

**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 ICT 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 might be more appropriate.

## **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, establishing incident notification frameworks and designating national competent authorities. Information shared through the CBM#2 could 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.

**B. "Cooperative side of the coin"** – ARF Participants 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. Taking into account the different technical capacity among ARF participants, such consultations should be carried out in the spirit of mutual cooperation and understanding.

The consultations mechanism would have the following indicative steps. ARF Participants are invited to further refine these steps bilaterally when deemed necessary.

1. **Notification.** An ARF Participant whose critical infrastructure is subject to malicious ICT acts (*further – the requesting party*) may notify another ARF Participant from whose territory the given malicious ICT acts are seen to be emanating (*further – the requested party*), using the point of contacts envisaged in CBM#1. 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.
2. **Acknowledgement.** The requested party makes a mandatory notice of receipt of the request and start of its processing to the requesting party as soon as possible, and in any case within [48] hours, and should also include indications on the timeline for transmission of more substantive elements as appropriate.
3. **Dialogue and consultations.** To further reduce misunderstanding, misperception and miscalculation, the requesting party can invite through diplomatic channels in accordance with international law the requested party to hold consultations. The two parties agree level, time, venue and funding of such consultations through diplomatic channels.
4. **[Observers and moderation.** The parties involved can invite by mutual agreement a third party to participate in the consultations as a mediator. The parties can also invite, by mutual consent, observers to part, or all, 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. If consultations fail to achieve defined goals, the States can exercise their right to refer to the UN Security Council.

### **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*)
  
- Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2010, 2013, 2015
  
- OSCE Permanent Council Decision 1202.

[End]