2015 ASEAN REGIONAL FORUM WORK PLAN ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES

Adopted in Kuala Lumpur, Malaysia on 6 August 2015

BACKGROUND

The Work Plan has been developed following the adoption of the Statement on Cooperation in Ensuring Cyber Security by the ARF Foreign Ministers at the 19th ARF Ministerial Meeting, 12 July 2012, Phnom Penh. The Statement sets out a number of measures to intensify regional cooperation. Ministers requested "a work plan on security in the use of ICTs focused on practical cooperation on confidence building measures". This plan gives effect to that request and is a step towards the implementation of Ministerial statement of 2012. As set out in the Chairman's Statement of the 21st ARF Ministerial Meeting on 10 August 2014 in Nay Pyi Taw, Ministers tasked officials to submit the plan to the 22nd ARF Ministerial Meeting in 2015.

PURPOSE

The purpose of the Work Plan is to promote 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, and by capacity building.

OBJECTIVES

The objectives of the work plan are to:

(a) promote transparency and develop confidence building measures to enhance the understanding of ARF Participating Countries in the ICT environment with a view to reducing the risk of misperception, miscalculation and escalation of tension leading to conflict;

(b) raise awareness on threats related to the security of and in the use of ICTs;

(c) enhance practical cooperation between ARF Participating Countries to protect ICT-enabled critical infrastructure with the view to also developing resilient government ICT environments; and

(d) Improve cooperation including develop regional capacity to respond to criminal and terrorist use of ICTs through improved coordination and coordinated response.

RELATIONSHIP TO THE WORK PLAN ON COUNTER TERRORISM AND TRANSNATIONAL CRIME (CTTC)

The Work Plan is a living document. It forms part of the CTTC Work Plan.

The ARF Unit will review its implementation progress annually and report to the Inter-sessional Meeting on Counter Terrorism and Transnational Crime and to the Inter-sessional Support Group on Confidence Building Measures and Preventive Diplomacy. The work plan shall be reviewed initially three years after its adoption.

The outcome of the review shall be endorsed by ARF Senior Officials' Meeting and be approved by Ministers.

IMPLEMENTATION

This Work Plan sets out activities which participants have identified as meeting the purpose and objectives of the plan. These activities will be implemented in accordance with ARF practices and procedures under which ARF participants put forward a concept paper for consideration and approval by the ARF Inter-sessional Support Group on Confidence Building Measures and Preventive Diplomacy, by ARF Senior Officials and ARF Foreign Ministers. Each implementation activity will have an ASEAN and a non-ASEAN host. Concept papers will set out the parameters of the activity. Participants taking forward an activity will be responsible for arranging financing. Lead countries, co-sponsors and participants are invited to bring forward concept papers, selected from the list of activities, and to implement the Work Plan. New proposals for activities are also welcomed. The sharing of information by ARF Participating Countries in connection with an activity will be voluntary.

PROPOSED ACTIVITIES

1) Establish an open ended Study Group on Confidence Building Measures to reduce the risk of conflict stemming from the use of ICTs. The Group will comprise ARF Members. The Study Group could submit consensus reports recommending confidence building measures, drawing on previous ARF discussions and reviewing relevant work in other regional and international forums, taking in account the suggested activities set out in this Work Plan.

- The Study Group should develop processes and procedures for sharing information between ARF contact points on preventing ICT crises, and criminal and terrorist use of ICTs; establishment of a contacts database (without duplicating existing CERT networks).

2) Conduct workshops and seminars for ARF Participating Countries.

The focus of these workshops and seminars, which would support the work of the Study Group, could include the following:

i. the voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations related to security of and in the use of ICTs as well as the procedures for this sharing of information;

ii. discussion exercises involving cooperation among ARF participating countries, on how to prevent incidents related to security of and in the use of ICTs becoming regional security problems;

iii. conduct of surveys on lessons learnt in dealing with threats to the security of and in the use of ICTs and creation of ARF databases on potential threats and possible remedies, taking into account the work that is already done in the commercial computer security sector and in the CERT community in this regard;

iv. capacity building related to security of and in the use of ICTs and to combating criminal use of the internet;

v. promotion of and cooperation in research and analysis on issues relevant to security of and in the use of ICTs;

vi. discussion on rules, norms, and principles of responsible behaviour by ARF Participating Countries and the role of cultural diversity in the use of ICTs;

vii. raising awareness for non-technical personnel and policy makers on threats in the use of ICTs and methods for countering such threats;

viii. measures to promote cooperation among ARF Participating Countries against criminal and terrorist use of ICTs including, inter alia, cooperation between law enforcement agencies and legal practitioners, possible joint task force between countries, crime prevention and information sharing on possible regional cooperation mechanism;

ix. discussion on the terminology related to security of and in the use of ICTs to promote understanding of different national practices and usage;

x. consideration of establishment of senior policy Point of Contacts between ARF Participating Countries to facilitate real time communication about events and incidents in relation to security of and in the use of ICTs of potential regional security significance; and

xi. consideration of establishment of channels for online information sharing on threats in ICT space, global ICT incidents and sources of ICT attacks threatening critical infrastructure, and development of modalities for real time information sharing (leveraging activities conducted by CERT networks).

It is important to establish relationships and cooperation, between government- mandated authorities on national security of ARF Participating Countries, through establishment of senior policy point of contacts between ARF Participating Countries to facilitate real time communication about events and incidents in relation to security in the use of ICTs of potential regional security significance.

The ARF will build on relevant work underway in other forums including the United Nations, the UN Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security, and the UN Open-ended Intergovernmental Expert Group on Cybercrime. It is not the intention of the ARF to duplicate this work.

PROPOSED PROJECTS:

1. ARF Workshop on Operationalising Confidence-Building Measures for Cooperation During Cyber Incident Response (proposed by the EU and Malaysia), first half of 2016, location tbc.

2. ARF Workshop on Cyber Security Capacity Building (proposed by China and Malaysia), 29-30 July 2015, Beijing.

3. ARF Seminar on Operationalising Confidence-Building Measures in the ASEAN Regional Forum (proposed by the United States and Singapore), fall 2015, Singapore.

IMPLEMENTED PROJECTS:

1. “ARF Workshop on Cyber Confidence Building Measures” by Australia and Malaysia, 25-26 March 2014, Kuala Lumpur, Malaysia.

2. “ARF Workshop on Measures to Enhance Cyber Security-Legal and Cultural Aspects” by China and Malaysia, 11-12 September 2013, Beijing, China.

3. “ARF Seminar on Confidence Building Measures in Cyberspace” by Republic of Korea and Malaysia, 11-12 September 2012, Seoul, Republic of Korea.

4. “ARF Workshop on Cyber Security Incident Response” by Australia and Singapore, 6-7 September 2012, Singapore.

5. “ARF Workshop on Proxy Actors in Cyberspace” by the United States and Vietnam, 14-15 March 2012, Hoi An, Vietnam.

PAST ARF/ASEAN WORK:

- ARF Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security, Phnom Penh, 12 July 2012.

- ARF Cybercrime Capacity-Building Conference by United States and Viet Nam, held in Brunei, April 2010.

- ARF Virtual Meeting of Experts on Cybersecurity and Cyber terrorism.

- The 1st - 4th ARF Seminars on Cyber Terrorism, 2004-2007: (13-15 November 2004, Busan, Republic of Korea; 3-5 October 2005, the Philippines; 6-8 September 2006, New Delhi, India; and 16-19 October 2007, Jeju, Republic of Korea)

- ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space, Kuala Lumpur, 28 July 2006.

REFERENCE DOCUMENTS:

- ARF Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security, Phnom Penh, 12 July 2012.

- ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space, Kuala Lumpur, 28 July 2006.

- Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013 (A/68/98).

- Initial Set of OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies, Decision No. 1106, PC.DEC/1106, 3 December 2013.

- Commission on Crime Prevention and Criminal Justice 2013 Resolution 22/7, “Strengthening International Cooperation to Combat Cybercrime”; and Resolution 22/8 “Promoting Technical Assistance and Capacity-building to Strengthen National Measures and International Cooperation Against Cybercrime”.