which processes much of the world's e-commerce transactions. Threat predictions for 2013[61] expect an increase in or introduction of threats such as mobile phone ransomware kits. The marked increase in the number of mobile-enabled threats[62] is particularly relevant for the ASEAN region when

---

"Ransomware attacks tend to come in two forms. In the first form of attack the cybercriminal expropriates confidential information either from the user system or enterprise IT infrastructure and then demands payment for not releasing the data into the public domain. In the second form of attack the cybercriminal establishes control of a user system (or mobile device), encrypts user data, and demands payment in exchange for this encryption key. Users who agree to the ransom demand may have no way of knowing if they will ever receive the promised encryption key."

[59] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

[60] McAfee Labs, *McAfee Threats Report: Fourth Quarter 2012 – Executive Summary*, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012-summary.pdf, last accessed 04 April 2013.

[61] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

[62] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

figures[63] show that average mobile phone density for the region is close to 967.5 units per 1,000 persons compared to an average of 232.8 Internet subscribers/Users.

An increase in or introduction of "hacking as a service", where anonymous buyers and sellers exchange malware kits and development services in underground forums, and "large-scale attacks like Stuxnet" that will attempt to destroy infrastructure rather than focus on financial gain are also to be expected.[64] Hacking as a service is a particularly concerning development since cybercriminals and organised cybercrime gangs, seeking financial gain by selling or leasing kits and services anonymously, may cause unintended or unexpected consequences if their customers are either criminals without programming skills or more malicious non-state or state actors.

Stuxnet is regarded as the first known "cyber missile" identified with the capability to destroy hardware and cause kinetic damage.[65] These new advanced cyber capabilities have the ability to cause physical damage and can manipulate the behaviour of a target in a way that could destroy the target.[66] Once released, they can be reverse-engineered, tampered with, and manipulated for new targets (including against the authors) by a multitude of actors. There is therefore an increasing concern over the evolution and

---

See also McAfee Labs, *McAfee Threats Report: Fourth Quarter 2012 – Executive Summary*, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012-summary.pdf, last accessed 04 April 2013.

[63] ASEAN Secretariat, *ASEAN Community in Figures 2012*, March 2013.

[64] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

[65] Costin Raiu, Director, Global Research and Analysis Team, Kaspersky Labs, *Cyber Terrorism – An Industry Outlook*, Speaking at Cyber Security Forum Asia, 03 December 2012.

[66] Ralph Langner, Cyber security consultant, Presentation, 28 September 2012, http://www.youtube.com/watch?v=v1EcziU_AtY, last accessed 06 January 2013.

escalation of these attacks and their possible "transition from disruptive to destructive"[67] as compared to Distributed Denial of Service (DDoS) attacks and theft of government data as well as intellectual property theft which can cause virtual destruction.

Dilemma of Accurate Attribution

Second, the accurate attribution and identification of those responsible for a cyber attack is not easily achieved. Varying techniques may be employed to avoid detection such as the more recently discovered trend of building out of a "superdomain" of infected websites, which allows hundreds or thousands of websites to be placed behind one IP address, and frequently changing the address in order to avoid detection.[68] A report of the Institute for Information Infrastructure Protection[69] further argues that without accurate appropriation of blame it is difficult to take action against a perpetrator and hold those responsible to account. It states that creating a system of deterrence is therefore difficult and that legal and policy frameworks for responding to cyber attacks cannot work unless there is adequate attribution since these frameworks remain incomplete if there is no basis to actually use them, in other words, "sufficient attribution". Finally, insofar as states may be concerned, misappropriation can lead to misunderstandings, misinterpretations, or possible escalation in tensions or conflict.

Increasing Number of State and Non-State Actors

The third issue is the recent increase in the involvement of state and non-state actors in cyber issues. The fundamental shift in challenges facing national security is particularly evident with cyber related threats where a wide range of varying threats are not coming

---

[67] American Forces Press Service, *NSA Chief: Cyber World Presents Opportunities, Challenges*, http://www.defense.gov/News/NewsArticle.aspx?ID=117060, 10 July 2012, last accessed 02 January 2013.

[68] McAfee Labs, McAfee Threats Report: Fourth Quarter 2012 – Executive Summary, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2012-summary.pdf, p.5, last accessed 04 April 2013.

[69] Dr. Jeffrey Hunker, Bob Hutchinson, Jonathan Margulies, *Role and Challenges for Sufficient Cyber-Attack Attribution*, Institute for Information Infrastructure Protection, p.5, January 2008.

solely from state actors but from a range of non-state actors such as cybercriminals, terrorists, hackers, hacktivists, and individuals (as well as natural disasters[70] or mistakes[71]). Solutions will therefore require cooperation between public authorities, the private sector and civil society. Finally, according to General Keith B. Alexander, Director of the National Security Agency in the United States, since such non-state actors must now also be considered, cyber attack deterrence is even more difficult than nuclear deterrence.[72]

Regarding non-state actors, some of the following reports comprise predictive components and are therefore worthy of consideration by ASEAN Member States. There is an increasing concern in the European Union over the possibility of politically motivated attacks and cyber threats from organised criminals and terrorist groups against the critical information systems and infrastructures of the EU and its Member States.[73] In March 2013, the U.S. Intelligence Community confirmed indications of "heightened interest" from terrorist organisations to develop offensive cyber capabilities, although it estimates that these groups will probably be constrained by resource and organisational limitations as well as competing priorities.[74] McAfee Labs considers that today, fears of a terrorist group moving to the next step and launching a "cyber-physical attack", in other words, an online attack in conjunction with a physical attack by remotely disrupting critical

[70] This should be of particular relevance to the ASEAN region where natural disasters are not an infrequent occurrence.

[71] Where intentions are not malicious but the unintended consequences are far-reaching.

[72] American Forces Press Service, *NSA Chief: Cyber World Presents Opportunities, Challenges*, http://www.defense.gov/News/NewsArticle.aspx?ID=117060, 10 July 2012, last accessed 02 January 2013.

[73] European Parliament, Committee on Foreign Affairs, *Draft Report on Cyber Security and Cyber Defence (2012/2096(INI),* p.5, 22 June 2012.

[74] James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*, Senate Select Committee on Intelligence, 12 March 2013.

infrastructure such as a defence or communications system and easily causing more damage are "not just fantasy".[75] Like the European Union, the U.S. Intelligence Community confirms[76] government concern that a more radical group of hacktivists could form "to inflict more system impacts" or perhaps even "accidentally trigger unintended consequences that could be misinterpreted as a state-sponsored attack". Equally, McAfee Labs researchers foresee a decline in online hacktivists such as Anonymous to be replaced by more politically committed or extremist groups in their wake.[77]

The U.S. Intelligence Report judges that "there is a remote chance of major cyber attack against US critical infrastructure systems during the next two years that would result in a long-term, wide-scale disruption of services, such as a regional power outage." While it estimates that the level of technical expertise and operational sophistication (including the ability to cause physical damage or overcome manual overrides) will be out of reach for most actors within this time, the concern is that isolated state or non-state actors might use less sophisticated cyber attacks to access poorly protected networks that control core functions and these less sophisticated attacks could cause unforeseen significant outcomes due to mistake.

Regarding the role of state actors in the cyber domain, which has also markedly increased, threat predictions for 2013 foresee that states and armies will now become "more frequent sources and victims of cyber threats".[78] A significant increase in state actors' use

[75] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

[76] James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*, Senate Select Committee on Intelligence, 12 March 2013.

[77] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

[78] McAfee Labs, *2013 Threats Predictions Report*, http://www.mcafee.com/sg/resources/reports/rp-threat-predictions-2013.pdf, last accessed 04 April 2013.

of cyber capabilities, which could possibly lead to an increase in the chances of miscalculations, misunderstandings, and unintended escalations is reported by the U.S. security community, although aside from a military conflict or crisis threatening vital interests, it suggests that it is unlikely that other advanced cyber state actors will launch a "devastating attack".[79]

According to a 2013 CSIS report[80] based on findings produced for the UNIDIR, while states are slow to admit possessing offensive cyber capabilities, ten Asian countries are developing cyber capabilities and "all are wrestling with how to adjust their policies and practices to new technology". Eight are developing military capabilities and doctrine – Australia, China, North Korea, India, Malaysia, Myanmar, Japan and South Korea; Brunei and Singapore are developing defensive capabilities; and capabilities of other Asian nations range from "nominal to relatively sophisticated". According to this report, cyber conflict has a "large Asian dimension" – in Asia it includes "planning for military competition and asymmetric warfare, engagement in economic espionage to gain long-term economic and trade advantages, as well as a new kind of transnational mass political action". It concludes that Asia has become the locus of cyber conflict, and that malicious activity in cyberspace, which could possibly inflame existing tensions or increase misperceptions or miscalculations among governments of the intent and risk of cyber actions, poses the greatest cyber risk to security in Asia.

Lack of Harmonised Definitions and Understanding of "Cyber" Terminology

This leads to the fourth issue for the global community, which is the lack of shared norms for responsible state behaviour at international level and agreement on the applicability of international law. There is no international or regional agreement on clear and harmonised definitions for what constitutes "cyber security", "cyber attack" or "cyber

[79] James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*, Senate Select Committee on Intelligence, 12 March 2013.

[80] James Lewis, CSIS, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia,* Prepared for the Lowy Institute MacArthur Asia Security Project.

defence", and the lines between cyber crime, cyber espionage and cyber attack are considered difficult to distinguish. Furthermore, the very understanding of cyber security and other key terminologies vary significantly between jurisdictions.[81]

Achieving Effective Public-Private Sector Cooperation

Finally, since critical infrastructure and critical information infrastructure are mostly either owned or operated by the private sector and the design and manufacturing of most software and hardware mainly conducted by it, close cooperation and information sharing with the public sector is essential to allow for real time response and the identification of threats. Trust and confidence issues arise and many known incidents often remain unreported[82] on account of the sensitive nature of information, fear of negative corporate publicity and possible damage to brand reputation.

The most suitable approach for cooperation between the public and private sector is contentious and an increasingly heated issue of concern across the international community. Aspects of current debate surround whether cooperation should be regulated and if so, whether it should be through voluntary or mandatory means. Some governments have chosen to regulate critical infrastructure providers by imposing minimum standards, while other governments have chosen to incentivise the private sector to encourage industry cooperation.[83]

[81] European Parliament, Committee on Foreign Affairs, *Draft Report on Cyber Security and Cyber Defence (2012/2096(INI),* p.4, 22 June 2012.

[82] For example, recent surveys in Australia show that less than 50% of the private sector reported known incidents to the authorities.

[83] Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, p.38, Tallinn 2012.

IV. Overview of ASEAN Cyber Security Related Measures: How the Region Currently Lacks a Resilient Cyber Security Regime

In light of the principles of the ASEAN Charter and Member States' aims to establish the ASEAN Community (comprising the ASEAN Political-Security Community, the ASEAN Economic Community, and the ASEAN Socio-Cultural Community) by 2015, in other words, a region that is "politically cohesive, economically integrated and socially responsible in order to take advantage of current and future opportunities, and effectively respond to regional and international challenges",[84] cohesive efforts to comprehensively tackle cyber security issues are crucial to these aims and in the shared interests of ASEAN's Members.

In this respect, ASEAN's intentions to contribute to and "be part of the solution" to global challenges as part of the international community are particularly noteworthy.[85] At the April 2013 ASEAN Summit,[86] Member States reconfirmed their commitment to facilitate the region in addressing global issues of common interest, thereby assisting in strengthening regional and international collaboration, and confirmed their determination to strengthen cooperation in addressing terrorism and transnational crime as well as to effectively tackle increasing non-traditional security threats in the region.

The shared responsibility of the region for comprehensive security is delineated in the ASEAN Political-Security Blueprint[87] (Appendix 2 provides an overview of ASEAN cyber security related official documents). It envisages a cohesive, peaceful, stable, and resilient

[84] ASEAN, *Chairman's Statement of The 22nd ASEAN Summit - "Our People, Our Future Together",* 25 April 2013.

[85] ASEAN Secretariat, *Joint Statement by United Nations, Association of Southeast Asian Nations*, 11 October 2012.

[86] ASEAN, *Chairman's Statement of The 22nd ASEAN Summit - "Our People, Our Future Together",* 25 April 2013.

[87] ASEAN Secretariat, *ASEAN Political-Security Community Blueprint*, June 2009.

region with shared responsibility for comprehensive security. Under the principles of comprehensive security, a key purpose of ASEAN is to respond effectively to non-traditional security issues - trans-boundary challenges, trans-national crimes and all forms of threats. ICT, important for social development, is promoted under the ASEAN Socio-Cultural Community Blueprint.[88] In accordance with the Economic Community Blueprint,[89] it is intended that by 2015 ASEAN will become a single market and production base, a highly competitive economic region, and one that is fully integrated into the global economy. Its capacity as a global production centre or as a part of the global supply chain is to be enhanced and regional sourcing promoted by integrating industries across the region. Furthermore, its competitiveness in attracting foreign direct investment (FDI) and intra-ASEAN investment is to be further enhanced. Improving and ensuring the region's attractiveness as a single production and investment destination is a key ambition and FDI figures for the region, which is regarded as a "USD2.2 trillion engine of global economic growth",[90] show increases of 23 per cent from USD92 billion in 2010 to a "record" USD114 billion in 2011.[91]

In order to sustain such regional economic growth and competitiveness, the Economic Community Blueprint identifies the importance of creating a secure and connected information infrastructure,[92] and areas of cooperation include enhanced infrastructure and communications connectivity.[93] The higher probabilities of cross-border challenges

[88] ASEAN Secretariat, *ASEAN Socio-Cultural Community Blueprint*, June 2009.

[89] ASEAN Secretariat, *ASEAN Economic Community Blueprint*, January 2008.

[90] ASEAN Secretariat, *Joint Statement of the 4th ASEAN-US Leaders' Meeting*, 20 November 2012.

[91] ASEAN Secretariat, *Chairman's Statement of The 22nd ASEAN Summit - "Our People, Our Future Together",* 25 April 2013.

[92] ASEAN Secretariat, *ASEAN Economic Community Blueprint*, January 2008.

[93] Under the *Master Plan on ASEAN Connectivity*, ICT infrastructure includes fixed, mobile, and satellite communication networks and the Internet as well as the software supporting the development and operation of these communication networks.

and transnational crime resultant from such closer connectivity are recognised by the 2011 Master Plan on ASEAN Connectivity[94] (as well as the ASEAN ICT Masterplan 2015 (AIM2015))[95] in its underscoring of the premise that enhanced ASEAN connectivity is essential to achieve the ASEAN Community. However, although ASEAN and other regional organisations are undertaking efforts to fight cyber crime[96] by improving legal structures

---

Of note, the Master Plan on ASEAN Connectivity requests a feasibility study on the possibility of developing an ASEAN Single Telecommunications Market post-2015 in the context of free flow of products, investments and skilled human resources.

[94] ASEAN Secretariat, *Master Plan on ASEAN Connectivity*, January 2011.

[95] ASEAN Secretariat, *ASEAN ICT Masterplan 2015*, 10th ASEAN TELMIN, 2011.

AIM2015 charts the approach for ICT to 2015 in line with the ASEAN Community and underlines that ASEAN can achieve greater competitiveness and attract global investments if it leverages ICT collectively.

[96] The concept of cybercrime is defined within the Cybersecurity Strategy of the European Union (07 February 2013) as commonly referring to the broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. online distribution of child abuse material or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

Please consult: ASEAN Ministerial Meeting on Transnational Crime (AMMTC); ASEAN Senior Officials Meeting on Transnational Crime (SOMTC); ASEAN Declaration on Transnational Crime, 20 December 2007; ASEAN Plan of Action to Combat Transnational Crime, 23 June 1999; Work Programme to

and enhancing law enforcement cooperation[97] and while INTERPOL is setting up its Global Complex for Innovation in Singapore in 2014, contemporary cyber incidents and cyber related threats are still a relatively new and emerging common global threat which requires further solutions.

AIM2015 calls for the development of a common framework for network security,[98] the establishment of common minimum standards for network security to ensure a high level of preparedness and integrity of networks across ASEAN, a network security "health screening" programme for ASEAN to be implemented at regular intervals, the development of best practice models for business continuity and disaster recovery for all sectors, and the establishment of a multi-stakeholder ASEAN Network Security Action Council (ANSAC) to promote Computer Emergency Response Team (CERT) cooperation and sharing of expertise.

In line with AIM2015 and in acknowledging the increased frequency of information and network security activities, the ASEAN Ministers responsible for Telecommunications and

---

Implement the ASEAN Plan of Action to Combat Transnational Crime, 17 May 2002; 7th SOMTC, 26-27 June 2007, Adoption of a common framework for ASEAN cybercrime enforcement.

[97] James Lewis, CSIS, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia,* Prepared for the Lowy Institute MacArthur Asia Security Project, 07 March 2013.

James Lewis explains that while "cooperation among Asian countries in combating cybercrime may in some ways be easier to obtain than cooperation in other aspects of cyber security that are more closely linked to state power and competition, the utility of cybercrime as a proxy for pursuing state goals could also limit the scope of any agreement or compliance with it".

[98] Also note: The Framework for Cooperation on Network Security and Action Plan adopted at the 11th ATRC Meeting, 16-18 August 2005.

Information Technology agreed in November 2012, under the Mactan Cebu Declaration[99] to implement a number of measures. These include:

1) International and regional collaboration to enhance security of the ASEAN information infrastructure for "sustainable economic and social development".
2) Working towards a "conducive, safe, secured and trusted environment and harmonised ICT rules and regulations that will promote trade, investment and entrepreneurship".
3) Providing safe and secured fixed and mobile broadband.
4) Cooperating in the building and promotion of a secure online environment to enhance cyber security and counteract online threats within and among ASEAN Member States.
5) Facilitating robust and resilient information infrastructure through the development and implementation of National Frameworks on Submarine Cable Connectivity Protection and Risk Mitigation.
6) Further enhancing policy framework development, cooperation and sharing of best practices on data protection and the protection of information infrastructures to safeguard the network among Member States.
7) Continue collaboration among ASEAN CERTs such as the ASEAN CERTS Incident Drills so as to enhance incident investigation and coordination among CERTs in support of ANSAC's activities.

ASEAN Regional Forum

In this respect, although the ARF has no authority beyond that of ASEAN's,[100] the opportunity that this forum provides for an environment of open dialogue for three of the most advanced global cyber actors as ARF participants - the United States, Russia and China – is particularly noteworthy. The ARF's objectives, which include fostering constructive dialogue and consultation on political and security issues of common interest and concern, more recently include cyber security issues of common interest and concern.

[99] ASEAN, *Mactan Cebu Declaration Connected ASEAN: Enabling Aspirations*, 19 November 2012.

[100] Joshua Kurlantzick, Council on Foreign Relations, *ASEAN's Future and Asian Integration*, November 2012.

Furthermore, the forum promotes the role of ASEAN in the centrality of the regional architecture, contributes to future regional security architecture, and serves as a platform for countries in the region to deal with challenges in the security environment.

At the 19th ASEAN Regional Forum of 12 July 2012,[101] the Foreign Ministers of the ARF participants underscored the need to foster coordination to ensure security for the use of ICT, an ARF *Statement on Cooperation in Ensuring Cyber Security* was adopted, and agreement made to develop an ARF Work Plan relating to cyber security. In addition, the forum has hosted a number of workshops on cyber security matters such as proxy actors, cyber incident responses, and confidence-building measures in cyberspace.[102]

IV. Moving Towards a Resilient Cyber Security Regime in ASEAN: Several Recommendations for Consideration

In order to achieve a more resilient architecture for ASEAN-wide cyber security, Member States should develop and implement as soon as possible a comprehensive forward-looking cyber security framework (plus plan of action) to coordinate cohesive regional cooperation and collectively tackle common global cyber security challenges.

Such a framework should be published openly for purposes of transparency and provision should be made for regular review and updating of agreed measures and plans to

---

[101] ASEAN Regional Forum, *Chairman's Statement of the 19th ASEAN Regional Forum*, Cambodia, 12 July 2012.

- *ARF Statement on Cooperation in Ensuring Cyber Security* appears as Annex 4.
- Also of note: *ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space*, 28 July 2006.

[102] ARF Workshop on Proxy Actors in Cyberspace, 14-15 March 2012; ARF Workshop on Cyber Incident Response, 6-7 September 2012; ARF Seminar on Confidence-building Measures in Cyberspace, 11-12 September 2012.

incorporate the principles of flexibility, adaptability, timely implementation, and strategic foresight. Since the nature of the threat environment is in constant flux, an inflexible framework with fixed work plans and work programmes might not be sufficiently effective.

A Comprehensive, Multi-pronged Cyber Security Framework: Several Measures and Tools for Consideration

A non-exhaustive set of possible measures are proposed as elements of the wider comprehensive framework in order to address common global cyber security challenges and fill several gaps identified in the preceding sections. These include:

- Establish a Permanent Coordinating Mechanism: Regional Coordination & Information Sharing
- Establish a Robust ASEAN-CERT: Further Enhancing and Strengthening National CERTs' Operational Cooperation & Information Sharing
- Ensure Adequate Security of the ASEAN Secretariat
- Create a Cyber Security Hub of Excellence in the Region: Training & Capacity Building
- Ensure a Secure Supply Chain & Regional Harmonisation of International Standards: A "Cyber-Secured Zone"
- Increase Public Awareness & Civil Liberties' Protection: Engaging Citizens
- Enhance Defence Cooperation & Law Enforcement Authorities' Coordination for Cyber Related Threats
- Agree a Common Position on Responsible State Behaviour and Applicability of International Law
- Further Strengthen International Cooperation

Although ultimately the wider purpose of a comprehensive framework including its proposed measures is the creation of a more resilient regional architecture for cyber security, given the inherent limitations of ASEAN it is worth considering that those measures which complement the aims of the ASEAN Economic Community and ASEAN

Socio-Cultural Community are perhaps more likely to be attained in the shorter term vis-à-vis the more politically sensitive measures.

1. *Establish a Permanent Coordinating Mechanism: Regional Coordination & Information Sharing*

At a minimum and in the shorter term, a rotating coordinator could be appointed to support a network of national points of contact established to ensure the timely and proper implementation of agreed action plans and work programmes as well as to prevent possible cyber related misunderstandings. The feasibility of establishing a permanent coordinating mechanism such as a committee or network to ensure functional coordination and cooperation in enhancing cyber security (possibly constituting Member State representatives from each of the ten members to abate concerns that control might be ceded) should be explored. This mechanism could possibly function as a stand-alone mechanism, either within the ASEAN Secretariat or a more robust regional CERT. It could serve to assist cooperative work on cyber security, to serve as a network for agencies and bodies within the region to exchange policy experience, to assist in information sharing outside of traditional CERT operational cooperation, to provide training and research to Member States when requested, and to coordinate pan-ASEAN and international cyber security exercises as well as tabletop exercises.

Such a mechanism can support ASEAN Member States in possibly establishing a regional high-level working group in line with the multi-stakeholder model. This working group should include foreign affairs, defence, justice, trade, science /technology, ICT, transport, and energy government officials as well as industry, academia, civil society, and law enforcement authorities (Track 1.5 ARF Experts and Eminent Persons (EEPS) Meetings and

the CSCAP working group on cyber security[103] can assist by producing further recommendations).[104]

It should be noted that although ANSAC's inaugural meeting was held on 05 June 2012 and a second meeting in June 2013, its activities are not yet sufficient nor do they seem to be developing at a fast enough pace to seriously tackle cross-border cyber threats.[105]

2. *Establish a Robust ASEAN-CERT: Further Enhancing and Strengthening National CERTs' Operational Cooperation & Information Sharing*

Under the Singapore Declaration, it was decided that all ASEAN Member States develop and operationalise national CERTs by 2005, in line with mutually agreed minimum performance criteria.[106] The Lao Computer Emergency Response Team (LaoCERT), which

[103] CSCAP Memorandum No. 20, *Ensuring a Safer Cyber Security Environment – A Memorandum from the Council for Security Cooperation in the Asia Pacific (CSCAP),* May 2012.

[104] A similar platform to the European Forum for Member States, which was launched to foster discussions among public authorities regarding good policy practices on security and resilience of critical information infrastructure could also be considered.

[105] By comparison, ENISA (http://www.enisa.europa.eu/) is engaged as a facilitator for EU Member States to support the exchange of good practices in cyber security by recommending how to develop, implement, and maintain a cyber security strategy. It has a supportive role in national cyber security strategies, national contingency plans, and development of scenarios for national exercises. Furthermore, under the more recent proposals of the EU Cybersecurity Strategy, the European Commission requests ENISA to assist EU Member States in developing strong national cyber resilience capabilities by building expertise on security and resilience of industrial control systems as well as transport and energy infrastructure. The Commission also requests ENISA to examine in 2013 the feasibility of Computer Incident Response Team(s) for Industrial Control Systems for the EU.

[106] Singapore Declaration, 3rd TELMIN 2003.

was established in February 2012, is the last of the ten Member States' national CERTs to be established[107] (Appendix 3 provides an overview of ASEAN national CERTs).

Operational cooperation, often informal, between national CERTs has been somewhat easier to achieve in past experience, and in crisis situations, cooperation at the CERT-to-CERT level can prove invaluable for response measures. CERT-to-CERT cooperation should therefore be further enhanced and since national CERTs across the ASEAN region vary in levels of development, Member States should consider developing their robustness. Furthermore, the feasibility of setting up an ASEAN-CERT to facilitate region-wide coordination and cooperation for its national CERTs, to enhance information exchange and real time response to cyber incidents, and to assist existing international operational cooperation with for example the Asia Pacific Computer Emergency Response Team (APCERT[108]) and CERT-EU,[109] either by way of a formal memorandum of understanding or informal cooperation, could be considered. Whether an even more robust and developed regional CERT could possibly undertake the functions delineated above for a permanent coordinating mechanism, and perhaps be more suited, could also be explored.

[107] http://www.laocert.gov.la/en/Page-1-, last accessed 14 August 2013.

[108] APCERT is a group of over thirty CERTs in operational cooperation, which assists other CERTs in the Asia Pacific region, jointly develops measures to deal with large-scale or regional network security incidents, facilitates information sharing and technology exchange and promotes collaborative research and development.

[109] CERT-EU was permanently established in September 2012 with responsibility for the security of the IT systems of the EU institutions, agencies and bodies, and for cooperation with EU Member States' National CERTs.

3. Ensure Adequate Security of the ASEAN Secretariat

The ASEAN Secretariat has been victim to intrusions such as the infamous Operation Shady RAT,[110] which began in October 2006, a month before the ASEAN summit in Singapore and continued for another ten months. A more recent emerging trend, which should concern the Secretariat, the ARF Unit at the Secretariat and ASEAN Members, is the use of organisations as "watering holes". Symantec's Internet Security Threat Report for 2013[111] identifies the watering hole attack as one of the most important trends in 2012. It explains how an organisation, irrespective of whether it might hold significant classified and sensitive information since it is not the real target, can be used in a targeted attack – a "watering hole" - where the website (such as the ASEAN website) is hijacked and used to infect the real target (such as Member State organs or specifically targeted individuals) when visiting the site in order to leverage the weaker security of one entity to defeat the stronger security of another. In December 2012 for example, the Council on

[110] As have the Vietnamese government and victims in Singapore.

Dmitri Alperovitch, Vice-President, Threat Research, McAfee, *Revealed: Operation Shady RAT*, White Paper, 2011.

Operation Shady RAT (RAT is an acronym for Remote Access Tool): The compromises were standard procedure for these types of targeted intrusions: a spear phishing email containing an exploit is sent to an individual with the right level of access at the company, and the exploit, when opened , on an unpatched system will trigger a download of the implant malware. That malware will execute and initiate a backdoor communication channel to the C&C web server and interpret the instructions encoded in the hidden comments embedded in the webpage code. This will quickly be followed by live intruders jumping on to the infected machine and proceeding to quickly escalate privileges and move laterally within the organisation to establish new persistent footholds via additional compromised machines running implant malware, as well as targeting for quick exfiltration the key data for which they came.

[111] Symantec, *Internet Security Threat Report 2013, 2012 Trends*, Volume 18, April 2013.

Foreign Relations and Capstone Turbine Corporation were targeted in this fashion using a zero-day vulnerability in Microsoft's Internet Explorer web browser to compromise the computers of individuals visiting their websites.[112]

Member States should therefore ensure that the ASEAN Secretariat (and the ARF Unit) determine the level of attacks against their systems, ensure cyber security resilience, and train its staff[113] on cyber security.

4. *Create a Cyber Security Hub of Excellence in the Region: Training & Capacity Building*

Member States should encourage and stimulate the creation of a global cyber security hub of excellence in tandem with and in support of AIM2015 visions to create a global ICT hub in the region and ASEAN's intentions to distinguish itself as a region of high quality ICT infrastructure, skilled manpower and technological innovation. In doing so, not only will Member States increase the attractiveness of the region for FDI and enhance competitiveness in line with aims for the ASEAN Economic Community (ICT is regarded as a growth industry sector for the region, employing more than 11.7 million and contributing more than USD32 billion to ASEAN's GDP with figures due to increase by 2015[114]), but they will also reduce the crucial skills gap which is of serious concern to most states across the international community in their countering of cyber incidents and enhancing of cyber security. Furthermore, in accordance with the social development

[112] James Lewis, Centre for Strategic and International Studies (CSIS), *List of Significant Cyber Incidents Since 2006*, last updated 14 May 2013.

[113] The 2012 European Parliament Committee on Foreign Affairs Report recommendation for annual cyber exercises for staff of the European institutions similar to existing emergency exercises could also be considered by the ASEAN Secretariat [European Parliament, Committee on Foreign Affairs, *Draft Report on Cyber Security and Cyber Defence (2012/2096(INI),* 22 June 2012].

[114] ASEAN Secretariat, *ASEAN ICT Masterplan 2015*, 2011.

goals of the ASEAN Community as well as Millennium Development Goals for local economic and social development in the region, these initiatives will address the development divide, help alleviate poverty, and create employment opportunities.

Investment in R&D and innovation should therefore be increased, cooperation strengthened between Member States and collaboration with the private sector encouraged for enhanced cyber security. Congruent with ASEAN aims to develop a workforce with high level ICT proficiency, Member States should implement parallel measures to build a cadre of cyber security professionals. Instruments to achieve these aims include *inter alia*:

- cyber security scholarships (like those proposed under the Mactan Cebu Declaration and AIM2015 for the creation of an ASEAN ICT Scholarship programme to attract ICT talent);
- the education of ICT and cyber security issues at the earliest possible age and incorporation into school curricula;
- the further development of "ASEAN Cyberkids Camp";
- initiatives to encourage and attract talent to choose ICT as a career;
- harnessing cyber security professionals from the database of ICT experts called for under AIM2015; and finally
- accrediting IT and cyber security professionals with a regionally recognised certification. ASEAN has completed eight Mutual Recognition Arrangements (MRAs) to facilitate the free movement of skilled labour in the region, albeit to varying degrees of cooperation in recognition of qualifications.[115] Although engineering services are included, computer scientists/IT professionals are not within the eight professional groups.

Cost effective, community-driven initiatives like CoderDojo,[116] which is a global movement with more than 15,000 children learning to write software in more than 35 countries,

[115] ASEAN Secretariat, *Master Plan on ASEAN Connectivity*, January 2011.

[116] CoderDojo (http://coderdojo.com/) is a not-for-profit organisation founded by James Whelton and Bill Liao. It was first started in James Whelton's school in early 2011 when James received some publicity

should also be considered, particularly where financial and manpower resource constraints exist. Currently, there is one CoderDojo in the ASEAN region (CoderDojo Bandung in Indonesia), five in India, and eight in Japan running free not-for-profit coding clubs and regular sessions for young people to learn how to code, develop websites, apps, and programs in a fun environment. Fun initiatives are important to reach levels such as those in China where indicators show that one out of three school children wants to be a "hacker" when they grow up – hackers are the new cool, the new rock star[117] - and 43 per cent of elementary students "adore" China's hackers.[118] Finally, with respect to social development goals, the CoderDojo focus on girls and women in technology at DojoCon2013 in April 2013 is particularly noteworthy for the ASEAN region.

In this regard, it is worth considering the European Commission's plans under the EU Cybersecurity Strategy to organise in 2014, with the support of ENISA, a "cyber security championship" where university students will compete in proposing network and information security solutions, its recent request for ENISA to propose in 2013 a roadmap for a "Driving Licence" as a voluntary certification programme to promote enhanced skills, and finally, in order to stimulate a culture of security and data privacy by design, the Commission recommends the introduction of training on network and information

---

after hacking the iPod Nano and some younger students expressed an interest in learning how to code. He setup a computer club in his school (PBC Cork) where he started teaching basic HTML and CSS. Later that year he met Bill Liao, an entrepreneur and philanthropist, who was interested in growing the project into something bigger than just an after-school computer club. In June 2011 the first CoderDojo was launched in the National Software Centre in Cork where CoderDojo saw extreme success. The Cork Dojo saw people travelling from Dublin frequently to attend sessions. Owing to this popularity a Dublin Dojo was launched soon after in Google's Montevetro building.

[117] Kah-Kin Ho, Head of Cyber Security Business Development, Threat Research, Intelligence and Development, Cisco, *Cyber Security: The Strategic Review*, Cisco Defence and National Security Summit 2013, 16 May 2013.

[118] MS Risk, *Chinese Hacking Report Released*, 23 February 2013, http://www.msrisk.com/china/chinese-hacking-report-released/, last accessed 03 June 2013, [Reference to the Shanghai Academy of Social Sciences 2005 survey].

security, secure software development, and personal data protection for computer science students.

5. *Ensure a Secure Supply Chain & Regional Harmonisation of International Standards: A "Cyber-Secured Zone"*

In the interests of ASEAN-wide cyber security and aims for a single market and production base as well as the enhancing of ASEAN intentions to become a global production centre or part of the global supply chain, it is essential that quality assurance and guarantee be provided that the supply chain (from design to production to delivery) is secure and standards harmonised in line with international cyber security standards. ASEAN Member States could therefore consider[119] creating a cyber-secured zone for the supply chain of products designed and manufactured within the region in order to ensure regional cyber security, to promote trade, to enhance the region's competitiveness, and to increase its attractiveness for intra-ASEAN investment and FDI as a single investment destination. In addition, Members could consider developing a regional guideline by adopting guidelines on international standards and best practices in accordance with the intentions of the ASEAN Economic Community (i.e. extra-ASEAN rules and regulations should be taken into account when developing policies to facilitate its competing internationally, support its aims to make the region a strong segment of the global supply chain, and ensure that the single market is attractive to FDI in the region). Finally, it is equally essential that a mechanism be established to ensure that hardware and software imported from outside the region is secure.

[119] It is also worth considering that it is highly likely that consumers will in future expect, if not demand, an assurance of such high-level security. Certification, or similar mechanism, should therefore be created for products and companies which adhere to the region's cyber security regulations and standards.

In this regard it is worth noting the European Commission has made a proposal to examine how providers of hardware and software could inform national authorities of detected vulnerabilities that could have significant security implications.[120]

6. Increase Public Awareness & Civil Liberties' Protection: Engaging Citizens

First, while recommended actions under AIM2015 include an outreach campaign to promote public awareness of cyber security through education about online security, further measures need to be employed in order to increase awareness among end-users. For instance, ASEAN could consider synchronising a region-wide "cyber security month" like that proposed for the EU from 2013 onwards and the EU-US Cybersecurity Month which will be organised from 2014.

Second, a balance between security initiatives and civil liberties must be ensured. Citizens' buy-in and loyalty as well as cooperation with the public sector are essential for fully functioning cyber security strategies. While the ASEAN Charter and more recent commitments under the Bali Concord III to respect and protect human rights and fundamental freedoms go some way to protecting civil liberties, if fundamental rights such as the rights to freedom of expression and association, the rights to data privacy and data protection (AIM2015 specifically calls for ensuring personal data protection), and the right of access to Internet are not responsibly managed by public authorities it could lead to a potential and possibly very serious flashpoint. Government transgression, including perceived wrongdoing, could be construed negatively and sometimes in the extreme, and could possibly cause backlash whether by physical protest, disruptive cyber incidents by personally empowered citizens or a combination of both. Such disruptive cyber incidents can either emanate from within the state held to be responsible or from outside its own

[120] European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final),* 07 February 2013.

borders. Mission creep should therefore be avoided and clear assurance provided to the public that it is not going to occur.

7. *Enhance Defence Cooperation & Law Enforcement Authorities' Coordination for Cyber Related Threats*

Coordination and cooperation among law enforcement authorities across the region and with third countries as well as Europol and INTERPOL should be strengthened. Given the unique nature of cyber threats, civil-military coordination should also be considered. At the 6th ASEAN Defence Ministers' Meeting (ADMM) in May 2012, the Minister of Defence for Malaysia, Datuk Seri Dr Ahmad Zahid Hamidi, reportedly said that it is crucial for the Defence Ministers to work together to restrain cyber threats for the sake of peace and stability of the region,[121] and in June 2012 he argued that with the increasing sophistication of cyber threats, national efforts to protect their networks might be left wanting.[122] Whether this might therefore be the right time to signal stronger collaboration in cyber defence among ASEAN members was discussed at the ADMM in May 2012 and the possible development of an "ASEAN master plan of security connectivity" was suggested.[123] However, these issues have not been fully discussed and a Defence White Paper on offensive cyber capabilities and techniques should at a minimum be published. Furthermore, those Member States, which do not yet have a cyber security and cyber

[121] New Straits Times, *ASEAN must tackle cyber security threat*, 31 May 2012.

[122] Shangri-La Dialogue, IISS, *New Forms Of Warfare - Cyber, UAVs And Emerging Threats: Dato' Seri Dr Ahmad Zahid Hamidi*, http://www.iiss.org/en/events/shangri%20la%20dialogue/archive/sld12-43d9/fourth-plenary-session-1353/dato-seri-dr-ahmad-zahid-hamidi-b13b, 03 June 2012, last accessed 22 August 2013.

[123] Shangri-La Dialogue, IISS, *New Forms Of Warfare - Cyber, UAVs And Emerging Threats: Dato' Seri Dr Ahmad Zahid Hamidi*, http://www.iiss.org/en/events/shangri%20la%20dialogue/archive/sld12-43d9/fourth-plenary-session-1353/dato-seri-dr-ahmad-zahid-hamidi-b13b, 03 June 2012, last accessed 22 August 2013.

defence unit within their military structure, should consider establishing a unit as soon as possible.

8. *Agree a Common Position on Responsible State Behaviour and Applicability of International Law*

Member States should agree on a common position regarding shared norms for responsible state behaviour and the applicability of international law for the use of advanced cyber capabilities and techniques. Positions should be coordinated to promote ASEAN values and policies and a common ASEAN position or at minimum a common position paper, agreed to reflect ASEAN's views in regional and international fora such as the G20 Summit and Seoul Cyberspace Convention in October 2013.

In addressing non-traditional security issues, the ASEAN Political-Security Community promotes the renunciation of aggression and of the threat or use of force or other actions in any manner inconsistent with international law.[124] Although, unlike nuclear weapons, it is impossible to prevent the creation of advanced cyber capabilities, possible agreements can instead focus on their use by agreeing to not use advanced cyber capabilities for destructive attacks in the region. Confidence building measures and preventive diplomacy such as exchanges among defence and military officials on cyber related threats should also be enhanced to ensure escalation does not occur between ASEAN States or between ASEAN Member States and third countries. Such instruments should aim to prevent conflict and ensure that the chances of mistake, miscalculation and misinterpretation are lessened.

[124] ASEAN Secretariat, *ASEAN Political-Security Community Blueprint*, June 2009.

9. Further Strengthen International Cooperation

ASEAN Member States should continue further strengthening relations with ASEAN Dialogue Partners and the international community on cyber security issues. Joint ASEAN-EU and ASEAN-EAS working groups could for example be established to deal with cross-border cyber challenges. The Asia-Europe Meeting (ASEM), whose partners include the ten ASEAN States, 27 EU Member States, the ASEAN Secretariat, and the European Commission (among other partner nations), could explore these issues of common concern in an open and informal fashion in order to complement bilateral and multilateral cooperation efforts, to discuss ways to enhance cyber security cooperation and to host working groups to include the private sector and civil society.

V. Conclusion

While there is no one-size-fits-all approach for this developing area, not only is it in the common interests of ASEAN Members to adopt a regional comprehensive and multi-pronged framework for cyber security to tackle serious cross-border cyber related threats, such measures would also benefit the region, wider regional efforts, and the international community.

In the words of the Master Plan on ASEAN Connectivity, they would "foster a win-win solution to reflect the interest of all ASEAN Member States". Furthermore, they would support ASEAN's ambitions to create a successful single market and production base, complement ASEAN connectivity, and assist in negotiations with dialogue partners from the wider Asia Pacific region where plans might include integrated intermodal transport or energy networks such as gas pipelines or railway links.

In accordance with the Bali Concord III,[125] these measures would further enhance ASEAN's common position in multilateral fora, and finally, in line with the 22nd ASEAN Summit of April 2013[126] they would support the region's integration efforts both in the lead up to 2015 and in the longer term, post-2015, while also strategically enhancing ASEAN's position in the evolving regional architecture and supporting current and future international cooperation as well as national efforts on cyber security that are required to deal effectively with the cross-border nature of serious cyber incidents.

Governments and institutions will in future be required to adapt quickly, to preempt incidents, and to foresee emerging trends. Therefore, in order to avoid becoming overwhelmed by these changes, this paper envisages a closer embracing of cyber related challenges by ASEAN and its Member States through the adoption of new structures and novel ways of thinking.

[125] ASEAN, *Bali Declaration on ASEAN Community in a Global Community of Nations "Bali Concord III",* 19th ASEAN Summit, 17 November 2011.

[126] ASEAN, *Chairman's Statement of The 22nd ASEAN Summit - "Our People, Our Future Together",* 25 April 2013.

Appendix 1

Overview: Cyber Incidents in the ASEAN Region (non-exhaustive)

For the Period January 2012-Present (last updated 21 August 2013)

ASEAN M/S	Nature of Cyber Incident	Month/Year
Brunei Darussalam	IT Protective Security Services (ITPSS) recorded more than 2,000 cyber attacks for the period 2010-2012 (62% virus attacks, 26% spam, 7% defacement and 4% scams.[127]	November 2012
Cambodia	A group of hackers called Nullcrew attacked Cambodian websites to protest Internet censorship and the arrest of Gottfrid Svartholm Warg (co-founder of The Pirate Bay). Nullcrew announced that its campaign would target Cambodian businesses and government including the armed forces and posted passwords for other hacktivists' use.[128]	September 2012
	Websites of Cambodia's National Military Police and Supreme Court were hacked. An Indonesian hacker called "Hmei7" claimed responsibility for the National Military Police attack but no attribution could be made for the attack on the Supreme Court's website. The Cambodian government has been subject to multiple cyber attacks in the past, including one in which Anonymous stole and leaked over 5,000 documents from the Ministry of Foreign Affairs.[129]	January 2013
Indonesia	A group called Anonymous Indonesia defaced more than twelve	January 2013

[127] http://www.bt.com.bn/news-national/2012/11/10/internet-users-cautioned-over-rise-cyber-attacks

[128] https://citizenlab.org/2012/09/southeast-asia-cyberwatch-september-2012/

[129] https://citizenlab.org/2013/01/southeast-asia-cyberwatch-january-2013/

	government websites following the arrest of Wildan Yani Ashair who was accused of hacking the President's website. In three years, Government websites have been attacked over 36.6 million times.[130]	
	Serious online fraud schemes involving losses of over USD500,000 accounted for 40% of 176 cybercrime cases reported for the first four months of 2013.[131]	April 2013
Lao PDR		
Malaysia	Police recorded 24 cases of hacking between January and September 2012 with estimated losses of USD1.1 million.[132]	November 2012
	Hackers posted a statement on the Department of Information website that Prime Minister Datuk Seri Najib Tun Razak was resigning.[133]	February 2013
	Alternative radio stations for the opposition and the news portal Sarawak Report claimed to be targeted by DDoS attacks. A FinSpy sample — part of the remote intrusion and surveillance software FinFisher distributed by Gamma International — appears to be specifically targeting Malay language speakers.[134]	March 2013
Myanmar	The Information Ministry website was defaced warning the Government to stop killing Muslims.[135]	August 2012
	Anonymous announced a new campaign to support the Muslim	May 2013

[130] https://citizenlab.org/2013/01/southeast-asia-cyberwatch-january-2013/

[131] https://citizenlab.org/2013/01/southeast-asia-cyberwatch, April 2013.

[132] https://citizenlab.org/2013/02/southeast-asia-cyberwatch, November 2012.

[133] https://citizenlab.org/2013/02/southeast-asia-cyberwatch, February 2013.

[134] https://citizenlab.org/2013/02/southeast-asia-cyberwatch, March 2013.

[135] https://citizenlab.org/2013/02/southeast-asia-cyberwatch, August 2012.

	Rohingya community focusing on government sites, the UN (for not involving itself with peacekeeping operations), and Aung San Suu Kyi over her lack of action regarding anti-Rohingya violence.[136]	
	Eleven Media was defaced by the Blink Hacker Group (http://www.blinkhackergroup.org/) in response to an editorial condemning hate speech. The group has also attacked pro-Rohingya sites in relation to violence between the Muslim Rohingya people and Buddhists in Myanmar's Rakhine state.[137]	June 2013
Philippines	Alleged defacements of several government websites by Chinese hackers related to the South China Sea dispute. Philippine hackers retaliated by launching similar attacks against Chinese websites.[138]	June 2012
	Anonymous Philippines hacked the President's website for "mishandling" the Sabah conflict accusing the Government of allowing Malaysian troops to kill Filipino citizens.[139]	March 2013
	Anonymous Philippines attacked prominent commercial entities, civil society organisations, and government in protest over the contentious Cybercrime Act.[140]	September 2012
	After the Philippine Coast Guard shot a Taiwanese fishing boat, Taiwanese and Filipino hackers conducted a "cyber battle" using the Taiwanese and Philippine government websites. A	May 2013

[136] https://citizenlab.org/2013/02/southeast-asia-cyberwatch, May 2013.

[137] https://citizenlab.org/2013/02/southeast-asia-cyberwatch, June 2013.

[138] https://citizenlab.org/2013/04/southeast-asia-cyberwatch, June 2012.

[139] https://citizenlab.org/2013/04/southeast-asia-cyberwatch, March 2013.

[140] https://citizenlab.org/2013/04/southeast-asia-cyberwatch, September 2012.

	Taiwanese group, Anon TAIWAN, claimed responsibility for the releasing DNS information of Filipino government websites on Pastebin, a text sharing website.[141]	
Singapore	A report by Trend Micro Smart Protection Network showed that more than 900 Singapore citizens were victim to online banking fraud in the first quarter of 2013.	May 2013
Thailand	The Turkish Agent Hacker Group compromised McDonald's Thailand releasing the contact information of 2,000 users. The same group claimed responsibility for an attack on the Red Cross Thailand website protesting disrespect the Prophet Mohammad accompanied with a Turkish flag. The group previously defaced the website of Pepsi Hungary with the same message.[142]	October 2012
	From January to May 2013, there were 1,475 intrusions into government sites, and hundreds of malware attacks and phishing incidents.[143]	June 2013
Vietnam	The Vietnamese version of Baidu, a Chinese search engine company, apparently infected computers with spyware and adware so that once downloaded compromised computers can be controlled remotely, data extracted, and computers used as "zombies" for DDoS attacks.[144]	July 2012

[141] https://citizenlab.org/2013/05/southeast-asia-cyberwatch-may-2013/

[142] https://citizenlab.org/2013/07/southeast-asia-cyberwatch, October 2012.

[143] https://citizenlab.org/2013/07/southeast-asia-cyberwatch, June 2013.

[144] https://citizenlab.org/2013/07/southeast-asia-cyberwatch, July 2012.

Appendix 2

Overview: ASEAN Cyber Security Related Official Documents as at 29 July 2013

Statements

1.	ASEAN Secretariat, *Chairman's Statement of The 22nd ASEAN Summit - "Our People, Our Future Together",* 25 April 2013

Action Plans/Work Plans/Frameworks

1.	ASEAN Secretariat, Master Plan on ASEAN Connectivity, January 2011
2.	ASEAN Secretariat, *ASEAN ICT Masterplan 2015 (AIM)*, 2011
3.	ASEAN Secretariat, *ASEAN Political-Security Community Blueprint*, June 2009
4.	ASEAN Secretariat, *ASEAN Socio-Cultural Community Blueprint*, June 2009
5.	ASEAN Secretariat, *ASEAN Economic Community Blueprint*, January 2008
6.	ASEAN, *Initiative for ASEAN Integration (IAI) Strategic Framework and IAI Work Plan 2 (2009-2015)*
7.	The Framework for Cooperation on Network Security and Action Plan adopted at the 11th ATRC Meeting, 16-18 August 2005

Declarations

1.	ASEAN, *Mactan Cebu Declaration Connected ASEAN: Enabling Aspirations*, 19 November 2012
2.	ASEAN, *Bali Declaration on ASEAN Community in a Global Community of Nations "Bali Concord III",* 19th ASEAN Summit, 17 November 2011
3.	*Singapore Declaration*, 3rd TELMIN 2003

Appendix 3

Overview: ASEAN Member States' National Computer Emergency Response Teams (CERTs) as at 21 August 2013

ASEAN Member State	CERT	Website	Year Operations Established
Brunei Darussalam	*BruCERT* Brunei National Computer Emergency Response Team	http://www.brucert.org.bn/	2004
Cambodia	*CamCERT* National Cambodia Computer Emergency Response Team	http://www.camcert.gov.kh/	2008
Indonesia	*ID-CERT* Indonesia Computer Emergency Response Team	http://www.cert.or.id/	1998
Laos	*LaoCERT* Lao Computer Emergency Response Team	http://www.laocert.gov.la/en/Page-1-	2012[145]
Malaysia	MyCERT Malaysia Computer Emergency Response Team	http://www.mycert.org.my/en/	1997
Myanmar	mmCERT Myanmar Computer Emergency Response Team	http://www.mmcert.org.mm	2004
Philippines	*PHCERT* Philippine Computer	http://www.phcert.org/	

[145] LaoCERT is currently under the Lao National Internet Center (LANIC). It is due to become an independent centre under the Ministry of Post and Telecommunications in early 2014.

	Emergency Response Team *GCSIRT* Government Computer Security and Incident Response Team		2004
Singapore	*SingCERT* Singapore Computer Emergency Response Team	http://www.singcert.org.sg/	1997
Thailand	*ThaiCERT* Thailand Computer Emergency Response Team	https://www.thaicert.or.th/	2000
Vietnam	*VNCERT* Vietnam Computer Emergency Response Team	http://www.vncert.gov.vn	2005

RSIS Working Paper Series

1.	Vietnam-China Relations Since The End of The Cold War *Ang Cheng Guan*	(1998)
2.	Multilateral Security Cooperation in the Asia-Pacific Region: Prospects and Possibilities *Desmond Ball*	(1999)
3.	Reordering Asia: "Cooperative Security" or Concert of Powers? *Amitav Acharya*	(1999)
4.	The South China Sea Dispute re-visited *Ang Cheng Guan*	(1999)
5.	Continuity and Change In Malaysian Politics: Assessing the Buildup to the 1999-2000 General Elections *Joseph Liow Chin Yong*	(1999)
6.	'Humanitarian Intervention in Kosovo' as Justified, Executed and Mediated by NATO: Strategic Lessons for Singapore *Kumar Ramakrishna*	(2000)
7.	Taiwan's Future: Mongolia or Tibet? *Chien-peng (C.P.) Chung*	(2001)
8.	Asia-Pacific Diplomac*ies:* Reading Discontinuity in Late-Modern Diplomatic Practice *Tan See Seng*	(2001)
9.	Framing "South Asia": Whose Imagined Region? *Sinderpal Singh*	(2001)
10.	Explaining Indonesia's Relations with Singapore During the New Order Period: The Case of Regime Maintenance and Foreign Policy *Terence Lee Chek Liang*	(2001)
11.	Human Security: Discourse, Statecraft, Emancipation *Tan See Seng*	(2001)
12.	Globalization and its Implications for Southeast Asian Security: A Vietnamese Perspective *Nguyen Phuong Binh*	(2001)
13.	Framework for Autonomy in Southeast Asia's Plural Societies *Miriam Coronel Ferrer*	(2001)
14.	Burma: Protracted Conflict, Governance and Non-Traditional Security Issues *Ananda Rajah*	(2001)
15.	Natural Resources Management and Environmental Security in Southeast Asia: Case Study of Clean Water Supplies in Singapore *Kog Yue Choong*	(2001)
16.	Crisis and Transformation: ASEAN in the New Era *Etel Solingen*	(2001)
17.	Human Security: East Versus West? *Amitav Acharya*	(2001)

18.	Asian Developing Countries and the Next Round of WTO Negotiations *Barry Desker*	(2001)
19.	Multilateralism, Neo-liberalism and Security in Asia: The Role of the Asia Pacific Economic Co-operation Forum *Ian Taylor*	(2001)
20.	Humanitarian Intervention and Peacekeeping as Issues for Asia-Pacific Security *Derek McDougall*	(2001)
21.	Comprehensive Security: The South Asian Case *S.D. Muni*	(2002)
22.	The Evolution of China's Maritime Combat Doctrines and Models: 1949-2001 *You Ji*	(2002)
23.	The Concept of Security Before and After September 11 a. The Contested Concept of Security *Steve Smith* b. Security and Security Studies After September 11: Some Preliminary Reflections *Amitav Acharya*	(2002)
24.	Democratisation In South Korea And Taiwan: The Effect Of Social Division On Inter-Korean and Cross-Strait Relations *Chien-peng (C.P.) Chung*	(2002)
25.	Understanding Financial Globalisation *Andrew Walter*	(2002)
26.	911, American Praetorian Unilateralism and the Impact on State-Society Relations in Southeast Asia *Kumar Ramakrishna*	(2002)
27.	Great Power Politics in Contemporary East Asia: Negotiating Multipolarity or Hegemony? *Tan See Seng*	(2002)
28.	What Fear Hath Wrought: Missile Hysteria and The Writing of "America" *Tan See Seng*	(2002)
29.	International Responses to Terrorism: The Limits and Possibilities of Legal Control of Terrorism by Regional Arrangement with Particular Reference to ASEAN *Ong Yen Nee*	(2002)
30.	Reconceptualizing the PLA Navy in Post – Mao China: Functions, Warfare, Arms, and Organization *Nan Li*	(2002)
31.	Attempting Developmental Regionalism Through AFTA: The Domestics Politics – Domestic Capital Nexus *Helen E S Nesadurai*	(2002)
32.	11 September and China: Opportunities, Challenges, and Warfighting *Nan Li*	(2002)
33.	Islam and Society in Southeast Asia after September 11 *Barry Desker*	(2002)

34.	Hegemonic Constraints: The Implications of September 11 For American Power *Evelyn Goh*	(2002)
35.	Not Yet All Aboard…But Already All At Sea Over Container Security Initiative *Irvin Lim*	(2002)
36.	Financial Liberalization and Prudential Regulation in East Asia: Still Perverse? *Andrew Walter*	(2002)
37.	Indonesia and The Washington Consensus *Premjith Sadasivan*	(2002)
38.	The Political Economy of FDI Location: Why Don't Political Checks and Balances and Treaty Constraints Matter? *Andrew Walter*	(2002)
39.	The Securitization of Transnational Crime in ASEAN *Ralf Emmers*	(2002)
40.	Liquidity Support and The Financial Crisis: The Indonesian Experience *J Soedradjad Djiwandono*	(2002)
41.	A UK Perspective on Defence Equipment Acquisition *David Kirkpatrick*	(2003)
42.	Regionalisation of Peace in Asia: Experiences and Prospects of ASEAN, ARF and UN Partnership *Mely C. Anthony*	(2003)
43.	The WTO In 2003: Structural Shifts, State-Of-Play And Prospects For The Doha Round *Razeen Sally*	(2003)
44.	Seeking Security In The Dragon's Shadow: China and Southeast Asia In The Emerging Asian Order *Amitav Acharya*	(2003)
45.	Deconstructing Political Islam In Malaysia: UMNO'S Response To PAS' Religio-Political Dialectic *Joseph Liow*	(2003)
46.	The War On Terror And The Future of Indonesian Democracy *Tatik S. Hafidz*	(2003)
47.	Examining The Role of Foreign Assistance in Security Sector Reforms: The Indonesian Case *Eduardo Lachica*	(2003)
48.	Sovereignty and The Politics of Identity in International Relations *Adrian Kuah*	(2003)
49.	Deconstructing Jihad; Southeast Asia Contexts *Patricia Martinez*	(2003)
50.	The Correlates of Nationalism in Beijing Public Opinion *Alastair Iain Johnston*	(2003)

51.	In Search of Suitable Positions' in the Asia Pacific: Negotiating the US-China Relationship and Regional Security *Evelyn Goh*	(2003)
52.	American Unilaterism, Foreign Economic Policy and the 'Securitisation' of Globalisation *Richard Higgott*	(2003)
53.	Fireball on the Water: Naval Force Protection-Projection, Coast Guarding, Customs Border Security & Multilateral Cooperation in Rolling Back the Global Waves of Terror from the Sea *Irvin Lim*	(2003)
54.	Revisiting Responses To Power Preponderance: Going Beyond The Balancing-Bandwagoning Dichotomy *Chong Ja Ian*	(2003)
55.	Pre-emption and Prevention: An Ethical and Legal Critique of the Bush Doctrine and Anticipatory Use of Force In Defence of the State *Malcolm Brailey*	(2003)
56.	The Indo-Chinese Enlargement of ASEAN: Implications for Regional Economic Integration *Helen E S Nesadurai*	(2003)
57.	The Advent of a New Way of War: Theory and Practice of Effects Based Operation *Joshua Ho*	(2003)
58.	Critical Mass: Weighing in on Force Transformation & Speed Kills Post-Operation Iraqi Freedom *Irvin Lim*	(2004)
59.	Force Modernisation Trends in Southeast Asia *Andrew Tan*	(2004)
60.	Testing Alternative Responses to Power Preponderance: Buffering, Binding, Bonding and Beleaguering in the Real World *Chong Ja Ian*	(2004)
61.	Outlook on the Indonesian Parliamentary Election 2004 *Irman G. Lanti*	(2004)
62.	Globalization and Non-Traditional Security Issues: A Study of Human and Drug Trafficking in East Asia *Ralf Emmers*	(2004)
63.	Outlook for Malaysia's 11th General Election *Joseph Liow*	(2004)
64.	Not *Many* Jobs Take a Whole Army: Special Operations Forces and The Revolution in Military Affairs. *Malcolm Brailey*	(2004)
65.	Technological Globalisation and Regional Security in East Asia *J.D. Kenneth Boutin*	(2004)

66.	UAVs/UCAVS – Missions, Challenges, and Strategic Implications for Small and Medium Powers *Manjeet Singh Pardesi*	(2004)
67.	Singapore's Reaction to Rising China: Deep Engagement and Strategic Adjustment *Evelyn Goh*	(2004)
68.	The Shifting Of Maritime Power And The Implications For Maritime Security In East Asia *Joshua Ho*	(2004)
69.	China In The Mekong River Basin: The Regional Security Implications of Resource Development On The Lancang Jiang *Evelyn Goh*	(2004)
70.	Examining the Defence Industrialization-Economic Growth Relationship: The Case of Singapore *Adrian Kuah and Bernard Loo*	(2004)
71.	"Constructing" The Jemaah Islamiyah Terrorist: A Preliminary Inquiry *Kumar Ramakrishna*	(2004)
72.	Malaysia and The United States: Rejecting Dominance, Embracing Engagement *Helen E S Nesadurai*	(2004)
73.	The Indonesian Military as a Professional Organization: Criteria and Ramifications for Reform *John Bradford*	(2005)
74.	Martime Terrorism in Southeast Asia: A Risk Assessment *Catherine Zara Raymond*	(2005)
75.	Southeast Asian Maritime Security In The Age Of Terror: Threats, Opportunity, And Charting The Course Forward *John Bradford*	(2005)
76.	Deducing India's Grand Strategy of Regional Hegemony from Historical and Conceptual Perspectives *Manjeet Singh Pardesi*	(2005)
77.	Towards Better Peace Processes: A Comparative Study of Attempts to Broker Peace with MNLF and GAM *S P Harish*	(2005)
78.	Multilateralism, Sovereignty and Normative Change in World Politics *Amitav Acharya*	(2005)
79.	The State and Religious Institutions in Muslim Societies *Riaz Hassan*	(2005)
80.	On Being Religious: Patterns of Religious Commitment in Muslim Societies *Riaz Hassan*	(2005)
81.	The Security of Regional Sea Lanes *Joshua Ho*	(2005)

82.	Civil-Military Relationship and Reform in the Defence Industry *Arthur S Ding*	(2005)
83.	How Bargaining Alters Outcomes: Bilateral Trade Negotiations and Bargaining Strategies *Deborah Elms*	(2005)
84.	Great Powers and Southeast Asian Regional Security Strategies: Omni-enmeshment, Balancing and Hierarchical Order *Evelyn Goh*	(2005)
85.	Global Jihad, Sectarianism and The Madrassahs in Pakistan *Ali Riaz*	(2005)
86.	Autobiography, Politics and Ideology in Sayyid Qutb's Reading of the Qur'an *Umej Bhatia*	(2005)
87.	Maritime Disputes in the South China Sea: Strategic and Diplomatic Status Quo *Ralf Emmers*	(2005)
88.	China's Political Commissars and Commanders: Trends & Dynamics *Srikanth Kondapalli*	(2005)
89.	Piracy in Southeast Asia New Trends, Issues and Responses *Catherine Zara Raymond*	(2005)
90.	Geopolitics, Grand Strategy and the Bush Doctrine *Simon Dalby*	(2005)
91.	Local Elections and Democracy in Indonesia: The Case of the Riau Archipelago *Nankyung Choi*	(2005)
92.	The Impact of RMA on Conventional Deterrence: A Theoretical Analysis *Manjeet Singh Pardesi*	(2005)
93.	Africa and the Challenge of Globalisation *Jeffrey Herbst*	(2005)
94.	The East Asian Experience: The Poverty of 'Picking Winners *Barry Desker and Deborah Elms*	(2005)
95.	Bandung And The Political Economy Of North-South Relations: Sowing The Seeds For Revisioning International Society *Helen E S Nesadurai*	(2005)
96.	Re-conceptualising the Military-Industrial Complex: A General Systems Theory Approach *Adrian Kuah*	(2005)
97.	Food Security and the Threat From Within: Rice Policy Reforms in the Philippines *Bruce Tolentino*	(2006)
98.	Non-Traditional Security Issues: Securitisation of Transnational Crime in Asia *James Laki*	(2006)
99.	Securitizing/Desecuritizing the Filipinos' 'Outward Migration Issue'in the Philippines' Relations with Other Asian Governments *José N. Franco, Jr.*	(2006)

100.	Securitization Of Illegal Migration of Bangladeshis To India *Josy Joseph*	(2006)
101.	Environmental Management and Conflict in Southeast Asia – Land Reclamation and its Political Impact *Kog Yue-Choong*	(2006)
102.	Securitizing border-crossing: The case of marginalized stateless minorities in the Thai-Burma Borderlands *Mika Toyota*	(2006)
103.	*The Incidence of Corruption in India: Is the Neglect of Governance Endangering Human Security in South Asia?* *Shabnam Mallick and Rajarshi Sen*	(2006)
104.	The LTTE's Online Network and its Implications for Regional Security *Shyam Tekwani*	(2006)
105.	The Korean War June-October 1950: Inchon and Stalin In The "Trigger Vs Justification" Debate *Tan Kwoh Jack*	(2006)
106.	International Regime Building in Southeast Asia: ASEAN Cooperation against the Illicit Trafficking and Abuse of Drugs *Ralf Emmers*	(2006)
107.	Changing Conflict Identities: The case of the Southern Thailand Discord *S P Harish*	(2006)
108.	Myanmar and the Argument for Engagement: *A Clash of Contending Moralities?* *Christopher B Roberts*	(2006)
109.	TEMPORAL DOMINANCE Military Transformation and the Time Dimension of Strategy *Edwin Seah*	(2006)
110.	Globalization and Military-Industrial Transformation in South Asia: An Historical Perspective *Emrys Chew*	(2006)
111.	UNCLOS and its Limitations as the Foundation for a Regional Maritime Security Regime *Sam Bateman*	(2006)
112.	Freedom and Control Networks in Military Environments *Paul T Mitchell*	(2006)
113.	Rewriting Indonesian History The Future in Indonesia's Past *Kwa Chong Guan*	(2006)
114.	Twelver Shi'ite Islam: Conceptual and Practical Aspects *Christoph Marcinkowski*	(2006)
115.	Islam, State and Modernity : Muslim Political Discourse in Late 19th and Early 20th century India *Iqbal Singh Sevea*	(2006)

116.	'*Voice of the Malayan Revolution*': The Communist Party of Malaya's Struggle for Hearts and Minds in the 'Second Malayan Emergency' (1969-1975) *Ong Wei Chong*	(2006)
117.	"From Counter-Society to Counter-State: Jemaah Islamiyah According to PUPJI" *Elena Pavlova*	(2006)
118.	The Terrorist Threat to Singapore's Land Transportation Infrastructure: A Preliminary Enquiry *Adam Dolnik*	(2006)
119.	The Many Faces of Political Islam *Mohammed Ayoob*	(2006)
120.	Facets of Shi'ite Islam in Contemporary Southeast Asia (I): Thailand and Indonesia *Christoph Marcinkowski*	(2006)
121.	Facets of Shi'ite Islam in Contemporary Southeast Asia (II): Malaysia and Singapore *Christoph Marcinkowski*	(2006)
122.	Towards a History of Malaysian Ulama *Mohamed Nawab*	(2007)
123.	Islam and Violence in Malaysia *Ahmad Fauzi Abdul Hamid*	(2007)
124.	Between Greater Iran and Shi'ite Crescent: Some Thoughts on the Nature of Iran's Ambitions in the Middle East *Christoph Marcinkowski*	(2007)
125.	Thinking Ahead: Shi'ite Islam in Iraq and its Seminaries (hawzah 'ilmiyyah) *Christoph Marcinkowski*	(2007)
126.	The China Syndrome: Chinese Military Modernization and the Rearming of Southeast Asia *Richard A. Bitzinger*	(2007)
127.	Contested Capitalism: Financial Politics and Implications for China *Richard Carney*	(2007)
128.	Sentinels of Afghan Democracy: The Afghan National Army *Samuel Chan*	(2007)
129.	The De-escalation of the Spratly Dispute in Sino-Southeast Asian Relations *Ralf Emmers*	(2007)
130.	War, Peace or Neutrality:An Overview of Islamic Polity's Basis of Inter-State Relations *Muhammad Haniff Hassan*	(2007)
131.	Mission Not So Impossible: The AMM and the Transition from Conflict to Peace in Aceh, 2005–2006 *Kirsten E. Schulze*	(2007)
132.	Comprehensive Security and Resilience in Southeast Asia: ASEAN's Approach to Terrorism and Sea Piracy *Ralf Emmers*	(2007)

133.	The Ulama in Pakistani Politics *Mohamed Nawab*	(2007)
134.	China's Proactive Engagement in Asia: Economics, Politics and Interactions *Li Mingjiang*	(2007)
135.	The PLA's Role in China's Regional Security Strategy *Qi Dapeng*	(2007)
136.	War As They Knew It: Revolutionary War and Counterinsurgency in Southeast Asia *Ong Wei Chong*	(2007)
137.	Indonesia's Direct Local Elections: Background and Institutional Framework *Nankyung Choi*	(2007)
138.	Contextualizing Political Islam for Minority Muslims *Muhammad Haniff bin Hassan*	(2007)
139.	Ngruki Revisited: Modernity and Its Discontents at the Pondok Pesantren al-Mukmin of Ngruki, Surakarta *Farish A. Noor*	(2007)
140.	Globalization: Implications of and for the Modern / Post-modern Navies of the Asia Pacific *Geoffrey Till*	(2007)
141.	Comprehensive Maritime Domain Awareness: An Idea Whose Time Has Come? *Irvin Lim Fang Jau*	(2007)
142.	Sulawesi: Aspirations of Local Muslims *Rohaiza Ahmad Asi*	(2007)
143.	Islamic Militancy, Sharia, and Democratic Consolidation in Post-Suharto Indonesia *Noorhaidi Hasan*	(2007)
144.	Crouching Tiger, Hidden Dragon: The Indian Ocean and The Maritime Balance of Power in Historical Perspective *Emrys Chew*	(2007)
145.	New Security Dimensions in the Asia Pacific *Barry Desker*	(2007)
146.	Japan's Economic Diplomacy towards East Asia: Fragmented Realism and Naïve Liberalism *Hidetaka Yoshimatsu*	(2007)
147.	U.S. Primacy, Eurasia's New Strategic Landscape,and the Emerging Asian Order *Alexander L. Vuving*	(2007)
148.	The Asian Financial Crisis and ASEAN's Concept of Security *Yongwook RYU*	(2008)
149.	Security in the South China Sea: China's Balancing Act and New Regional Dynamics *Li Mingjiang*	(2008)
150.	The Defence Industry in the Post-Transformational World: Implications for the United States and Singapore *Richard A Bitzinger*	(2008)

151.	The Islamic Opposition in Malaysia:New Trajectories and Directions *Mohamed Fauz Abdul Hamid*	(2008)
152.	Thinking the Unthinkable: The Modernization and Reform of Islamic Higher Education in Indonesia *Farish A Noor*	(2008)
153.	Outlook for Malaysia's 12th General Elections *Mohamed Nawab Mohamed Osman, Shahirah Mahmood and Joseph Chinyong Liow*	(2008)
154.	The use of SOLAS Ship Security Alert Systems *Thomas Timlen*	(2008)
155.	Thai-Chinese Relations:Security and Strategic Partnership *Chulacheeb Chinwanno*	(2008)
156.	Sovereignty In ASEAN and The Problem of Maritime Cooperation in the South China Sea *JN Mak*	(2008)
157.	Sino-U.S. Competition in Strategic Arms *Arthur S. Ding*	(2008)
158.	Roots of Radical Sunni Traditionalism *Karim Douglas Crow*	(2008)
159.	Interpreting Islam On Plural Society *Muhammad Haniff Hassan*	(2008)
160.	Towards a Middle Way Islam in Southeast Asia: Contributions of the Gülen Movement *Mohamed Nawab Mohamed Osman*	(2008)
161.	Spoilers, Partners and Pawns: Military Organizational Behaviour and Civil-Military Relations in Indonesia *Evan A. Laksmana*	(2008)
162.	The Securitization of Human Trafficking in Indonesia *Rizal Sukma*	(2008)
163.	The Hindu Rights Action Force (HINDRAF) of Malaysia: Communitarianism Across Borders? *Farish A. Noor*	(2008)
164.	A Merlion at the Edge of an Afrasian Sea: Singapore's Strategic Involvement in the Indian Ocean *Emrys Chew*	(2008)
165.	Soft Power in Chinese Discourse: Popularity and Prospect *Li Mingjiang*	(2008)
166.	Singapore's Sovereign Wealth Funds: The Political Risk of Overseas Investments *Friedrich Wu*	(2008)
167.	The Internet in Indonesia: Development and Impact of Radical Websites *Jennifer Yang Hui*	(2008)
168.	Beibu Gulf: Emerging Sub-regional Integration between China and ASEAN *Gu Xiaosong and Li Mingjiang*	(2009)

169.	Islamic Law In Contemporary Malaysia: Prospects and Problems *Ahmad Fauzi Abdul Hamid*	(2009)
170.	"Indonesia's Salafist Sufis" *Julia Day Howell*	(2009)
171.	Reviving the Caliphate in the Nusantara: Hizbut Tahrir Indonesia's Mobilization Strategy and Its Impact in Indonesia *Mohamed Nawab Mohamed Osman*	(2009)
172.	Islamizing Formal Education: Integrated Islamic School and a New Trend in Formal Education Institution in Indonesia *Noorhaidi Hasan*	(2009)
173.	The Implementation of Vietnam-China Land Border Treaty: Bilateral and Regional Implications *Do Thi Thuy*	(2009)
174.	The Tablighi Jama'at Movement in the Southern Provinces of Thailand Today: Networks and Modalities *Farish A. Noor*	(2009)
175.	The Spread of the Tablighi Jama'at Across Western, Central and Eastern Java and the role of the Indian Muslim Diaspora *Farish A. Noor*	(2009)
176.	Significance of Abu Dujana and Zarkasih's Verdict *Nurfarahislinda Binte Mohamed Ismail, V. Arianti and Jennifer Yang Hui*	(2009)
177.	The Perils of Consensus: How ASEAN's Meta-Regime Undermines Economic and Environmental Cooperation *Vinod K. Aggarwal and Jonathan T. Chow*	(2009)
178.	The Capacities of Coast Guards to deal with Maritime Challenges in Southeast Asia *Prabhakaran Paleri*	(2009)
179.	China and Asian Regionalism: Pragmatism Hinders Leadership *Li Mingjiang*	(2009)
180.	Livelihood Strategies Amongst Indigenous Peoples in the Central Cardamom Protected Forest, Cambodia *Long Sarou*	(2009)
181.	Human Trafficking in Cambodia: Reintegration of the Cambodian illegal migrants from Vietnam and Thailand *Neth Naro*	(2009)
182.	The Philippines as an Archipelagic and Maritime Nation: Interests, Challenges, and Perspectives *Mary Ann Palma*	(2009)
183.	The Changing Power Distribution in the South China Sea: Implications for Conflict Management and Avoidance *Ralf Emmers*	(2009)

184.	Islamist Party, Electoral Politics and Da'wa Mobilization among Youth: The Prosperous Justice Party (PKS) in Indonesia *Noorhaidi Hasan*	(2009)
185.	U.S. Foreign Policy and Southeast Asia: From Manifest Destiny to Shared Destiny *Emrys Chew*	(2009)
186.	Different Lenses on the Future: U.S. and Singaporean Approaches to Strategic Planning *Justin Zorn*	(2009)
187.	Converging Peril : Climate Change and Conflict in the Southern Philippines *J. Jackson Ewing*	(2009)
188.	Informal Caucuses within the WTO: Singapore in the "Invisibles Group" *Barry Desker*	(2009)
189.	The ASEAN Regional Forum and Preventive Diplomacy: A Failure in Practice *Ralf Emmers and See Seng Tan*	(2009)
190.	How Geography Makes Democracy Work *Richard W. Carney*	(2009)
191.	The Arrival and Spread of the Tablighi Jama'at In West Papua (Irian Jaya), Indonesia *Farish A. Noor*	(2010)
192.	The Korean Peninsula in China's Grand Strategy: China's Role in dealing with North Korea's Nuclear Quandary *Chung Chong Wook*	(2010)
193.	Asian Regionalism and US Policy: The Case for Creative Adaptation *Donald K. Emmerson*	(2010)
194.	Jemaah Islamiyah:Of Kin and Kind *Sulastri Osman*	(2010)
195.	The Role of the Five Power Defence Arrangements in the Southeast Asian Security Architecture *Ralf Emmers*	(2010)
196.	The Domestic Political Origins of Global Financial Standards: Agrarian Influence and the Creation of U.S. Securities Regulations *Richard W. Carney*	(2010)
197.	Indian Naval Effectiveness for National Growth *Ashok Sawhney*	(2010)
198.	Exclusive Economic Zone (EEZ) regime in East Asian waters: Military and intelligence-gathering activities, Marine Scientific Research (MSR) and hydrographic surveys in an EEZ *Yang Fang*	(2010)
199.	Do Stated Goals Matter? Regional Institutions in East Asia and the Dynamic of Unstated Goals *Deepak Nair*	(2010)

200.	China's Soft Power in South Asia *Parama Sinha Palit*	(2010)
201.	Reform of the International Financial Architecture: How can Asia have a greater impact in the G20? *Pradumna B. Rana*	(2010)
202.	"Muscular" versus "Liberal" Secularism and the Religious Fundamentalist Challenge in Singapore *Kumar Ramakrishna*	(2010)
203.	Future of U.S. Power: Is China Going to Eclipse the United States? Two Possible Scenarios to 2040 *Tuomo Kuosa*	(2010)
204.	Swords to Ploughshares: China's Defence-Conversion Policy *Lee Dongmin*	(2010)
205.	Asia Rising and the Maritime Decline of the West: A Review of the Issues *Geoffrey Till*	(2010)
206.	From Empire to the War on Terror: The 1915 Indian Sepoy Mutiny in Singapore as a case study of the impact of profiling of religious and ethnic minorities. *Farish A. Noor*	(2010)
207.	Enabling Security for the 21st Century: Intelligence & Strategic Foresight and Warning *Helene Lavoix*	(2010)
208.	The Asian and Global Financial Crises: Consequences for East Asian Regionalism *Ralf Emmers and John Ravenhill*	(2010)
209.	Japan's New Security Imperative: The Function of Globalization *Bhubhindar Singh and Philip Shetler-Jones*	(2010)
210.	India's Emerging Land Warfare Doctrines and Capabilities *Colonel Harinder Singh*	(2010)
211.	A Response to Fourth Generation Warfare *Amos Khan*	(2010)
212.	Japan-Korea Relations and the Tokdo/Takeshima Dispute: The Interplay of Nationalism and Natural Resources *Ralf Emmers*	(2010)
213.	Mapping the Religious and Secular Parties in South Sulawesi and Tanah Toraja, Sulawesi, Indonesia *Farish A. Noor*	(2010)
214.	The Aceh-based Militant Network: A Trigger for a View into the Insightful Complex of Conceptual and Historical Links *Giora Eliraz*	(2010)
215.	Evolving Global Economic Architecture: Will We have a New Bretton Woods? *Pradumna B. Rana*	(2010)

216.	Transforming the Military: The Energy Imperative *Kelvin Wong*	(2010)
217.	ASEAN Institutionalisation: The Function of Political Values and State Capacity *Christopher Roberts*	(2010)
218.	China's Military Build-up in the Early Twenty-first Century: From Arms Procurement to War-fighting Capability *Yoram Evron*	(2010)
219.	Darul Uloom Deoband: Stemming the Tide of Radical Islam in India *Taberez Ahmed Neyazi*	(2010)
220.	Recent Developments in the South China Sea: Grounds for Cautious Optimism? *Carlyle A. Thayer*	(2010)
221.	Emerging Powers and Cooperative Security in Asia *Joshy M. Paul*	(2010)
222.	What happened to the smiling face of Indonesian Islam? Muslim intellectualism and the conservative turn in post-Suharto Indonesia *Martin Van Bruinessen*	(2011)
223.	Structures for Strategy: Institutional Preconditions for Long-Range Planning in Cross-Country Perspective *Justin Zorn*	(2011)
224.	Winds of Change in Sarawak Politics? *Faisal S Hazis*	(2011)
225.	Rising from Within: China's Search for a Multilateral World and Its Implications for Sino-U.S. Relations *Li Mingjiang*	(2011)
226.	Rising Power… To Do What? Evaluating China's Power in Southeast Asia *Evelyn Goh*	(2011)
227.	Assessing 12-year Military Reform in Indonesia: Major Strategic Gaps for the Next Stage of Reform *Leonard C. Sebastian and Iisgindarsah*	(2011)
228.	Monetary Integration in ASEAN+3: A Perception Survey of Opinion Leaders *Pradumna Bickram Rana, Wai-Mun Chia & Yothin Jinjarak*	(2011)
229.	Dealing with the "North Korea Dilemma": China's Strategic Choices *You Ji*	(2011)
230.	Street, Shrine, Square and Soccer Pitch: Comparative Protest Spaces in Asia and the Middle East *Teresita Cruz-del Rosario and James M. Dorsey*	(2011)
231.	The Partai Keadilan Sejahtera (PKS) in the landscape of Indonesian Islamist Politics: Cadre-Training as Mode of Preventive Radicalisation? *Farish A Noor*	(2011)

232.	The Trans-Pacific Partnership Agreement (TPP) Negotiations: Overview and Prospects *Deborah Elms and C.L. Lim*	(2012)
233.	How Indonesia Sees ASEAN and the World: A Cursory Survey of the Social Studies and History textbooks of Indonesia, from Primary to Secondary Level. *Farish A. Noor*	(2012)
234.	The Process of ASEAN's Institutional Consolidation in 1968-1976: Theoretical Implications for Changes of Third-World Security Oriented Institution *Kei Koga*	(2012)
235.	Getting from Here to There: Stitching Together Goods Agreements in the Trans-Pacific Partnership (TPP) Agreement *Deborah Elms*	(2012)
236.	Indonesia's Democratic Politics and Foreign Policy-Making: A Case Study of Iranian Nuclear Issue, 2007-2008 *Iisgindarsah*	(2012)
237.	Reflections on Defence Security in East Asia *Desmond Ball*	(2012)
238.	The Evolving Multi-layered Global Financial Safety Net: Role of Asia *Pradumna B. Rana*	(2012)
239.	Chinese Debates of South China Sea Policy: Implications for Future Developments *Li Mingjiang*	(2012)
240.	China's Economic Restructuring : Role of Agriculture *Zhang Hongzhou*	(2012)
241.	The Influence of Domestic Politics on Philippine Foreign Policy: The case of Philippines-China relations since 2004 *Aileen S.P. Baviera*	(2012)
242.	The Forum Betawi Rempug (FBR) of Jakarta: An Ethnic-Cultural Solidarity Movement in a Globalising Indonesia *Farish A. Noor*	(2012)
243.	Role of Intelligence in International Crisis Management *Kwa Chong Guan*	(2012)
244.	Malaysia's China Policy in the Post-Mahathir Era: A Neoclassical Realist Explanation *KUIK Cheng-Chwee*	(2012)
245.	Dividing the Korean Peninsula: The Rhetoric of the George W. Bush Administration *Sarah Teo*	(2012)
246.	China's Evolving Fishing Industry: Implications for Regional and Global Maritime Security *Zhang Hongzhou*	(2012)
247.	By Invitation, Mostly: the International Politics of the US Security Presence, China, and the South China Sea *Christopher Freise*	(2012)

248.	Governing for the Future: What Governments can do *Peter Ho*	(2012)
249.	ASEAN's centrality in a rising Asia *Benjamin Ho*	(2012)
250.	Malaysia's U.S. Policy under Najib: Ambivalence no more? *KUIK Cheng-Chwee*	(2012)
251.	Securing the State: National Security in Contemporary Times *Sir David Omand GCB*	(2012)
252.	Bangladesh-India Relations: Sheikh Hasina's India-Positive Policy Approach *Bhumitra Chakma*	(2012)
253.	Strengthening Economic Linkages Between South and East Asia: The Case for a Second Round of "Look East" Policies *Pradumna B Rana and Chia Wai-Mun*	(2013)
254.	The Eurozone Crisis and Its Impact on Asia *Pradumna B Rana and Michael Blomenhofer*	(2013)
255.	Security Identity, Policymaking Regime and Japanese Security Policy Development *Bhubhindar Singh*	(2013)
256.	The Rising Chorus of Chinese Exceptionalism *Benjamin Ho Tze Ern*	(2013)
257.	Iran: How Intelligence and Policy Intersect *Robert Jervis*	(2013)
258.	Enhancing Global and Regional Mechanisms for Conflict Management and Resolution *Ibrahim A. Gambari*	(2013)
259.	A New Containment-Policy – The Curbing of War and Violent Conflict in World Society *Andreas Herberg-Rothe*	(2013)
260.	The Strategy of Coercive Isolation in U.S. Security Policy *Timothy W. Crawford*	(2013)
261.	Beyond its Mineral/Natural Resources: Why Africa Matters to the World *Ibrahim A. Gambari*	(2013)
262.	Wahhabism vs. Wahhabism: Qatar Challenges Saudi Arabia *James M. Dorsey*	(2013)
263.	Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime *Caitríona H. Heinl*	(2013)