Report on the Second Meeting of the CSCAP Study Group on Cyber Security

10th to 12th Oct, 2011 | Bengaluru

Table of Contents

1. Background 232
2. Second Meeting of the Study Group 232
3. The Draft Memorandum 233
4. Study Group Consideration 233
5. National Responsibility for Cyber Security 234
6. Regional Cooperation 235
7. Memorandum by the CSCAP Study Group on Cyber Security 236
8. List of participants 237

REPORT

2nd Meeting of the CSCAP Study Group on Cyber Security

Oct 11-12, 2011, Bengaluru, India

1. Background

CSCAP Study Group on 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.

The Co-Chairs of the CSCAP Study Group, CSCAP Malaysia, CSCAP Australia, CSCAP Singapore and CSCAP India jointly prepared a draft memorandum to be taken for the discussion.

2. Second Meeting of the Study Group

The second meeting of the CSCAP study group meeting was commenced with an opening remark of Chairman, CSCAP India. The chairman highlighted the importance of the CSCAP study group, which deliberates on the issue in the hand on merit based. Being an informal mechanism, it gives an opportunity to address bigger issues. The CSCAP study group, thus, becomes a relevant platform to deliberate on a new set of the issues that have been emerging in the cyber space.

CSCAP Singapore, in its remark, laid down the context of the meeting and also made the members aware about the expected outcome from the meeting. The Memorandum by the study group should lead to amenable proposals that have a potential to be accepted at the ARF Steering Committee, and then it will be taken forward to the respective government. Hence, the recommendation should be concrete and specific.

3. The Draft Memorandum

CSCAP Malaysia led the discussion that presented the Draft Memorandum by the study group on cyber security. CSCAP Malaysia also briefed on the deliberations of the first meeting and positions that have been taken by the study group to proceed for development of the draft memorandum.

The Draft Memorandum structures the work of the study group in two groups:

(i) Study Group Considerations: reference to the leanings from other regional and global organizations and fifteen distinct considerations by the study group

(ii) Recommendation of the CSCAP study group which are grouped under "*National Responsibility*" and " *Regional Cooperation*"

The members of the CSCAP study group expressed their confidence in the structure of the report. It was decided to pursue the same structure, while each of the sections would be debated, refined and amended based the deliberations of the study group.

4. Study Group Consideration

CSCAP Australia led the discussion on the section "*study group consideration*". The Draft Memorandum articulates fifteen considerations that study group had evaluated while preparing its recommendations. However, it was recommended by the members of the group to categories these points into some logical groups for better comprehension and readability. The Memorandum was accordingly amended to group the considerations in three groups:

(i) Significance of Cyber Security
(ii) Cyber Security as Domestic Security Issue
(iii) Cyber Security as a Regional Security Issue

Presentations on the other regional and global arrangements: The study group, in the first meeting, deliberated on the initiatives at UNO level. The second meeting had focused sessions on the other regional arrangement for the cyber security as follows:

(i) Study of Shanghai Cooperation Organization (SCO) by CSCAP Russia
(ii) Council of European Convention on Cyber Crime, presented by the CSCAP New Zealand
(iii) UN Global Cyber Security Agenda, CSCAP Russia

The Draft Memorandum was amended to reflect these discussions and mention their references.

Draft presented in the meeting: Apart from the presentation, following drafts were also presented for the discussion in meeting:

(i) Proposal of representatives of China, Russia, Tajikistan and Uzbekistan to UN on "International Code of Conduct for Information Security"

(ii) Proposal of the US “ARF Transnational Threat Information-sharing Center (ATTIC)”

Other issues:

The Study Group acknowledged the existence of a mounting cyber threat from the international and regional activities arising from hostile conduct by nation states, state-sponsored and non-state actors. The regional nations should recognize the urgent necessity of forging regional and international regimes, which prohibit such hostile activities and aggression in cyber space. The Study Group noted the importance of state related aggression as potential cyber security threats to all nations, and could be the subject for separate consideration. The Study Group recommends that CSCAP elaborate these issues further within an appropriate format.

5. National Responsibility for Cyber Security

The Draft Memorandum necessitates a need of the “*National Responsibility”* towards regional cyber security. It recommends that the nation state to have a comprehensive domestic cyber security strategy. It recommends that the government should exhibit strong leadership in ensuring cyber security in the national agenda and engage with all stakeholders that are important for national cyber security. CSCAP India led the discussion on the National Responsibility. For ensuring regional cooperation, seeking coordinated response and building capacity for regional cyber security, need of national responsibility towards cyber security was identified as the most critical step. The national role towards cyber security in the context of ARF regional cooperation was stated as:

(i) Responsibility of a ARF member country in ensuring security of cyber space
(ii) Contributing to an ecosystem for cyber security in Asia Pacific region

The members of the study group felt a need to add a new articulation of the national responsibility that reflects on three dimensions:

(i) Cyber Security as a National Responsibility

(ii) Enabling Legal Frameworks to enhance cyber security

(iii) Ensuring participation in Multilateral Cooperation. The members also suggested adding, “*minimize risk*” as an objective of national responsibility

The Draft Memorandum delves on a need of establishment of a Computer Emergency Response Team (CERT). However, the members feel that the study group should recommend for strengthening and empowering the CERT-In. Some of them expected to have definitive recommendations to ensure that ARF member countries assign significant resources and provide required enablement towards the task of cyber security. The memorandum was amended with these suggestions.

6. Regional Cooperation

CSCAP Australia led the discussion on the "*Regional Cooperation*". The following summarizes the deliberations and outcome of the discussion:

(i) Cyber Security Awareness and Education

There has been largely an agreement on the content of this section. However, with respect to situational awareness and early warning, the member suggested that outcome of this should be to enhance cyber security of nation states and coordinated response in the region. The same text was felt more relevant to in the information sharing than this particular section. The Memorandum was amended accordingly.

(ii) Sharing of Information and Experience

The study group deliberated at a greater length on the possible options for recommending the information and experience sharing. The members of the group felt that APCERT is a right place to take on the responsibility of information and experience sharing. However, US proposal on ARF Transnational Threat Information Sharing Center (ATTIC) came up into the discussion. The ATTIC proposal talks about real time sharing of information. Moreover, the coverage of the ATTIC is limited to sharing of information about conventional threat vectors.

The possibility of the linking information sharing about cyber security was deliberated in the meeting. The study group felt that in the future the relationship and interactions between APCERT and ATTIC can be examined.

(iii) Capacity Building and Technical Assistance

The study group members agreed on the content of this section of the Draft Memorandum.

(iv) Asia Pacific Computer Emergency Response Team (APCERT)

The study group members agreed on the content of this section of the Draft Memorandum. However, the members felt a need of development and expansion of APCERT capabilities.

(v) Legal Approach

The members of the study group suggested a change of "Soft Legal Approach" to "Legal Approach" and structurally put this point in the regional cooperation. The members were strongly in favor of inclusion of harmonization of laws for effectively deal with transnational cyber crimes, including terrorist misuse of cyber space. More specifically, the acts such as intentionally accessing, intercepting and interfering with computer systems and data without authorization should be termed as a criminal offense. It is also felt such laws should seek to distinguish criminal and civil offence with respect to cyber space violations.

(vi) Creation of a Regional Cyber Security Action Task Force (CSATF)

The study group members were in strong favor of recommending creating a "*Regional Cyber Security Task Force,*" as proposed by the Draft Memorandum. This task force will liaise with all key stakeholders to develop recommended standards, mechanisms, and policies to assist in the harmonization of laws.

7. Memorandum by the CSCAP Study Group on Cyber Security

The CSCAP study group finalized the Memorandum as per the suggestions and deliberations in the second meeting. The final memorandum will be submitted, as a separate document, to ARF Steering Committee.

8. List of participants

No.	Name	Contact details	Country
1.	Mr. Ian Dudgeon	Ian Dudgeon & Associates P/L 40, Couvreur Street, Garran, ACT Australia 2605, Ph: 02 62828096, Fax: 02 62828-096 E-mail: iandudgeon@netspeed.com.au	AUSTRALIA
2.	Mr. Seng Chong Poh	Department of Information Technology and Communication, Ministry of Foreign Affairs and Trade,, Jalan Subok, B.S. Begawan BD 2710, NEGARA BRUNEI DARUSSALAM. Ph: 673-2-2261177 Extn. 246, Fax: 673-2-262033 E-mail: sengchong.poh@mfa.gov.bn	BRUNEI
3.	Mr. Yi Yang	China Institute of International Studies (CIIS), 3, Toutiao, Taijichang, Beijing, China, 100005. Ph: 86-10-85119550, Fax: 86-10-65598133 E-mail: yangyi@ciis.org.cn	CHINA
4.	Mr. Lixin Wang	Third Secretary, Ministry of Foreign Affairs, China, Chaoyangmen Nandajie 2, Beijing. Ph: 0086-10-65963278, Fax: 0086-10-65963209 E-mail: wang_lixin1@mfa.gov.cn	CHINA
5.	Amb. Leela K. Ponappa	Chairperson, CSCAP India, Indian Council of World Affairs, Sapru House, Barakhamba Road, New Delhi-110 001. Mob: Mob: 9910893330 E-mail: lkponappa@yahoo.com; lkponappa@gmail.com	INDIA
6.	Mr. B.J. Srinath	Sr. Director(Sci.'G'), CERT-in Deptt. of Information Technology, M/o. Communications & Information Technology, Government of India, Electronics Niketan, 6, CGO Complex, New Delhi-110 003. Ph: 2436 3138 (O), 2618 7415 (R), Fax: 2436 6808 E-mail: bj.srinath@nic.in	INDIA
7.	Mr. Vinayak Godse	Director – Data Protection DATA SECURITY COUNCIL OF INDIA (DSCI) | A NASSCOM® Initiative **L:** Niryat Bhawan, 3rd Floor | Rao Tula Ram Marg | New Delhi – 110057. Mob: 9873083123 E-mail: vinayak.godse@dsci.in	INDIA

8.	Prof. Yasuhide Yamanouchi	New Institute for Social Knowledge and Collaboration, Tama University (NItama), Tama University Daigakuin bldg. 701, 4-10-26 Shimomeguro Meguro-ku, Tokyo, Japan 153-0064 Ph: 03-3712-3758, Fax: 03-3712-3485 E-mail: yama@ni.tama.ac.jp	**JAPAN**
9.	Mr. Sazali Sukardi	CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No. 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor, Malaysia. Ph: +603-8946 0999, Fax: +603-8946 0888 E-mail: sazali@cybersecurity.my	**MALAYSIA**
10.	Dr. Malcolm Shore	NZ 13, Canterbury University, Creyke Road, Christchurch, New Zealand. Ph: 61-413097384(Aus); Ph: 64-21-1255191 (NZ) Ph: 64-27-2713153(NZ) E-mail: malcolm@autumnriver.co.nz	**NEW ZEALAND**
11.	Mr. Oleg Demidov	The Russian Federation, The Russian Centre for Policy Studies (PIR Center), 4th Dobryninsky Pereulok 8, Moscow, Russia 119019. + 7 (926) 839-35-41; + 7 (495) 987-19-15, Fax: + 7(495) 987-19-14 E-mail: demidovov@mail.ru	**RUSSIA**
12.	Mr. Chong Guan Kwa	S. Rajaratnam School of International Studies, Nanyang Technological University, Block S4, Level B4, Nanyang Avenue, Singapore 639798. Ph: +65 6790 6975, Fax: +65 6794 0617 E-Mail: iscgkwa@ntu.edu.Sg	**SINGAPORE** **Co Chair**
13.	Mr. Yeow Boon Ng	Ministry of Home Affairs, 28 Irrawaddy Road, New Phoenix Park, Singapore 329560. Ph: 65-64785780, Fax: 65-62541626 E-mail: ng_yeow_boon@mha.gov.sg	**SINGAPORE**
14.	Mr. (Dr.) Dang-Hai Hoang	VNCERT – Ministry of Information and Communications, A12, Lo. 11, DTM DINH CONG, HOANG MAI, HANOI, VIETNAM. Ph; +84-4-36404424, Fax: +84-4-36404425 E-mail: hdhai@mic.gov.vn	**VIETNAM**
Other Participants			
15.	Prof. Chung Young Chang,	Department of Public Affairs, Fo Guang University cychang@mail.fgu.edu.tw	