Co-Chairs' Summary Report of the 2nd ASEAN Regional Forum (ARF) Seminar on Cyber Terrorism

Cebu City, Philippines
03-05 October 2005

1. Pursuant to the decision of the 12th ASEAN Regional Forum (ARF) Ministerial Meeting in Vientiane in July 2005, the Philippines hosted the 2nd ARF Seminar on Cyber Terrorism on 03-05 October 2005 in Cebu City, Philippines. The seminar was co-chaired by Commissioner Angelo Timoteo Diaz De Rivera of the Commission on Information and Communications Technology (CICT) on behalf of the Philippines, while Ambassador for Counter-terrorism, His Excellency Cho Il-hwan, co-chaired on behalf of the Republic of Korea. Delegates from sixteen (16) ARF countries, as well as observers from the ASEAN Secretariat and the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) attended the Seminar. Attached as **Annex A** is the list of delegates.

2. The seminar provided a venue for ARF participating countries to openly share information and ideas on national policies on cyber terrorism, and encouraged them to continuously cooperate and collaborate with each other in effectively addressing diverse cyber-related threats and cyber terrorism.

3. The participants recognized the seminar as a concrete confidence-building measure that would sustain the momentum of cooperation and ensure continuity of efforts towards addressing the outstanding issues relating to cyber terrorism. The seminar was conducted in a professional and sincere manner, with the participants exchanging constructive ideas and best practices to combat cyber terrorism.

4. The seminar consisted of six [6] sessions:

- Session 1: Cyber Terrorism as Regional Security Threat
- Session 2: Protection of Nation's Critical Infrastructures
- Session 3: Crisis Management in Cyber Terrorism Incidents
- Session 4: Issues and Concerns Affecting Regional Response
- Session 5: Simulation Exercise: Regional Cooperation to Address Cyber Terrorism
- Session 6: Consideration and Adoption of the Summary Report

Opening Session

5. The Philippine Co-Chair welcomed the participants and expressed the view that despite the great differences in the level of adoption of information technology in the various sectors of society among the ARF countries, much commonality could nevertheless still be found, as cyber terrorism is transnational and borderless in nature. He said that only by "knowing our enemy" can ARF countries become more effective in the prevention and mitigation of cyber-terrorist attacks.

6. The Korean Co-chair expressed his pleasure at the opportunity to come together in a united effort to combat the common threat of cyber terrorism and stressed that now is the time to accept cyber terrorism as one of the main security threats. He added that a clear understanding of these emerging challenges and taking appropriate measures would be crucial in ensuring the security of the region.

7. DFA Assistant Secretary Erlinda Basilio, the ARF Intersessional Support Group (ISG) Leader of the Philippines, welcomed the participants to the seminar. She stated that the hosting of this seminar by the Philippines manifests the country's steadfast commitment to the global fight against terrorism as well as its confidence in the future of ARF as a platform for cooperative activities.

***Session 1: Cyber Terrorism as Regional Security Thr*eat**

8. The American delegate presented the U.S. working definition of cyber terrorism and noted the debate on the reality versus the hype of cyber terrorism. He suggested a two-pronged approach in combating cyber terrorism whereby governments plan for attacks and focus on terrorists' use of the internet. Attached as **Annex B** is the presentation of the U.S.

9. The U.S. presentation noted the emerging strategy of terrorists, such that their attacks are both symbolic and functional to their cause. Cyber based terrorism has therefore become a viable alternative to traditional acts of violence. The U.S. representative elaborated on the definition, methodology, and impact of cyber terrorism. Attached as **Annex C** is the presentation of the U.S.

10. The Chinese delegate discussed the definition of CT, the main types and trends of CT as well as tactics and countermeasures of the Chinese government. She proposed that the ARF have a common understanding and ultimately a definition of cyber-terrorism, establish close point of contact among each country's law enforcement agencies, and establish an efficient and effective intelligence sharing mechanism. Attached as **Annex D** is the presentation of China.

11. The presentation of the National Cyber Security Center of Korea focused on the recent trends in cyber threats, the response measures implemented at the state level, and the need for cooperation among ARF member-countries to combat cyber terrorism. Korea provided a definition of cyber terrorism on a national scale and cited its ill effects on the various spheres and dimensions of national security. Attached as **Annex E** is the presentation of the Republic of Korea.

12. In line with the discussion of the current threat environment in the region, the Korean delegation put forward three (3) proposals namely; (a) the nomination of contact points in each ARF member-country, (b) establishment of a network for cooperation among the various contact points through exchange of basic information among point of contacts preferably by the end of October 2005, and (c) setting up of a cyber terrorism regional cooperation center that would facilitate

communication and coordination among member-countries as well as to provide the development of a CERT for countries without existing CERTs.

13. The delegations from U.S., Russia, and EU suggested that the ARF undertake a review of existing mechanisms and procedures that could be utilized for regional cooperative efforts against cyber terrorism. The delegations cited among others the network and structures under the G8 and the Interpol. The delegations from Malaysia and the Philippines pointed out that the existing structures and systems may not be adequate to address the broader issues and concerns of cyber terrorism in the region. Noting all comments, the participants agreed to further study the proposal.

Session 2: Protection of Nation's Critical Infrastructures

14. The International Crime and Terrorism Division of the Foreign Affairs of Canada highlighted Canada's strategies, policies, and programs in protecting critical infrastructure. The Canadian presentation identified necessary steps to undertake in the fight against cyber terrorism. In regard to the management of crisis incidents, Canada is in the process of defining its Federal Cyber Security responsibilities through enhanced cooperation and coordination among concerned agencies and sectors. Attached as **Annex F** is the presentation of Canada.

15. The Russian presentation gave an overview of the information security infrastructure in Russia and of the Russian Association of Networks and Services (RANS), an association of network and service providers that has developed into a platform for collaboration between private and government entities. The Russian delegate stressed the importance of ASEAN activity as a key tool of dialogue in all aspects of anti-terrorism including cyber security in the Asia Pacific Region. Attached as **Annex G** is the presentation of Russian Federation.

16. The representative from the National Security Research Institute (NSRI) of Korea presented their country's response structure and system in the event of a cyber attack. He noted that despite the policy and institutional initiatives of Korea, there is a need for cooperation among ARF member-countries to address cyber intrusion attempts. Specifically, the NSRI suggested greater information sharing among ARF member-countries on cyber threats and incident responses. Attached as **Annex H** is the presentation of the Republic of Korea.

17. The Pakistani delegate presented several threats to cyber security from the perspective of Pakistan and the corresponding measures that their government had undertaken. He cited, among others, the establishment of the Pakistan Computer Emergency Response Team (PakCERT) which is a member of the Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG). He recommended the enactment of international legislation to penalize entities which engage in cyber terrorism and the establishment of an information sharing mechanism on a case-to-case basis. He also proposed the holding of the 3rd ARF

Seminar on Cyber Terrorism in Islamabad in 2006. Attached as **Annex I** is the presentation of Pakistan.

18. In addition to this, the delegate from Korea indicated its intention to host the 4th ARF Seminar on Cyber Terrorism in the Republic of Korea in 2007.

19. The representative of the Philippines gave a presentation on the country's "National Cyber Security Plan" (NCSP), a comprehensive plan that is part of the Philippine 16-Point Counter Terrorism Framework. He pointed out that the NCSP gives emphasis to the country's focus on mobilizing public-private capabilities, the stress on cyber security awareness, and making security a basic social function. Attached as **Annex J** is the presentation of the Philippines.

20. In regard to the discussion concerning the protection of critical infrastructures, the Canadian delegate explained that the provincial governments, having jurisdiction in the implementation of measures to protect the ten (10) sectors comprising critical infrastructures, coordinate with the private sector primarily through consultations.

21. The Russian delegation clarified that the sharp decrease in the number of computer related crimes in Russia from 2003 to 2004 was attributed to the merger of Russia's various internet providers into four to five major services and the adoption of anti-virus and anti-spam systems by all of Russia's merged internet providers.

22. The delegate from Pakistan clarified that the definition of cyber terrorism provided in their proposed legislation (Pakistan Electronic Crime Bill 2005) – i.e. *"The Cyber Terrorism. Any person, group, organization or faction who with terroristic intent utilizes or exercises or causes to assist a computer or computer network by any available means and thereby knowingly engages in or attempts to engage in terroristic act shall be guilty of a crime of cyber terrorism."* – was used as basis for the suggested imposition of capital punishment for crimes involving cyber terrorism.

23. The participants recognized the importance to push for longer retention periods of ISP logs and other related data that may be crucial in the investigation of computer-related crimes. They noted, however, that such initiatives to extend the retention period beyond two months will require high maintenance cost.

Session 3: Crisis Management in Cyber Terrorism Incidents

24. The presentation of the European Union represented by UK centered on the types of electronic attack and several projections on the capability of terrorists to use more information technology and network communication to target critical national infrastructure. The EU delegate cited the specific steps that had been

undertaken to protect the UK critical national infrastructure. Attached as **Annex K** is the presentation of the EU

25. The presentation of Singapore focused on their national incident and management program. The Singaporean delegate also discussed the structures and their corresponding responsibilities that have been established by the Singapore government in order to meet the needs of cyber security. He also provided an update of their activities to combat cyber terrorism. Attached as **Annex L** is the presentation of Singapore.

26. The Malaysian presentation noted that cyber terrorism could serve as tools to intensify state conflicts since many cases involve cross-border crimes. Thus, international and regional cooperation is deemed crucial. The Malaysian delegate proposed intensified collaboration on digital forensics and the establishment of points of contact in all levels of cyber security ranging from law enforcement to CERTs to provide, among others, early information warning. Attached as **Annex M** is the presentation of Malaysia.

27. The presentation of Thailand focused on the cyber terrorism counter measures of the Thai government that have been undertaken to address the threat of cyber terrorism, among others, the establishment of the Cyber Inspector Group (CIG) under the Ministry of Information and Communication Technology. The CIG monitors websites and prevents the abuse of the internet, facilitates the enactment of crucial legislation governing electronic transactions, and the conduct of training for personnel to combat cyber terrorism. Attached as **Annex N** is the presentation of Thailand.

28. The private sector representative from the Computer Associates gave a presentation which focused on both the target environment and defense strategy including various technologies against cyber terrorism. He cited several technologies beyond perimeter defense and these included security information management, centralized security incident management, vulnerability management, endpoint protection for PCs, identity and access management, Service Oriented Architecture Protection (SOA), and network forensics. Attached as **Annex O** is the presentation of the Computer Associates.

29. In line with the discussion on crisis management in cyber terrorism incidents, the participants discussed the experiences of the United Kingdom with regards to the protection of critical infrastructure.

30. The Korean Co-Chair appreciated the EU delegate's forecast for 2010 in regard to the capability of cyber terrorists. He shared the view that both government and private sectors should further enhance their capabilities towards 2010 to address cyber terrorism.

31. The EU delegate pointed out that terrorists would certainly use the speed of network and technological changes. Thus, he stressed that countries need to be more prepared in the future as well as to build public and private trust and confidence as foundation for cooperation.

32. In response to the query of the Pakistani delegate regarding counter measures against cyber terrorism, the EU delegate explained that they are in the process of organizing towards strengthening international and regional cooperation.

33. The Pakistani delegate sought further information on the UK's practices concerning private and wireless telecommunications technology that uses satellites. He pointed out that this type of technology could be utilized in countries without local legal restrictions.

34. The EU delegate explained that while there is no legal expertise that addresses all types of vulnerabilities, the laws of the country could apply with respect to international gateways. He pointed out that the absence of legislation could be exploited by terrorists. In the case of the UK, he said that the government is also working closely with ISPs and the companies using International Private Leased Circuits.

Session 4: Issues and Concerns Affecting Regional Response

35. The U.S. Federal Bureau of Investigation (FBI) presented a paper on the InfraGard which is aimed at providing support to private-public sectors information-sharing and to all FBI investigative programs particularly those concerning counter-terrorism, counterintelligence, and anti-cyber crime. He stressed the crucial role of the FBI and of law enforcement agencies in securing critical infrastructure as well as the need for information-sharing through partnerships with concerned industries. Attached as **Annex P** is the presentation of the U.S..

36. The Indonesian presentation gave an overview of the cyber threat situation and the measures that the government has adopted to address cyber crimes and terrorism. The Indonesian delegate pointed out the destructive impact of terrorism and cyber crimes not only to critical infrastructures but to the country as a whole as it can cause disturbance, chaos, and damage to the socio-economic and political life of the nation. He specifically cited the on-going process of establishing the Indonesian CERT or the Indonesian Security Incident Response Team on Information Infrastructure (ID SIRTII). Attached as **Annex Q** is the presentation of Indonesia.

37. The Korea Information Security Agency (KISA) gave a presentation on "The Security Issues in Korea and International Cooperation". The KISA highlighted a test of Personal Computer Survival Time as a capsule of the reality facing the security environment in Korea. The Korean delegate stressed the importance of

collaborative activities for the Asia-Pacific Region, concluding that international cooperation must be further enhanced with emphasis on closer cooperation between the public and private sector. Attached as **Annex R** is the presentation of the Republic of Korea.

38. The Korean Co-Chair thanked the delegate from Indonesia for updating the seminar on the Bali bombing incident of 01 October 2005. In this regard, he expressed deepest condolences and sympathies to the victims of the Bali bombing incident and stressed that the ARF would take a positive stance in the fight against terrorism.

39. The delegate from the EU concurred with the concerns of the delegates from Korea and the U.S. regarding the problems posed by malicious BotNets on national critical infrastructure. The EU, Korean, and U.S. delegations also agreed that cyber terrorists now have the opportunity to benefit from hackers carrying out activities for financial gain rather than from a desire to exploit the technology.

40. In response to the query of Korea concerning the measures undertaken by the U.S. in case of breach of the U.S. Government Code of Ethics concerning public and private partnerships specifically on the unauthorized disclosure of classified information, the U.S. delegate clarified that information sharing between the U.S. public and private sectors is discretionary on the part of the owners of the information. He added that should the shared information be compromised, the same would not be an issue if it is unclassified.

41. In regard to the query of the Korean delegate on the interface and cooperative mechanism being adopted by U.S. Government concerning Weapons of Mass Destruction (WMD) Response, the U.S. delegate replied that U.S. Government efforts remain very focused, specific, and goal-oriented; and emphasis is given to supplement intelligence information which is crucial in pursuing criminal cases.

42. In reply to the query of the Chinese delegate on the manner of coordination between the Department of Homeland Security (DHS) and the FBI specifically concerning the use of CERT and FBI InfraGard, the delegate from the U.S. clarified that the U.S.A. Patriot Act has defined the roles of the DHS and FBI whereby the latter is required to share information with the DHS on threat warning and analysis. He said that the role of the FBI is to share intelligence information on counterterrorism, threats to national critical infrastructures, and criminal investigations.

43. Responding to the query of the Chinese delegate on provision of legal assistance to China on matters concerning cyber terrorism under the U.S.-China Mutual Legal Assistance Agreement (MLAA), the U.S. delegation explained that under the MLAA the U.S. Department of Justice serves as the central authority to which the Chinese Government could convey its request for any legal assistance on any matters covered by the MLAA. He added that the U.S. Department of Justice

would be the focal point should the legal assistance require the participation of other concerned U.S. departments and agencies.

Session 5: Simulation Exercise: Regional Cooperation to Address Cyber Terrorism

44. A simulation exercise was conducted. Attached as **Annex S** are the scenarios and the summary of the workshop results.

Session 6: Consideration and Adoption of the Summary Report

45. The participants made following recommendations on measures to improve capabilities to address cyber terrorism:

A. The issuance of an ARF ministerial statement that will:

- *recognize the following:*
  - CT is a destructive and devastating method of global terrorism
  - The magnitude, rapid spread and the trans-national nature of the problem due to increasing global cyber interconnectivity
  - The urgency and imperative to address the problem at the national and regional levels
  - The importance of regional cooperation to combat CT and the coordinating role of the ARF in addressing CT in the region

- *call for the following:*
  - Identification of national cyber security units and establishment of a regional directory of national contact points
  - Establishment of an ARF-wide network of CERTs to facilitate the regular exchange of threat and vulnerability assessment and issuance of required warnings and patches
  - Identification of each country's areas of expertise on CT
  - Enhancement of each country's capabilities to deal with CT through capacity building programs (training in forensics, legal, technical etc)
  - Collaboration with international and regional organizations with similar concerns to address the issue of CT
  - Identification of critical infrastructure which could be potential targets for CT attack and critical infrastructure protection measures
  - Encouragement of private sector partnership with the government in the field of information security and fighting cyber crime including the protection of critical infrastructure
  - Encouragement of the enactment and implementation of cyber crime and cyber security baseline laws that are consistent with the provisions of international legal instruments
  - Increasing public awareness on cyber security and cyber ethics with emphasis on safety and security, best practices, the

responsibilities of using information networks and negative consequences from misuse of networks.
- Encouragement of the annual meeting of CT experts to arrive at a program of cooperation and monitoring of its progress

B. The formulation of a national framework for cooperation and collaboration in addressing cyber-terrorism with the following elements:

- Inter-agency coordinating body to deal with strategic and operational issues
- Policy and legislation related to cyber terrorism
- Establishment of bilateral, regional and international linkages
- Mechanisms
- Regulatory measures

Given the above terms of reference, the essential organs to be included in the above-proposed coordinating body would be those agencies in charge of: (a) National security and intelligence; (b) Legal and law enforcement; (c) Foreign affairs; (d) Information and communication; (e) Computer Emergency Response Team (CERT); (f) IT business societies; and (g) Non-government organizations.

The national framework should look into the political, legal, technical, security, and training and capacity-building aspects of cooperation, as well as aim to achieve the following proposed solutions to address perceived challenges in the fight against cyber-terrorism.

- Develop pertinent legal framework
- Increase coordination among national agencies.
- Collaboration/cooperation with international and regional agencies; and, effective management of resources
- Awareness enhancement programmes and advocacy on citizens/user responsibility
- Training/ technology transfer and counter-measures, especially digital forensics
- Reinforce capabilities to protect critical infrastructure

C. The formulation of a regional framework for cooperation and collaboration with the following elements, for consideration by the ARF Ministers:

Short term

- Establishment of a directory of Focal Points for public authorities in-charge of protection of critical infrastructure, law enforcement agencies and CERTs

- Convening of Technical or Expert Working Group meeting with the following objectives:

  – To revisit/improve capacity of Public Authority in charge of protection of critical infrastructure, law enforcement agencies and CERTs to promote interoperability among countries, e.g. Exchange of information
  – To work towards the establishment of a regional legal framework pertaining to cyber terrorism
  – To enhance confidence-building measures among different CERT networks (e.g., training programs among different CERTs) to continue closer country-to-country cooperation
  – Advocacy - public awareness and participation on issues related to combating cyber terrorism among public authorities in-charge of protection of critical infrastructure, law enforcement agencies and CERTs

- Encourage ARF participating countries to submit their national legislation pertaining to cyber terrorism to the ARF Unit at the ASEAN Secretariat for further dissemination among ARF participating countries
- Advise China and Brunei to consider the inclusion of Cyber Terrorism as one of the agenda items of the ARF ISM on CTTC in 2006

Medium-term

- To enhance capacity-building and training aimed at improving capabilities of law enforcement agencies and other agencies responsible for combating cyber terrorism
- Mobilize technical assistance to enhance the capacity of regional law enforcement agencies and other agencies responsible for combating cyber terrorism
- Inclusion of cyber-terrorism in the ongoing establishment of the ASEAN Convention on Counter-terrorism

Long term

- Further consultations on best practices regarding agreements to meet the operational requirements of the CERTs among ARF participating-countries
- Encourage ARF participating-countries to establish or update national legislation pertaining to cyber terrorism
- Establishment of mechanisms for regional cooperation to combat cyber terrorism (eg., information sharing for rapid resolution of cyber terrorism incidents)
- Establishment of an ARF Centre on Counter Cyber-terrorism