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

Council for Security Cooperation in the Asia Pacific (CSCAP)
Memorandum No. 20
Ensuring A Safer Cyber Security Environment
May 2012

Introduction

As the global economic centre of gravity shifts from Europe and North America, the Asia Pacific region is becoming the most important political, economic, strategic and socially diverse and dynamic region in the world. One major factor driving this change is the development of the capabilities offered by the rapid changes in information and communications technology (ICT), and the ability of the region to harness the resultant opportunities to both national and regional advantage. However, this situation is dependent on the effectiveness of Information Assurance across cyber space to ensure the secure, resilient and trusted electronic operating environment that is essential to sustain progress and prosperity.

Potential cyber-related threats to Information Assurance can originate from natural disasters, accidental events, or hostile targeting. The latter may include, particularly, such common threats to all regional nations as organized crime and terrorism. Measures to maximize protection against cyber threats and also maximize the regional benefits of the digital economy, comprise two essential, separate, but inter-related activities. Firstly, each regional state should implement a domestic cyber security strategy that is holistic and encompasses government, the private sector and civil society. Secondly, regional states should establish common collective measures of cooperation that provide an additional umbrella of protection against cyber threats that is not achievable unilaterally.

This Memorandum identifies considerations and recommendations concerning measures to implement an ARF cyber security strategy to enhance cyber security to the mutual benefit of all states, individually and collectively within the Asia Pacific region.

Observations

CSCAP notes previous ARF statements and views concerning the serious nature of common cyber-related threats to all regional nations, and the need for regional cooperation to mitigate these threats, including:

- ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space issued in Kuala Lumpur on 28 July 2006.

- Co-Chair's Summary Report of the 4th ARF Seminar on Cyber Terrorism, held in Busan during 16-19 October 2007.

- The Hanoi Plan of Action to Implement the ARF Vision Statement endorsed by the ARF SOM, 20 May 2010

CSCAP makes the following observations:

- Significance of Cyber Security

  - Today's Information Society provides unprecedented opportunities for nations to utilize the related benefits of the increased capability and use of ICT to national advantage.

  - A secure, resilient and trusted operating environment to enable nations individually, regionally and globally to take advantage of these opportunities.

  - National advantage is maximized where the benefits are holistic across government, the private sector and civil society.

  - Critical infrastructure, including that relating to telecommunications, banking and finance, transport, energy, water, essential government services and the media, is important in the enhancement of national advantage

- Cyber Security as a Domestic Security Issue

  - Government leadership is essential in enabling all sectors of society to recognize and exercise their individual and collective responsibilities, to promote a secure, resilient and trusted operating environment.

- The necessity for each government to establish a national cyber security strategy involving all domestic stakeholders to create the above operating environment.

- Public-private partnerships as part of the above collective responsibilities.

- Highly interconnected and interdependent ICT systems are potentially vulnerable to accidental or deliberate threats.

- Threats due to natural causes include fire, earthquake and flood. Those due to accidental human causes include operating errors or the unintentional consequence of other physical activity such as construction work.

- Deliberate threats include threats common to all nations such as organized crime, terrorism, commercial espionage, or malicious hacktivism by individuals or issue motivated groups.

- The need for internal and international collaborative measures to maximize Information Assurance (IA) – availability, integrity and confidentiality – of ICT systems.

- Cyber Security as a Regional Security Issue

  - Closer cooperation between all regional nations to establish common collective measures to further enhance Information Assurance and their ability to minimize and mitigate cyber threats.

  - Common collective measures include the sharing of information and experience about cyber threats, and cooperative arrangements for capacity development and technical assistance.

  - Development of National Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) to facilitate national coordination of the above, and the development of Asia Pacific CERT (APCERT) to facilitate regional cooperation and coordination amongst CERTs and CSIRTs.

  - Harmonization of laws to criminalize unauthorized access, interception and interference with computer systems and data, and enable legal mutual support.

Recommendations

The formulation and implementation of an ARF cyber security strategy that meets the individual and collective needs of all ARF states is an urgent requirement. The aim of this strategy is to ensure a secure, resilient and trusted electronic operating environment that best serves the interests of all regional states through effective domestic and collaborative international cyber security measures.

It is recommended that at the level of **national responsibilities**, strong leadership to coordinate the involvement of all stakeholders is required, whereby governments should:

- ***Enact a holistic cyber security strategy***. The strategy should maximize national protection and resilience against cyber threats, and also maximize the national and regional benefits of the digital economy. Such a strategy would include measures that seek to implement effective policies and "best practice" procedures that maximize the availability, integrity and confidentiality of national ICT systems while at the same time minimize the threats and risks by enabling the detection, analysis, mitigation and effective response to specific threats.

- ***Increase cyber security awareness and education across government, the private sector and society generally***. This would build stakeholder confidence in the domestic and international digital environment, and create the knowledge and tools with which stakeholders can protect themselves, and respond to threats. Specific targeting would include instilling a fundamental consciousness of the importance of Information Assurance (IA) to protect both information and system, and the individual and mutual responsibilities of all stakeholders.

- ***Promote an effective partnership arrangement between government and the private sector***. Government and industry should develop a menu of market incentives to motivate companies to voluntarily upgrade their cyber security to desirable standards.

- ***Develop an effective legal framework and enforcement capabilities to combat cyber crime***. Regional states should review their relevant domestic laws and, wherever practical, implement changes to harmonize laws to effectively deal with transnational cyber crimes including terrorist misuse of cyberspace. Such laws should make it an offence including, but not limited to, intentionally accessing, intercepting and interfering with computer systems and data without authorization. Mutual legal cooperation

for the investigation, collection of evidences and other related forms of mutual legal assistance should also be enabled.

- ***Establish and strengthen CERTs with adequate resources and empowerment*.** A CERT may be either a government or non-government organization, depending on national preference. The role of the CERT would be to facilitate coordination for the provision of information and advice amongst all domestic stakeholders, and to facilitate regional and global cooperation.

The Memorandum recommends that at the level of **regional cooperation**, the ASEAN Regional Forum should:

- ***Enhance mechanism to facilitate sharing of information and experience about cyber threats focusing on detection, containment, and mitigation measures***. Regional states (potentially through their CERTs) should be able to share threat information in real time to assist on a regional level to collectively mitigate cyber threats and vulnerabilities. The development of international shared situational awareness and warning capabilities will enhance the cyber security of states and coordinated responses in the region.

  The added value of such a system is that it would strongly complement the cyber security awareness and education recommendation at the national level. In this context, the relationship and interaction between APCERT and the ARF Transnational Threat Information Sharing Centre (ATTIC) which was proposed by the US at the ARF SOM June 2011 should also be examined if it is established in future.

- ***Implement capacity building and technical assistance measures***. Priority should be given on developing a program of advice, training and technical assistance that strengthens the cyber security capacity, including capability of crisis management of all states. Ongoing ARF activities such as the Cyber Security Incident Response Workshop (CSIRW) to be co-chaired by Australia and Singapore in 2012 would be an important part of any such program. A very practical activity the ARF could undertake would be to initiate a program where those nations with a CERT capacity would assist those without to establish this function.

- ***Consider expanding the role and responsibility of APCERT***. APCERT should be upgraded to become the coordination centre for the distribution of information and advice about cyber threats, vulnerabilities, and protective and mitigation measures. In this role, APCERT will facilitate the

broadening of information and technical exchanges by providing specific incident reporting, advice on “best practice’, and conduct collaborative research and digital forensics.

- ***Increase level of legal harmonization***. In support of the harmonization of laws, an inventory of international conventions on cyber security that have been accepted/adopted by ARF members should be undertaken. The benefits of a regional or global arrangement that, over time, would facilitate the harmonization of laws to combat cyber crime should also be explored by the ARF.

- ***Establish a Regional Cyber Security Action Task Force (CSATF)***. The main responsibility of CSATF would be to liaise with all key stakeholders to develop recommended standards, mechanisms, and policies to assist in the harmonization of laws.

  CSATF should also review the cyber-related activities of other regional or global organizations (e.g. UN, ITU, APEC, OECD etc) in order to assess whether the effectiveness of those activities might benefit from improved regional coordination.

CSCAP notes with concern the existence of the increasing cyber threat, regionally and internationally from hostile activities by nation states, state-sponsored and non-state actors. Regional states should recognize the urgent necessity of establishing regional and international regimes, which prohibit such hostile activities in cyber space. CSCAP suggests that state-related hostile activities as a potential cyber security threat to all states could be the subject for separate consideration.

Conclusion

An effective regional cyber security strategy is an essential requirement for ensuring that all ARF members, individually and collectively, are able to operate within and benefit from the advantages of a secure, resilient and trusted electronic operating environment. CSCAP recommends these measures required to implement such a strategy.

ABOUT CSCAP

CSCAP is a non-governmental (second track) process for dialogue on security issues in the Asia Pacific. Membership in CSCAP is on an institutional basis and consists of Member Committees. Current membership comprises Australia, Brunei Darussalam, Cambodia, Canada, China, India, Indonesia, Japan, the Democratic People's Republic of Korea, the Republic of Korea, Malaysia, Mongolia, New Zealand, the Philippines, Russia, Singapore, Thailand, Vietnam and the USA.

The functions of CSCAP are as follows:

a. to provide an informal mechanism by which political and security issues can be discussed by scholars, officials, and others in their private capacities;
b. to encourage the participants of such individuals from countries and territories in the Asia Pacific on the basis of the principle of inclusiveness;
c. to organise various working groups to address security issues and challenges facing the region;
d. to provide policy recommendations to various intergovernmental bodies on political-security issues;
e. to convene regional and international meetings and other cooperative activities for the purpose of discussing political-security issues;
f. to establish linkages with institutions and organisations in other parts of the world to exchange information, insights and experiences in the area of regional political-security cooperation; and
g. to produce and disseminate publications relevant to the other purposes of the organisation.

Study groups are the primary mechanism for CSCAP activity. As of April 2012, there were five CSCAP Study Groups. These are concerned with: (i) Countering the Proliferation of Weapons of Mass Destruction in the Asia Pacific; (ii) Multilateral Security Governance in Northeast Asia/North Pacific; (iii) Naval Enhancement in the Asia Pacific; (iv) Water Resources Security; and (v) Cyber Security.

This memorandum was produced by the CSCAP Study Group on Cyber Security and was approved by the out of session CSCAP Steering Committee Meeting via electronic consultation on 21 May 2012.

Further information on CSCAP can be obtained from the CSCAP website at www.cscap.org or by contacting the CSCAP Secretariat:

CSCAP Secretariat
c/o ISIS Malaysia
1 Persiaran Sultan Salahuddin
PO Box 12424
50778 Kuala Lumpur
Malaysia
T: +603-2693 9366 Ext 125
F: +603-2693 9375
E: cscap@isis.org.my

CSCAP Memoranda

CSCAP Memoranda are the outcome of the work of Study Groups approved by the Steering Committee and submitted for consideration by the ASEAN Regional Forum and other bodies.

- Memorandum No.19 – Reduction and Elimination of Nuclear Weapons
  Author: Study Group on Countering the Proliferation of Weapons of Mass Destruction in the Asia Pacific
  Date published: February 2012

- Memorandum No.18 - Implementing the Responsibility to Protect (RtoP)
  Author: Study Group on the Responsibility to Protect (RtoP)
  Date published: September 2011

- Memorandum No.17 - Promoting the Peaceful Use of Nuclear Energy
  Author: Study Group on Countering the Proliferation of Weapons of Mass Destruction in the Asia Pacific
  Date published: June 2011

- Memorandum No.16 - Safety and Security of Offshore Oil and Gas Installations
  Author: Study Group on Safety and Security of Offshore Oil and Gas Installations
  Date published: January 2011

- Memorandum No.15 - The Security Implications of Climate Change
  Author: Study Group on the Security Implications of Climate Change
  Date published: July 2010

- Memorandum No.14 - Guidelines for Managing Trade of Strategic Goods
  Author: Export Controls Experts Group (XCXG)
  Date published: March 2009

- Memorandum No.13 - Guidelines for Maritime Cooperation in Enclosed and Semi-Enclosed Seas and Similar Sea Areas of the Asia Pacific
  Author: Study Group on Facilitating Maritime Security Cooperation in the Asia Pacific
  Date published: June 2008

- Memorandum No.12 - Maritime Knowledge and Awareness: Basic Foundations of Maritime Security
  Author: Study Group on Facilitating Maritime Security Cooperation in the Asia Pacific
  Date published: December 2007

- Memorandum No.11 - Human Trafficking
  Author: Study Group on Human Trafficking
  Date published: June 2007

- Memorandum No.10 - Enhancing Efforts to Address the Factors Driving International Terrorism
  Author: Study Group on Enhancing the Effectiveness of the Campaign Against International Terrorism with Specific Reference to the Asia Pacific Region
  Date published: December 2005

- Memorandum No.9 - Trafficking of Firearms in the Asia Pacific Region
  Author: Working Group on Transnational Crime
  Date published: May 2004

- Memorandum No.8 - The Weakest Link? Seaborne Trade and the Maritime Regime in the Asia Pacific
  Author: Working Group on Maritime Cooperation
  Date published: April 2004

- Memorandum No.7 - The Relationship Between Terrorism and Transnational Crime
  Author: Working Group on Transnational Crime
  Date published: July 2003

- Memorandum No.6 - The Practice of the Law of the Sea in the Asia Pacific
  Author: Working Group on Maritime Cooperation
  Date published: December 2002

- Memorandum No.5 - Cooperation for Law and Order at Sea
  Author: Working Group on Maritime Cooperation
  Date published: February 2001

- Memorandum No.4 - Guidelines for Regional Maritime Cooperation
  Author: Working Group on Maritime Cooperation
  Date published: December 1997

- Memorandum No.3 - The Concepts of Comprehensive Security and Cooperative Security
  Author: Working Group on Comprehensive and Cooperative Security
  Date published: December 1995

- Memorandum No.2 - Asia Pacific Confidence and Security Building Measures
  Author: Working Group on Confidence and Security Building Measures
  Date published: June 1995

- Memorandum No.1 - The Security of the Asia Pacific Region
  Author: CSCAP
  Date published: April 1994