Agenda item 9o

Protection of Critical Infrastructures and Consultations Mechanism (CBM #3)
[Proposal by Singapore and the EU for ARF-ISM on ICTs Security]

1. Objectives

The ARF cyber CBM #3 will aim to reduce misunderstanding, misperception, and miscalculation, as well as the risk of conflict stemming from the use of ICTs through capacity and awareness building in critical infrastructures protection which will in turn, facilitate closer cooperation and understanding between States in the event of an ICT-enabled attack that could potentially lead to possible emergence of political or military tension or conflict.

The proposal recommends the implementation of preventive and cooperative frameworks with regard to the protection of critical infrastructures as a practical avenue for cooperation, and applied through a consultations mechanism, to be used on a voluntary basis and at the appropriate level as determined by participating states.

CBM#3 does not aim at solving conflicts, but at reducing the risk of conflict stemming from the Use of Information and Communication Technologies. In case a conflict already emerged following an ICT-enabled attack, other tools should be used.

2. Details of Proposed Activities and Modality

A. "Preventive side of the coin" – ARF members would take appropriate measures aiming at protecting their critical national infrastructures, including by defining baseline security requirements and establishing incident notification frameworks. The EU's NIS Directive is an example of such set of measures and could be supplemented by other relevant regional and international frameworks as may be applicable. [Information shared through the proposed CBM#2 could also inform the design of such measures.] The effort under this section would also be supported by the development of a Framework for Identifying Critical Infrastructures that would serve as a guide to assist States in defining their respective critical infrastructures, without any obligation of reporting what these critical infrastructures are. A regular workgroup meeting of critical infrastructure operators from ARF members could facilitate sharing of progress on a voluntary basis and in accordance with their respective laws and regulations.

Commented [A1]: Bracketed until CBM#2 is agreed.

B. "Cooperative side of the coin" – ARF members would commit to hold consultations, on a voluntary basis and in accordance with their laws and regulations, at the appropriate level as determined by and when deemed necessary by a State whose critical infrastructure is subject to malicious ICT acts, in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs.

The consultations mechanism would have the following indicative steps:

1. ***Notification.*** An ARF Member whose critical infrastructure is subject to malicious ICT acts may notify another ARF Member from whose territory the given malicious ICT acts are seen to be emanating Notifying another ARF Member is a way to cooperate and initiate the consultations, and does not imply responsibility of the notified State for the malicious ICT acts. [The proposed ARF Directory of Cyber Points of Contact (CBM#1) or established CERT-CERT information exchange mechanisms could be used to transmit the notifications.]

2. ***Acknowledgement.*** An acknowledgement shall be transmitted by the ARF Member receiving the notification within 48 hours, and should also include indications on the timeline for transmission of more substantive elements.

3. ***Dialogue and consultations.*** The two parties may determine the best format for the dialogue and consultations. The two parties should use the notification and the acknowledgement to shape the details, including any meetings or timelines for transmission of additional elements. Flowing dialogue and consultations are expected.

4. ***Observers and moderation***. Based on mutual consent of the parties to the consultations, observers can be invited to part, or all, of the consultations. A third party, or several third parties, can be designated to take on a mediating role and the chairmanship of the consultations.

5. ***End of the consultations***. The end of the consultations can be pronounced at any time by consensus of the two parties to the consultations.

3. Reference Documents (if any)

- Chairman's Statement of the 24th ASEAN Regional Forum and its annex 16 (*Concept Paper for the Establishment of ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies*)

- Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 (A/70/174), and in particular its para 13.(g),(h) and 16(d) (*States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;*

(*h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;*

16(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national border.)

- OSCE Permanent Council Decision 1202, and in particular paragraphs 3 and 15.

[End]