CO-CHAIRS SUMMARY REPORT
ARF CYBERCRIME CAPACITY-BUILDING CONFERENCE
BANDAR SERI BEGAWAN, BRUNEI DARUSSALAM
APRIL 27-28, 2010

1. Pursuant to the decision made by expedited procedure from the ARF Senior Officials, the United States and Vietnam co-chaired, with Brunei serving as host, the ARF Cybercrime Capacity-Building Conference April 27-28, 2010. 91 delegates from 19 ARF participating countries and representatives of ASEAN Secretariat participated in the workshop. The Agenda appears as **Annex 1.** The List of Delegates appears as **Annex 2.**

Session 1 – Opening Remarks and Introduction

2. The meeting was co-chaired by U.S. Department of Justice Senior Counsel for the Cyber Crime Infrastructure Protection Service Anthony Teelucksingh and Vietnamese Deputy Director of Hi-tech Crime Department Ministry of Public Security Colonel Tran Van Hoa. They opened the meeting and thanked the Brunei government for their warm hospitality and assistance in hosting arrangements. The co-chairs stressed the importance of international cooperation and assistance in the investigation of cyber crime incidents. They welcomed the input of all delegates toward forming a common understanding of the threats, laws, cooperation, international instruments, and actions and investigations taken related to cyber crime.

Session 2 – The Cybercrime Threat and Impact on ARF Nations

3. Delegates delivered presentations and discussed the cybercrime threat to their country and national responses to it. The Conference took note of the lessons learned from the national case studies in combating cybercrime, which include the following:

- Regional cooperation is crucial to support national efforts,
- Raising public awareness of the nature of cybercrime, and
- Strengthening international law to limit the spread of cybercrime by the same criminals after their release from prison.

4. The Philippines Undersecretary of the Office of the President, National Cybersecurity Coordinator, Virtus Gil, noted that Philippines' cybercrime incidents are in an upward trend, particularly in the defacement of government websites. Local and international terrorist groups have attacked critical infrastructures, computer networks, and the Internet. Security agencies are closely monitoring the numerous uses that terrorists make of the Internet every day given the high financial costs of attacks. Cases also indicate that international organized criminal syndicates operate in the country. Of note, some Philippines lessons learned include:

- Organized crime groups typically have a home base in weak economies that provide safe havens from which they conduct their transnational operations,
- It is critical to identify some of the ways in which organized crime is already overlapping with cybercrime, and

- It is also critical for law enforcement to build its capacity to harden their targets through effective intelligence gathering. Intelligence was crucial in thwarting a deadly terrorist attack or economic sabotage. His presentation appears as **Annex 3.**

5. Australian Director for E-security Policy, Marcella Hawkes, outlined the nature of the cybercrime threat facing Australia and its international partners, and its response to these issues. Cyber security has been identified as a top-tier national security priority and that the risk to the Australian economy from financially motivated organized crime has been identified as high. The inaugural Australian Government Cyber Security, released in November 2009, articulates the aims, objectives and Australia's cyber security strategy and the measures it pursues to maximize the security of individuals, business and government online. Specifically, Australia's strategic priorities, with which a comprehensive range of policies, programs and capabilities are aligned, are: threat awareness and response, cultural change, business-government partnerships, secure and resilient government systems, international engagement, legal and law enforcement, and knowledge, skills and innovation. Her presentation appears as **Annex 4.**

6. Thailand's Ponganun Karoonyavanich, Senior Public Prosecutor, of the Office of the Attorney General noted that one problem faced in trials in cybercrime cases is when no victim came to lodge complaints. Thailand can only prosecute the accused only after the victim/co-conspirator came to the authorities and insisted on being a victim due to lack of education and awareness. Arrests were often made on the basis of the evidence on the victim's account or transaction. Informal, followed by formal international, collaboration is necessary when the accused resides outside national jurisdiction. Thailand recommended that:

- Public education and raising awareness to reduce the opportunities to become victims and/or co-conspirators.
- Need to have *shared responsibilities* in international assistance procedures between the investigating country , the country where the accused resides or has nationality, and the country where the victim resides.
- Laws need to be amended to push the burden of proof to the accused side. A summary of his presentation appears as **Annex 5**.

7. Russian delegation member Mr. S.Komov highlighted military aspects of Russia's regional policy in the area of international information security. He stressed the necessity of a comprehensive approach in ensuring international information security which comprises its military, terrorist and criminal aspects. The speaker underlined the importance of creation of the regional legal base for joint activities of the ASEAN countries in this field, taking into account the experience of other regional organizations. He drew attention to the necessity of strict implementation of the UN documents in the sphere of international information security, creation of a universal legal instrument in this sphere, elaboration of definitions and concerted approaches to and criteria for the ensuring international information security. During the discussion on introduction to the Council of Europe Convention on Cybercrime made by the American co-chair, the Russian Federation representative T.Gureeva said that this Convention cannot fully serve

as a model for other regional organizations. Russia being a member of the Council of Europe did not sign the said Convention because of article 32 "b" (Trans-border access to stored computer data), which makes possible for one Party to access or receive through a computer system in its territory, stored computer data located in other Party without notification of its official authorities. Article 32 "b" contradicts Russia's legislation and effects its sovereignty. The existing possibilities of misusing the Convention do not, in fact, facilitate international cooperation in such a sensitive field, but make it very problematic for Russia. In June 2009 the Shanghai Cooperation Organization (SCO) adopted the Agreement on International Information Security which reflects a comprehensive approach to the solution of problems in this field. Russia believes the SCO countries' experience in creation of the legal base for cooperation in the sphere of international information security could be effectively used by the ASEAN countries in their future work to ensure international information security in their region.
His presentation appears as **Annex 6.**

Session 3 – Technology Talk: Computers, Networks, and the Internet

8. Carol Sipperly of the US Department of Justice CCIPS Division presented on topics relating to computers, networks and the internet. The talk focused on various types of electronic evidence and the methods used by criminals to exploit networks and the internet. Starting with an understand of the applications offered by internet service providers and used by customers, the talk focused on locating evidence on the internet and on individual computers and networks. The "decentralized" network that makes up the internet makes investigation of cyber crimes a challenge, requiring international cooperation from governments and international entities to track nodes on the network exploited by cyber criminals. The internet is a packet-switched network. Systems keep many records about their interactions with the rest of the network. Those records can help locate, identify, and ultimately gather evidence against cyber criminals in addition to tracing communications, the record of the actual communication can also be located and collected. Her presentation appears as **Annex 7**.

Session 4 – Group Discussion: Cybercrime Issues in Participants' Countries

9. South Korean police senior inspector for cyber terror response center, Young Pil Lee, introduced a DDOS (Denial of Service) attack which happened in July 2009, the biggest DDOS attack South Korea had experienced. A presentation distributed to delegates appears as **Annex 20.**

10. Indonesian delegation representative, Mr. Ratno Kuncoro from Indonesian National Police gave a presentation about cyber crime in Indonesia. In his presentation, he explained about the case-handled by Indonesia Cyber Crime Unit in 2006-2009. He underscored that Indonesia has had official regulations concerning cybercrime since 2008 (Law No. 11 year 2008 regarding Information and Electronic Transaction) despite the Cyber Crime Unit's establishment in 2005. He also mentioned several cases related to cyber crime in Indonesia such as phishing, cyber gambling, trade fraud, and child pornography. He mentioned some obstacles in handling this issue, such as the needs of

human resources who have the skills in the cyber crime area, and some efforts that has been done at the national and regional level, such as the establishment of ID SIRTII (Indonesia-Security Incident Response Team on Internet Infrastructure) and cooperation with other countries to develop technology and infrastructure for handling cybercrime issues. His presentation appears as **Annex 8.**

11. Australia expanded on its presentation in session two and provided more detail on a number of aspects of its Cyber Security Strategy, including:

- Australia's legislative framework, including the computer offences contained in the Commonwealth Criminal Code,
- Law enforcement capability and capacity, including some of the challenges confronting law enforcement agencies in keeping pace with a rapidly technological and threat environment, and
- Information sharing mechanisms between the government and the owners and operators of Australia's systems of national interest, including critical infrastructure. This includes the Trusted Information Sharing Network for Critical Infrastructure Resilience and Australia's new national computer emergency response team - CERT Australia. Her presentation appears as **Annex 9.**

12. The representative Vietnam, Pol. Col Tran Van Hoa, Deputy Director of Vietnam Hightech Crime Department, Ministry of Public Security gave a presentation about cyber crime in Vietnam. In this presentation, he explained about cybercrime trends as well as Vietnam' s efforts in combating it. He highlighted that the cyber crime has become more organized, sophisticated and has negative effects on economic development. In 2009, Vietnam amended the Penal Code with the introduction of five new articles related to cybercrime. This is basic legal foundation for law enforcement agencies to effectively prevent and suppress cybercrime. To deal with the cyber crime, he stressed the need to have intensified exchange of information and experiences among and within the ARF region, promoting ARF cooperation on cybercrime investigation as well as training for law enforcement agencies in developing countries on cybercrime investigation and data recovering. His presentation appears as **Annex 10.**

13. The Philippines Director for National Cyber Security Center, Maria Lourdes, noted that addressing cybersecurity and cybercrime is a national security priority for the Philippines as the Philippines pursues passage of cybercrime laws based on the Budapest Convention of Cybercrime. The Office of the National Cybersecurity Coordinator was established in order to provide strategic and coordinative direction to all government and non-government sectors that are crucial in addressing cybercrime. Additional laws are needed to institutionalize and empower the current initiatives or ad hoc organizations. The Philippines needs to educate the legislators, regulators and administrators and standardize its policies, technical platforms, and operational procedures. Her presentation is found in **Annex 11**.

Session 5 – Investigating Crimes Involving Computers and the Internet

14. Carol Sipperly presented on investigative techniques used by law enforcement as is pertains to computer crimes and evidence. Specifically, the delineation as to the types of crimes was explained breaking down the nature of the activity into (1) committing crimes against internet users and internet service providers, (2) using computers and networks as a tool to commit crimes, and (3) using computers and networks to communicate during the course of crime and storing evidence of crime. Techniques used to find and gather evidence of the above was further explored. Legal standards as to the collection of evidence were highlighted throughout the discussion. Her presentation and additional participants' guide appears as **Annexes 12 and 13.**

Session 6, 7, and 8 – International Cooperation on Investigations Involving Computers; the Internet and International Standards and Legislation; Criminal Law Definitions Related to Computers and the Internet

15. After participant countries offered updates on the state of the investigative techniques used in the individual countries and the need for international cooperation, Anthony Teelucksingh followed with presentations citing examples of online criminal activity requiring international cooperation. Online phishing scams, bank intrusions, and other economic crimes cross international borders regularly. International standards within national definitions and legislation are needed. In particular, specific articles of the Budapest Convention on Cybercrime were discussed. Necessary substantive offenses as well as procedural provisions were detailed. Laws that would criminalize cyber related conduct must be supported by laws that enable law enforcement to investigate them. Examples of legislation enacted in various countries were provided. The presentation discussed samples of what constitutes as "intrusion" in national legislation of some countries. As regard to punishment issues, the United States discussed its best practices. However, it was emphasized that punishment is always unique to the individual country's national laws. His presentations and associated participants' guides appear as **Annexes 14-18**.

Session 10 – Conference Closing and Recommended Next Steps

16. The conference closed and opened up the floor for recommendations from its participants on follow-on ARF efforts. The meeting gave the following recommendations to the ISM-Counter Terrorism and Transnational Crime meeting and to ARF's other bodies:

- ARF should focus on the practical, operational implications of international cooperation given inevitable differences in national policies related to cybercrime.
- ARF should consider convening a tabletop exercise that tests notional cases requiring international collaboration from ARF members and develop best practices and better regional understanding on national capabilities from the exercise. A checklist of National Efforts/status of monitoring capabilities for cyber crime may be a useful outcome of such an exercise.
- Extradition, mutual legal assistance, and other legalities of cross-border case are important topics for future consideration.

- ARF should develop a contact point database for law enforcement agencies to utilize as needed for follow-up on specific cases. The ARF Virtual Meeting of Experts' proposal was considered in this light. The meeting urged countries to consider participating in the G-8 24/7 network which remains open to all ARF members
- A follow-on workshop was considered based on these ideas as well as a broader dialogue that would hope to comprehensively discuss national views on international cybercrime cooperation.

17. The List of meeting documents appears as **Annex 19.** The Meeting agreed to adopt the Co-Chairs Summary Report of the conference.