# Council for Security Cooperation in the Asia Pacific (CSCAP)

## Study Group Proposal

### General Information

| | | |
|---|---|---|
| **Title:** | **Developing cyber norms of behaviour and confidence building measures for Asia Pacific** | |
| **Date of Submission:** | **May 2018** | |
| **Applicant:** | **CSCAP Singapore** | |
| **Proposed Co-Chairs:** | **TBC** | |
| **Number of Meetings:** | **1-2 times per year** | |
| **Timeframe:** | **Start of Mandate** | **End of Mandate** |
| | **Summer 2018** | **Winter of late 2019 or early 2020** |

### Description of Subject Matter

**Introduction and Significance of Study**

Countries in the Asia-Pacific are actively developing military cyber capabilities and doctrine, ranging from offensive to defensive cyber capabilities, but there are presently no universally agreed norms governing these capabilities, such as protection of critical infrastructure from cyberattacks, non-interference in political processes, or economic espionage. ASEAN supports ongoing work to promote international voluntary cyber norms of responsible state behaviour development of cyberspace and confidence building measures (CBMs) in cyber. This includes discussions on the adoption of basic, operational and voluntary norms of behaviour to guide the use of ICTs (information communications technologies) in a responsible manner, which would take reference from the eleven norms set out in the 2015 UNGGE (United Nations Group of Governmental Experts) Report.

*Countries in the Asia-Pacific can develop cyber norms that are appropriate and relevant to the region's social, economic, political, and technological context.* The UNGGE in 2017 was unable to reach consensus on the implementation of the abovementioned eleven norms. While discussions on international norms appear to have stalled, countries in the Asia-Pacific should develop regional cyber norms that reflect shared regional priorities, a multi-stakeholder approach, and recognition of the particular needs of individual states and the region as a whole.

*Cyber norms and cyber CBMs should be developed together.* Cyber norms establish the level of expectations about states' behaviour, whereas CBMs provide practical tools to manage these expectations.[i]

*Regional cyber norms and CBM's developed by countries in the Asia-Pacific, as members of the United Nations, can be a valuable resource for the development of international cyber norms and CBM's*. The EU also believes regional fora have a key role to play in building effective CBMs.[ii] Combined with the work being done in this field by the OSCE and other regional bodies, this regional approach is an alternative way to achieve international goals of promoting peace and stability in cyberspace.

**Objectives of Study**

The objectives of this study are in three-folds. First, the study group will identify shared priorities, shared vocabulary, stakeholders, and the diverse needs of various states, where cyberspace is concerned.

Second, the study group will build the findings above to identify and propose cyber norms of behaviour, and the corresponding CBMs that support them, which can be agreed on by countries in the Asia-Pacific.

Third, the study group will identify potential obstacles to implementation of the above, and recommend means of addressing those challenges.

**Anticipated Output**

By the end of the CSCAP study group's mandate, we anticipate that Asia-Pacific countries will have made significant progress in the participation and collaboration in developing cyber norms of behaviour and CBMs. Specifically, we anticipate:

- Identifying cyber norms and CBMs that Asia-Pacific countries can generally agree upon, and the obstacles to their implementation
- Recommending steps to implement cyber norms and CBMs
- Making a critical evaluation of the cyber maturity of Asia-Pacific countries and their capacity to implement cyber norms and CBMs
- Refining the existing capacity building programmes being conducted for Asia-Pacific countries, in order to support cyber norms and CBMs
- Reaching out to other regional organizations such as the ASEAN Regional Forum so that relevant policy initiatives are undertaken to implement policies by the study group.

**How does this proposed Study Group differ from previous studies undertaken by CSCAP in the past?**

Previous CSCAP study groups have done substantial work on CBMs. At the CSCAP Cybersecurity Workshop in Semarang, Indonesia, in April 2017, it was noted that CBMs were already recommended in the 2015 work plan, but have faced obstacles in implementation since then. It was suggested that "progress ultimately depends on shared priorities, a shared vocabulary, a multi-stakeholder approach, and a readiness to tailor solutions to the particular needs of individual states." The proposed study group seeks to explore these solutions and overcome the obstacles to implementing the 2015 work plan.

The proposed study group also builds upon these previous study groups, with the aim of further developing cyber norms of behaviour. The discussion about acceptable cyber norms of state behaviour is closely linked to the parallel debates about CBMs in cyberspace – they are both "two sides of the same coin".[iii] This is illustrated by the UNGGE 2015 Report which emphasises the importance of both "norms, rules, and principles for the responsible behaviour of states" and "confidence-building measures (CBMs)".

**How does this Study Group relate to the on-going concerns of ARF ISMs? (For extension of completed mandate only)**

Pursuant to the ARF Statement on Cooperation in Ensuring Cybersecurity, the ARF completed a work plan in May 2015, and held a series of workshops and seminars in 2015 and 2016. The Co-chairs' Summary Report from the ARF Seminar on Operationalizing Cyber Confidence Building Measures (Singapore 2015) reiterated that "Cyber norms and CBMs can contribute greatly to international security".

The group at the CSCAP Cybersecurity Workshop in Semarang, Indonesia, in April 2017 further agreed that "a valuable first step for any CBM project within the ARF would be inauguration of the ARF ICT Security ISM and/or ARF Study Group on Confidence Building Measures".

The proposed study group will foster constructive dialogue and consultation on political and security issues of common interest and concern, and will make significant contributions to efforts towards confidence-building and preventive diplomacy.

[i] Patryk Pawlak, Confidence-Building Measures in Cyberspace: Current Debates and Trends, in International Cyber Norms: Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016

[ii] Co-chairs' Summary Report from ARF Seminar on Operationalizing Cyber Confidence Building Measures (Singapore 2015)

[iii] Patryk Pawlak, ibid