Protection of ICT-Enabled Critical Infrastructures
[Proposal by Singapore and the EU]

1. Objectives

The initiative aims 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 ICT protection, which will, in turn, facilitate closer cooperation and understanding between States in the event of a malicious ICT-enabled act that could potentially lead to possible emergence of political or military tension or conflict.

The initiative recommends as a first step the implementation of preventive and cooperative activities with regard to the ICT protection of critical infrastructures as a practical avenue for cooperation.

2. Details of Proposed Activities and Modality

ARF participants would take appropriate measures aiming at protecting their ICT-enabled critical national infrastructures, including by defining baseline ICT security requirements, establishing national ICT incident notification measures and designating national competent authorities. Through the "Sharing of Information on National Laws, Policies, Best Practices and Strategies as well as Rules and Regulations" initiative, ARF participants are encouraged, as one of the topics, to share information on the modalities and mechanisms of such measures.

The effort under this section would also be supported by workshops assisting requesting States in identifying their respective ICT-enabled critical infrastructures, without any obligation of reporting what these critical infrastructures are.

3. Arrangements of the first workshop

i. Participants

All ARF participating countries are invited to send representatives from relevant ministries/agencies that are authorized to overseeing foreign affairs, national critical infrastructure protection, national ICT security etc., to the Workshop. Participants are encouraged to present their views/ideas on relevant topics of choice and share best practices. Regional and international experts will be invited as speakers.

ii. Reporting

The outcomes and recommendations of the Workshop will be reported to the ARF Inter-sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF ISM on ICTs Security).

iii. Administrative arrangements

Singapore and the European Union will jointly run the Workshop. Other ARF participating countries are encouraged to join as co-sponsors.

The Workshop will be held in the 2019-2020 intersessional year.

4. 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*)

- *ASEAN Regional Forum Work Plan 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]