Adopted on 6 March 2018

ASEAN Regional Forum Experts and Eminent Persons (ARF/EEP)
Recommendations for ARF Initiatives on Promoting Cyber Security

The ASEAN Regional Forum (ARF) should become a model for regional cyber security cooperation, given its recognized role as the leading multilateral security cooperation mechanism in the Asia-Pacific tasked with regional confidence building. The distinctive "ASEAN way" of international cooperation, the region's cultural and political diversity, and the opportunity to "build-in" cyber security as it develops its connectivity initiative and various ASEAN communities will afford the ARF a chance to lead the advancement of multilateral efforts to promote regional cyber security.

The EEPs, at their Feb 28-March 1, 2017 meeting in Canberra urged Ministers to recognize the high priority given by all nations to the growing threat of cyber incidents and attacks, and to prioritize the development of preventive diplomacy initiatives and confidence building measures on cyber security, including:

> The establishment of an on-line EEP working group to examine possible cyber confidence building measures; and
>
> The adoption and implementation by the ARF of a voluntary Cyber Points of Contact Directory to facilitate communication among regional cyber officials.

The ARF Ministers at the 24th ARF in Manila on August 7, 2017 noted the recommendations made by the ARF EEPs and commended the work of the EEPs in advancing the ARF process through their discussions and recommendations.

Challenges in Cyberspace

The advent of cyber capabilities provides both opportunities and challenges, not least of which is the need for common definitions. Cyberspace is reshaping the international security environment and the economic and social development of nations worldwide, opening up a new world of capabilities and opportunities. However, cyber threats also pose an increasingly serious challenge to regional security. This threat is multifold.

First, there is the economic damage inflicted by cyber crimes. According to the World Economic Forum's 2018 Global Risk Report, cyber attacks against businesses have doubled in the past 5 years, and in 2017 several major ransomware attacks were launched. 64% of all malicious emails contained ransomware (between July-Sep 2017), effectively doubling the number of businesses affected by ransomware compared to 2016. Given the centrality of connectivity to the many plans and visions for the future of the Asia-Pacific region, proliferating cyber threats ultimately threaten the region's future growth and prosperity.

Second, there is the threat posed by the use of the internet for terrorist purposes, including online radicalization. Third, there is the threat to national security broadly defined, which reflects, in part, the growing vulnerability of ICT networks and servers, including those that support critical infrastructure. Finally, more states are developing military cyberspace capabilities, a prospect that is increasingly viewed as threatening to both national and international security.

ARF Efforts to Date

The ARF has not ignored this danger. At the 19th ARF in July 2012, ARF foreign ministers adopted a Statement of Cooperation on Ensuring Cyber Security; two years later, at the 21st ARF, the chair tasked officials to develop a work plan that addressed practical cooperation and confidence building measures. The following year, at the 22nd ARF, attendees adopted the ARF Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs Security). The ARF has held 13 workshops, seminars, and conferences on cyber security issues since 2007.

In 2017, the ARF Ministers approved the creation of the Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technologies (ARF ISM on ICTs Security) with a subordinate open-ended Study Group on Confidence Building Measures (Study Group) to reduce the risk of conflict stemming from the use of information and communication technology. The mandate of the ARF ISM on ICTs Security is to provide a focused forum for ARF Participants to comprehensively discuss issues on security of, and in the use of, ICTs; to consider and approve proposals developed by an open-ended Study Group on Confidence Building Measures to reduce the risk of conflict stemming from the use of ICTs; to implement the ARF Work Plan on Security of and in the Use of ICTs (Work Plan); to assist in the development of a peaceful, secure, open, and cooperative ICT environment; and to prevent conflict and crises by developing trust and confidence between states in the ARF region by capacity building. This EEP report aims to complement and support this effort.

Obstacles to Progress

While ARF Participants well understand the significance and nature of challenges in cyberspace and have taken steps to address cyber security challenges, their response has been less effective than hoped. Several factors have hindered the response. They include: other security priorities among ARF Participants; the wide range of capacities across member states; lack of trust in infrastructure information; national security concerns; differences in national perceptions regarding cyberspace threats and challenges; gaps in cyber and IT capabilities; inadequate domestic legal frameworks for countering cyber threats; failure to engage all stakeholders to address cyber challenges; limited understanding of the cyber status quo in member states; and a reluctance to acknowledge shortcomings to other ARF Participants. While gaps in capabilities (and sensitivities about admitting them) are a fact of life and must be accommodated, it is nevertheless critical that ARF Participants do more to address these challenges.

Adopted on 6 March 2018

EEP Recommendations

To better promote cyber security among ARF Participants, the ARF should make full use of the newly created ISM on ICTs Security and its Study Group on CBMs, raise the importance of cyber issues, increase understanding of the challenge and threat, push forward the implementation of cyber-related initiatives, and strengthen regional capacity consistent with the UN Charter and broader global initiatives. To accomplish this, the following specific steps are recommended for ARF Participants to consider on a voluntary basis:

Intensify responsibility of ARF Participants

1. ARF Participants should develop and share national cyber security laws/regulations and strategies that reflect whole-of-government roles and responsibilities. A regional survey could facilitate this type of cooperation.

2. ARF Participants should promote sharing of national assessments of cyber threats, including developing baselines in member countries to assess their standing and capabilities, and coordinate on responding to cyber incidents and criminal and terrorist use of ICT. Cyber security tabletop exercises could help measure cyber readiness.

3. ARF Participants should encourage the compilation of the ARF Directory of Cyber Points of Contact to facilitate communication and information sharing, particularly in times of cyber incidents that have the potential to threaten regional stability. The responsibilities and exchanges expected of the Cyber Points of Contact should be more clearly defined.

4. ARF Participants are encouraged to cooperate in sharing national cyber policies to promote transparency and enhance the understanding of ARF Participants in the ICT environment with a view to reducing the risk of misperception, miscalculation and escalation of tension leading to conflict, as laid out in the ARF Work Plan. Stakeholders are encouraged to develop common understandings of key cyber terms to improve regional communication.

5. ARF Participants should build on relevant work underway in the United Nations and discuss the norms, rules, and principles of responsible behavior of states, including how international law applies to the use of ICTs consistent with UN General Assembly Resolutions.

Promote cooperation among all stakeholders

6. Stakeholders should utilize best-practices models to assess national status of and progress in the implementation of cyber security policies. Establishing a more robust baseline of the status of national cyber security efforts is imperative.

7. All relevant stakeholders, including governments, organizations, and private tech firms, should improve cooperation in cyber security to build a public-private partnership in cyber security, and

encourage all relevant stakeholders, to get further involved in cyber security discussions and the cyber policymaking process. ICT information threat sharing and best practices' exchange among stakeholders are strongly encouraged.

Strengthen capacity building and promote cross-regional cooperation

8. Countries and organizations offering assistance in capacity building should coordinate to minimize duplication and consider how their efforts can support the ARF's work in implementing regional cyber confidence building measures.

9. The ARF should study the possibility of cross-regional engagements on cyber security with other multilateral international organizations, as well as intra-regionally with the other relevant regional mechanisms and initiatives.

10. To this end, the ARF should consider commissioning a study of how other regional organizations address growing cyber challenges, along the lines of the earlier ARF Joint Study on Best Practices and Lessons Learned in Preventive Diplomacy.

Work on confidence building measures

11. All stakeholders should recognize cyber security as a major national security priority for ARF participants and promote the notion that international cooperation to ensure cyber security promotes confidence and facilitates economic growth and development.

12. The ARF should make full use of the new ISM on ICTs Security and its Study Group on CBMs to address rapidly increasing and evolving cyber threats, consider and approve CBMs proposed by the Study Group that reduce the risk of conflict stemming from ICT use, and address the current lack of scheduled confidence building measures as soon as possible.

13. The ARF EEPs may provide their findings to the ISM on ICTs Security and its Study Group on CBMs and continue to work where possible in close cooperation with track-two organizations like the Council for Security Cooperation in the Asia Pacific to build on one another's examination of cyber-related security challenges.

14. The ARF should also examine the consensus report of the 2015 UN GGE on "Developments in the Field of ICT in the context of International Security," which contains an excellent menu of CBMs worth considering.

Promote technical cooperation

15. ARF Participants should support and promote cooperative cyber efforts in specific sectors, including mutual legal assistance and CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team) cooperation.

16. ARF Participants are encouraged to share vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities with proper protocol and protection of communication channels.

The EEPs applaud the creation of the ARF ISM on ICTs Security and its Study Group on CBMs and stand ready to assist. We trust this Memo will help support their deliberations.