ASEAN Regional Forum

Development of the ARF Work Plan on Cyber Security

Purpose

- The purpose of this paper is to outline possible objectives for the ASEAN Regional Forum's work in cyber security and to identify activities that could be undertaken by ARF members to help achieve those objectives.

Development of an ARF work plan on cyber security

- The development of an ARF work plan on cyber security provides us with a timely opportunity to review ARF activity in this field, our current needs and whether to adjust or broaden our focus.

- The ARF has a long history of activity in cyber security. ARF Foreign Ministers have adopted two statements. Members have hosted a wide range of workshops, seminars and conferences. Much of the ARF's work has focused on non-state actors in cyberspace and how governments might manage and respond to non-state threats – in particular, cybercrime and cyber terrorism. A second focus has been assisting ARF members to understand and respond to the different cyber threats. This work is important and should continue under the work plan on cyber security.

- In July 2012 the ARF Foreign Ministers adopted a second Statement on Cooperation in Ensuring Cyber Security. It refers to the need to further intensify regional cooperation on ICT security on a range of measures. It draws attention to the need to address the implications of ARF members' use of ICTs, including the potential use of ICTs in conflict.

- Possible aims for the next phase of ARF activity in cyber security could be:

  – preventing conflict in cyberspace between States through practical measures to enhance transparency and to develop confidence between States;

  – raising regional awareness of the security dimensions of cyberspace including the implications of State use of ICTs; and

  – practical cooperation between ARF participants to help each other develop strong government ICT networks and to protect their critical infrastructure.

- In line with the Ministerial Statement, it is proposed that the objectives for the work plan on cyber security should be to:

  <u>Confidence building & transparency measures</u>

  – develop confidence-building and other transparency measures to reduce the risk of misperception, escalation and conflict

- consideration of strategies to address threats emerging in this field consistent with international law and its basic principles.

Capacity building

- encourage and enhance cooperation in bringing about a culture of cyber security
- develop the capacity of governments to secure their ICT systems and to protect their critical infrastructure.

Possible Activities

- The types of activities that ARF members may wish to consider undertaking under the proposed ARF work plan on cyber security could include the following:
    - ARF-wide or sub-regional training focused on the development, enhancement and/or promotion of State responses to emerging cyber security threats, including inter-agency coordination
    - capacity-building workshops that share information on experiences in cyber security, bringing in government, private sector and other relevant experts to train and develop/promote best practices
    - table-top and/or field exercises between several ARF members that would test the modes of communication (including information sharing) among ARF and sub-regional members, and
    - studies on selected aspects of cyber security, in particular focused on improved risk assessment and risk reduction.

- Possible confidence building and transparency, and capacity building activities that might assist us in meeting the objectives of the work plan and that ARF participants may wish to consider offering to lead on are:

Confidence building and transparency activities

- a workshop on the importance of the need for each ARF member to share information on their respective points of contact with responsibility for cyber incidents, with a view to the establishment of a central database of such contact points, and an agreed methodology for their use
- the sharing of information on national organisational structures devoted to cyber security
- the publication of national policy papers or strategies on cyber security, which could be uploaded on the ARF website.

Capacity building

- a workshop on national approaches, best practice and lessons learned in the countries of ARF members for ensuring ICT security, for establishing a culture of ICT security and for the protection of critical infrastructure and telecommunications networks

  - a briefing to ARF members from APCERT on its capacity building work with national CIRTs/CERTs with a view to identifying possible gaps
  - a table top exercise for policy makers from ARF members on how disruptive ICT activity might be handled or prevented
  - a workshop on national approaches to dealing with cyber threats from different actors, including criminal and terrorist use of cyberspace
  - a workshop on national approaches to working and collaborating with the private sector and civil society to ensure ICT security.

- ARF members may wish to propose their own activity or an activity which encapsulates two or more of the ideas above.

Timeframe

It is proposed that the duration of the ARF work plan on cyber security be for a period of two years, once approved by Ministers. The work plan would be reviewed at the end of that period.

It is also proposed that an update on development of the work plan be provided to the Inter-Sessional Group meeting (April-May 2013), the Senior Officials Meeting (May-June 2013) and to the Ministerial meeting (June-July 2013). Depending on progress, we could have the work plan approved by Ministers at their annual meeting in 2014.

The Co-leads invite ARF members to submit their ideas for leading on particular activities under the work plan.