REPORT

1ST MEETING OF CSCAP STUDY GROUP ON CYBER SECURITY

March 21-23, 2011, Putrajaya, Malaysia

1. BACKGROUND

Today’s Information Society has seen the increase in the capability and use of Information and Communications Technology (ICT) as a vital tool for development. The significant increase in communication networks and connectivity has multiplied the potential for knowledge-sharing and enhanced prosperity among nations, especially within the Asia Pacific region.

However, ICT also has its vulnerabilities. The increasing dependency on cyberspace, regionally and globally, has become a significant risk. In today’s interconnected world, no nation is immune from cyber attack, and these attacks are able to be launched by any nation or non-state organisation, directly or through other unwitting nations. If a nation is attacked, the impact may not be confined to that country. The damage can spread throughout the region, as well as globally. There is a need, therefore, for an effective strategy to be developed by all Asia Pacific member states to address cyber security issues in our region.

On 2 June 2010, the CSCAP Steering Committee approved the establishment of the CSCAP Study Group (CSCAP SG) in Cyber Security. The CSCAP Study Group was to convene two meetings, namely:

a. **First meeting**. To examine the various cyber security issues and challenges that are relevant to the Asia Pacific region, and their likely security risks.

b. **Second meeting.** To propose an effective strategy to accommodate cyber security challenges in the region based on the findings of the 1st meeting, the CSCAP SG.

The report of the CSCAP SG will serve as the basis for the preparation of a draft CSCAP Memorandum to be submitted to the CSCAP Steering Committee and the ASEAN Regional Forum (ARF) for further consideration.

2. 1ST MEETING OF CSCAP STUDY GROUP ON CYBER SECURITY

CSCAP SG in Cyber Security convened its first meeting on 21-23 March 2011 at IOI Palm Garden Hotel, Putrajaya. The meeting was attended by 20 delegates from 12 member committees (Australia, Brunei, Cambodia, China, India, Japan, Malaysia, Mongolia, New Zealand, Singapore, South Korea, USA, and Vietnam), and a non-member from Chinese Taipei. The 2-day meeting aimed at providing an avenue for the delegates to share their ideas about various cyber security issues and challenges that are relevant to the Asia Pacific region, and their likely security risks. The meeting was organized into 6 sessions and 8 papers were presented during the meeting.

3. SESSION 1 - CYBER SECURITY ISSUES AND CHALLENGES IN THE ASIA PACIFIC

This session examined various cyber security issues in Asia Pacific region that threaten the common interests of the member states. There were 2 presentations in this session which are summarized as follows:

3.1 Presentations

The first discussant highlighted the comprehensive study conducted by the United Nations Expert Group on Cyber Crime. During the Twelfth United Nations Congress on Crime Prevention and Criminal Justice in 2010, *“member states discussed in some depth the issue of cybercrime and decided to invite the Commission on Crime Prevention and Criminal Justice to convene an open-ended inter-governmental expert group to conduct a comprehensive study of the problem of cybercrime, as well as the response to it.”* This would include the response by member states, the international community and the private sector, and include the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen the existing responses and to propose new responses to cybercrime.

The structure for the above study consists of 6 main areas, namely “Problem of Cyber Crime, Legal Responses to Cyber Crime, Non-Legal Responses to Cyber Crime, Responses by International Community, Technical Assistance and Responses by Private Sectors”. These in turn have been converted into 13 topics. The discussant said this study is still on-going and he recommended that the topics being addressed by the United Nations Expert Group on Cybercrime might be considered by the CSCAP Study Group. He also said that, on legal and non-legal means to address cyber threats, legal approaches would take a long time due to the bureaucratic processes involved. Therefore, non-legal approaches should be pursued as more timely attainable measures.

The second discussant highlighted the impact of ICT on productivity and that this has exceeded the effect of any other technology-enabler to date, including electricity and the combustion engine. Online traffic has increased at a compound annual growth rate of 66% over the past five years. However, our high dependency on ICT systems has posed new vulnerabilities and placed all organizations at risk. Industry estimates the value of losses from intellectual property and data theft in 2008 as high as $1 trillion. A U.S. Cyberspace Policy Review reported that in 2007 the FBI estimated that dedicated cyber attack organizations seeking industrial secrets operated out of 108 countries. . The loss due to cyber crime has exceeded USD100 billion, and more than 60% of US businesses believed that cyber crime was more costly to them than traditional crime. The presentation also highlighted the rise of cyber attacks targeting critical infrastructures and the increased threat of cyber war as in the case of cyber attacks on Estonia in 2007.

3.2 Issues and Discussion

The types of cyber threats are continually changing and new threats are becoming more sophisticated. The evolution in cyber threats are driven by advances in technology, the introduction of new internet-based services, and the increasing use of the internet world wide. Discussion during this session covered a range of cyber security issues and challenges. Salient points highlighted were:

a. **The Scope of the Cyber Security Study**. All representatives present expressed great concern about the rise of cyber crime, and potential threat of cyber terrorism and cyber war that targets individuals, businesses, critical infrastructures and governments within our region. No nation could act alone and successfully combat cross-border cyber attacks. Because of ICT connectivity and interdependence, if a one nation is struck by a cyber attack, the effects could also spread and adversely impact other regional nations. All nations share common interests in ensuring the security of the cyber domain. In view of this, the Study Group would focus on the examination of fundamental cyber security issues that impact on regional common interests, and propose a strategy to address these issues.

b. **Similar Studies by Other Organizations**. There are several studies that have been conducted by other organizations on cyber security related issues e.g. Asia Pacific Economic Cooperation (APEC), Organization for Economic Cooperation and Development (OECD), European Council (EC), International Telecommunication Union (ITU), The Study Group should consider aligning its work with these organizations**.**

c. **Definitions**. The Study Group recognized the problem of obtaining agreed definitions relating to cyber security issues, particularly what constitutes a threat or criminal activity because of differences of perceptions by various nations. Most nations agree with the identification of technical-related threats to Information Assurance (availability, integrity, confidentiality, authentication), including phishing, malicious codes, hacking, spam, botnets etc. However, there are diverse perspectives about content-related threats posed by web and blog sites, and social networking on the internet etc. Some nations might criminalize the dissemination of certain content i.e. pornography, sedition, hatred speech and defamation etc. However, such “illegal content” might be considered as protected by the principle of freedom of speech by others. Because of these differences, content-related threats posted on web, blog and social networking sites will not be included in the scope of the study.

d. **Legal Means and Challenges**. The Study Group discussed the possibility of common regional legal approaches to address cross-border cyber crimes and jurisdictional issues. Discussion included the harmonization of related legislation amongst nations. Despite certain common cyber threats, the differences in legislation between nations remain significant. This was due to differences between nations in national interests and threat perceptions. Because of the legal complexities involved, it was recommended the Study Group would not pursue legal means beyond a statement as to the desirability of each nation reviewing its legislation to criminalize, where practical, those activities that they commonly assess as technical threats (see c. above),

e. **Non-Legal Means**. The Study Group emphasised the importance of all regional nations being more proactive in dealing with cyber security by non-legal approaches. These approaches included the adoption by all national stakeholders of “best practice” involving public cyber security awareness, information sharing and technical assistance between nations, and capacity building including the development of technical means and solutions. As cybercrime is a truly transnational crime, the Study Group recognizes the importance of international cooperation to achieve common understanding, practices and solutions.

4. SESSION 2 - CYBER SECURITY PARTNERSHIPS: THE ROLES AND RESPONSIBILITIES OF THE GOVERNMENT, PRIVATE SECTOR, AND CIVIL SOCIETY

This session highlighted the importance of cyber security partnerships involving the government, business and civil society. It also emphasised the role of public-private partnerships as a strategy to manage cyber security in win-win situation. There were 2 presentations in this session which are summarized as follows:

4.1 Presentations

The first discussant outlined Australia’s cyber security strategy and details of a recent comprehensive high level government and industry supported review by the Kokoda Foundation of existing and future cyber security challenges, and proposed responses to these. The review highlighted that cyber threats to Australian security applied at the personal, industry, national and international level, and what needed to be done by individual stakeholders in each category, and collectively, to mitigate these threats.. Considerations included the importance of threat recognition and recognition of the implications of threats, co-dependent and partnership relationships, public education and information sharing to ensure understanding and focus, law enforcement issues, and toplevel structural change within government to ensure the required leadership, allocation of resources, national co-ordination, policies, strategies and action, including proactive and reactive measures, by all stakeholders to more effectively meet existing and future challenges.

The second discussant shared New Zealand's perspective on cyber security public-private partnerships (PPP), including Critical Infrastructure Protection (CIP) and the nation's general strategy for cyberspace security. That strategy comprises five priorities, namely a Response System, a Threat and Vulnerability Reduction Program, a Security Awareness and Training Program, Securing Government's Cyberspace, and National and International Security Cooperation. The cyber security strategies of other nations were outlined, namely the US, Estonia, UK, Canada, Australia, India, South Korea, and Qatar, as well as those of the UN/ITU and APEC. The taxonomy of PPP was discussed, including requirements in the context of cyber warfare and cyber espionage. New Zealand's approach to its cyber security strategy is to deliver a high level of outcome assurance. This approach would establish their cyberspace and cyber security requirements, and how they could be realised within an enhanced PPP spectrum.

4.2 Issues and Discussion

Cyber security is beyond the reach of any single entity. Effective cyber security requires a national strategy that combines the individual, industry, nation and international stakeholders in dynamic partnerships that deliver required outcomes in the short and longer term. The national strategy requirements and framework for promoting cyber security through effective public-private partnerships have been identified. There is no need for CSCAP to create any new framework or partnership model. The key is to maximize the effectiveness of strategies within the existing partnership model to meet existing and future threats. Several matters raised pertaining to cyber security partnerships were:

a. **Development and Adoption of Very High Level Cyber Security Standards**. To ensure maximum security and safety, and to foster confidence in computer networks that are mostly owned and managed by the private sector.

b. **Strengthening of Critical Information Infrastructure**. To ensure the resilience of critical information infrastructure, upon which governments and industry depend on to function and deliver their key services.

c. **Cyber Security Incentives**. Government and industry should develop a menu of market incentives to motivate companies to voluntarily upgrade their cyber security to desirable standards.

d. **Coordinated Response to Cyber Crisis**. To enable both government and industry to respond to any cyber crisis in a coordinated and integrated manner based on a high quality coherent strategy.

e. **Information Sharing & Early Warning**. To articulate information needs and promote effective information-sharing. Such sharing must be two-way to provide early warning of cyber attacks and malicious activities in cyber space, and time to ensure effective counter measures.

f. **Cyber Security Awareness and Capacity Building**. To enhance cyber security public awareness and education, and increase capability of systems and people to combat cyber threats.

5. SESSION 3 - LEGAL POLICY AND FRAMEWORK: TERRITORIAL AND UNIVERSAL JURISDICTIONAL CHALLENGES IN CYBER SECURITY

This session highlighted the issues of territorial and universal jurisdictional challenges in cyber security. It examined the current international legal systems and their gaps in addressing cross-border cybercrime issues. Summaries of the two presentations in this session follow:

5.1 Presentations

The first discussant highlighted cyber-related laws in various nations, and noted while nations such as Malaysia, Australia, India, Singapore and the Philippines have updated their laws to address cyber crime, many nations have not yet done so. Therefore, a person who has committed an act which would be a serious crime in many nations may not have committed an offence in the nation where the act was committed. For example, the perpetrators responsible for the world wide “ILOVEYOU” virus attacks in 2000 were not prosecuted because their offence was not covered under the law of the nations where the offence was committed. In addition, it may not be possible for the nation where the perpetrator is located to extradite that person because existing extradition treaties usually require that the acts be an offence in both nations. Some nations also have a policy that they do not extradite their own nationals. The discussant also highlighted that it would be very difficult, if not impossible, for all nations, or even all regional nations to adopt a convention providing for universal/regional jurisdiction among contracting parties. A more practical alternative would be for all regional nations to review their legislation in the context of cybercrime and amend existing or introduce new cybercrime-related laws, including provision for extraterritorial jurisdiction and mutual legal assistance in investigations.

The second discussant shared India’s perspective on the cyber security ecosystem that encompasses legal frameworks, government initiatives, important projects, industry initiatives and law enforcement. The presentation highlighted supportive legislation and special legislation in India’s Data Protection & Privacy Legal Model, and their conformity with international conventions. The government initiatives include the Computer Emergency Response Team (CERT) that is legally empowered, other legal mechanisms and important projects that cater for education and capacity building programs, and cyber forensics. One challenge to legally pursuing cyber crime was the reluctance by many individuals and commercial organizations to report cybercrime due to their fear of adverse publicity and loss of reputation and share price. In addition, the transnational nature of cyber crime and jurisdictional issues also contribute to the complexity of investigation. Criminal including cybercrime investigations comprise a 7 stage continuum being perpetration to registration, reporting, investigation, prosecution, adjudication and execution. Delays in investigation and prosecution also affect the commitment to bring a criminal to justice.

5.2 Issues and Discussion

The Study Group recognised that legislative change would take a long time to implement for political reasons and tedious bureaucratic processes. In the meantime, existing international legal methods should be investigated, and nations should seek to implement initiatives that are achievable and measurable, as a start point. Others issues highlighted were:

a. **Legal Issues on Cyber War**. There are some concerns about the application of the Geneva Convention and Hague Convention regarding cyber war. When is undeclared cyber attack an act of cyber war? If the act does not involve armed conflict, can the Law of Armed Conflict or International Humanitarian Law be applied? These situations can also be exploited by non-state actors to create chaos in cyber space.

b. **Global Responses to Cyber Attack**. The “ILOVEYOU” virus attacks could have been less damaging if prompt appropriate action had been taken earlier to mitigate the virus from spreading into the global environment. Cyber security awareness, information sharing, technical assistance and other collaborative efforts among regional nations are vital to being able to respond effectively to serious cyber incidents.

c. **Public Awareness and Education**. Public awareness and education was again highlighted as vital for combating cyber crime. Many crimes are undetected, others unreported. Also there are new forms of cybercrime, sometimes known as cyber safety, such as cyber stalking, cyber harassment, and cyber bullying etc. that do not involve physical contact but can cause serious harm to their victims.

6. SESSION 4 - MULTINATIONAL CYBER SECURITY COOPERATION: POSSIBLE COOPERATIVE MEASURES IN THE ASIA PACIFIC REGION

This session discussed the importance of multinational cyber security cooperation, examined current international initiatives and their gaps, and explored possible strategic collaborative cyber security programs. There were 2 presentations in this session, summarized as follows:

6.1 Presentations

The first discussant provided an overview of considerations by 2009/10 meetings by the UN Group of Governmental Experts' (GGE) on ICT developments in the context of international security. The UN resolution leading to the establishment of GGE in 2009, has been supported by many nations. It was stated that there are three concerns that can put the issue of cyber security beyond the domain of a nation state namely: the targeting critical infrastructure, the growth of botnets, and risk of misperception, as nation states contemplate use of ICT for warfare, intelligence, and political purposes. India maintains that every nation has a responsibility to protect its information and information infrastructure, and a legitimate right to counter cyber attacks against its interests. There is an imperative for India and other nations to implement an effective national strategy to enhance domestic cyber security. There is also an imperative for international cooperative and collaborative mechanisms to elaborate common terms and definitions, for information sharing, capability building, ICT forensic skills to identify the source of perpetrators and procedures for preserving the legal admissibility of electronic evidence, and for visible and demonstrable coordinated responses contain and mitigate attacks that threaten international peace and security.

The second discussant stated that aspects of international cooperation on cyber security were difficult due to the complexity and sensitivity of each nation's approach to national security. Three important elements were identified to help initiate international cooperation, namely: to identify mutual interests amongst regional nations that are vital for all nations' survivability, to recognize common cyber attacks that all nations see as a threat, and to work on issues that are not politically sensitive. It was emphasized that most cyber attacks adversely affect social and economic areas, without significant affects on political and military areas. Mobilization of national resources or political commitment is also difficult as it can trigger political sensitivity. It was also highlighted that cyber security education can set a suitable platform for member states to work together.

6.2 Issues and Discussion

Discussion about international cooperation on cyber security included:

a. **The Scope of International Cooperation**. The scope of proposed international cooperation needs to be clearly defined to avoid political, military or other sensitive issues that would delay or impede cooperation. Instead, the Study Group should focus on areas of common interest shared by all regional nations.

b. **Crisis Management**. Cyber attack is cross-border in nature and can threaten all regional nations. As such, security should be managed in a cooperative and integrated manner. Crisis management arrangements should be considered to enable regional nations to share information, technology and build the necessary capacity to effectively respond to a regional cyber crisis.

c. **Risk Analysis**. The Study Group should consider conducting a risk analysis of potential cyber threats, their impact on regional interests, and common effective counter measures to mitigate the risks. Regional nations could then focus on their cyber security strategies and resources based on national priorities as they see them.

7. SESSION 5: STUDY GROUP DISCUSSION AND CONCLUSION

7.1 Cyber Security Considerations

The Study Group reviewed the presentations and discussions of previous sessions. Major considerations were:

a. **ICT in the Asia Pacific Region**. The Information Revolution has facilitated significant advances in the capability and use of ICT in the Asia Pacific region, resulting in enhanced prosperity amongst regional nations. Cyber security that ensures a secure, trusted and resilient ICT domain is a critical factor in underwriting that prosperity.

b. **Nations' Roles and Responsibilities**. The first priority for each regional nation is to implement an effective domestic cyber security strategy, related policies and "best practice" procedures to reduce vulnerabilities and minimize and mitigate threats, and to extend all possible supports to the other nations in their legitimate requests for cooperation in dealing with cyber security issues. That strategy and policies will include all domestic stakeholders, namely government, the private sector and the civil population.

c. **Regional Cooperation – The Requirement**. The ICT domain is transnational and its functionality and security is interdependent across borders. Concurrent with the development of national strategies and policies, it is vital that regional nations cooperate in establishing effective common collective measures to ensure that cyber security across the whole region meets their mutual interests.

d. **Regional Cooperation – What Can Be Done**. There are optional ways forward. There are also national sensitivities, political, military and other, that must be recognized and would be obstacles to future cooperation if confronted. It is important to identify areas of mutual concern that each nation will embrace and commit to cooperative measures. The way ahead, therefore, should identify those areas of mutual concern that will enable collective cooperation, the setting and measuring goals and action within those areas, and related priorities.

e. **Terms and Definitions**. Different nations have different definitions of cyber security-related activities, and some activities that may be considered a threat or illegal in one nation are not considered so in another nation. It is important to identify those terms and definitions that shared or acceptable to all, and those that are not. We should progress those areas where nations agree and, as necessary, those where there is disagreement.

7.2 Legal Approaches

It is important to identify perceptions of common threats, and for each nation to then review cyber-related laws and implement changes to harmonise legislation wherever practical that includes provision for mutual legal assistance in investigations. Such laws should address illegal activities by individuals and organizations, and also apply to the use of computers for illegal purposes. However, there will be different perceptions of threat or illegal activities that will limit this process, at least in the short term. The possibility of a cyber security treaty amongst regional nations should be considered using a soft law approach that can be expanded over time. This treaty route can help removing legal hurdles in cooperation among nations in the Asia Pacific region.

7.3 Non-Legal Approaches

The Study Group agreed to the adoption of non-legal activities as an immediate strategy to address some regional cyber security issues. Methods to measure the success of these activities was considered equally important. In some cases the cooperative activities below may need to establish initially on a bilateral or multinational basis amongst a limited group of regional nations but with the opportunity for other nations to join at a later date.

a. **Cyber Security Awareness and Education**. This is an essential part of every effective cyber security program, and all national strategies. All regional nations should promote, and in most cases were already promoting, cyber security awareness across government, the private sector and civil population to instill related competencies and values of responsibility. Education is also critical in developing the number of professionally qualified persons in a nation to help identify, contain and mitigate cyber threats and attacks.

b. **Sharing of Information and Experience**. The sharing of information about cyber security threats, and exchanging experiences in combating these, is considered very important, and able to be implemented immediately.

c. **Technical Assistance.** Cyber security incidents will occur that are beyond the immediate technical capability of some nations to fully comprehend and combat. Arrangements to provide timely technical assistance in these situations are important.

d. **Capacity Building**. Developing technical capabilities in particular to combat cybercrime is a major priority for the international community. In some cases nations do not have the general skills but often do not have the higher technical skills and resources to identify, contain and combat threats and attacks. An action plan to enhance technical capacity building in particular should be implemented immediately.

e. **Asia Pacific Computer Emergency Response Teams (APCERT) and Cyber Crisis Management**. All CERTs should review regional coordination through APCERT to ensure regional nations receive timely coordinated and analysed information about cyber security trends, incidents, threats, alerts and possible cyber crises.

f. **References to Other Similar Studies**. The Study Group should review related studies by other cyber-related international organizations, to avoid unnecessary duplication of effort. Such studies include those undertaken by APEC, the ITU, EU and OECD.

8. WAY FORWARD

It was agreed that the Study Group's report would form the basis of a draft CSCAP Memorandum to be submitted to the CSCAP Steering Committee later in 2011 for its further consideration. The Memorandum should briefly highlight likely cyber threat scenarios in the Asia Pacific region, probable associated security risks, and a proposal that a cyber security strategy be considered by the ASEAN Regional Forum (ARF). To assist in the preparation of this Memorandum, the CSCAP Study Group should:

a. Determine the actual needs of the ARF and focus the CSCAP study on these needs.

b. Recommend cyber security as part of the ARF's agenda.

c. Emphasise within the Memorandum the importance of cyber security to regional governments. The Memorandum should highlight the fundamental cyber security issues and their importance for the Asia Pacific region.

d. Refer to other related studies done by other organizations i.e. UN, APEC, OECD, EC, ITU etc.

e. Recommend a framework for a cyber security action plan, including an awareness, education and technical assistance program, a capacity building program, legal .approaches, and measures to monitor the progress of cyber security goals.