Co-Chairs' Summary of the ARF Seminar on Cyber Terrorism

Jeju Island, Republic of Korea

13-15 October 2004

1. As agreed by the Foreign Ministers at the 11th ASEAN Regional Forum (ARF) FMM, the "ARF Seminar on Cyber Terrorism" was held on 13-15 October 2004 in Jeju and was co-chaired by the Republic of Korea and the Philippines. The seminar was attended by 90 participants from 20 members of the ARF.

2. The objective of the seminar was to share information and ideas on the national policies of ARF member countries on cyber terrorism and to encourage the cooperative and effective efforts to combat diverse cyber threats and cyber terrorism. It was also intended to build trust and confidence and enlarge the network of the cyber security community

3. The seminar was recognized by the participants as the important first step in dealing with the issue of cyber terrorism as a new milestone for the further undertaking of this issue within the ARF framework and was also meaningful in a sense that a mixed combination of participants both from the security policy and cyber security sectors enabled the meeting to take stock of countering cyber terrorism at the policy, as well as operational levels in a balanced manner. The seminar was conducted in a professional and sincere manner with participants exchanging constructive ideas on the countermeasures to combating cyber terrorism.

4. The seminar was composed of the following 5 sessions:

- Session I: Cyber Terrorism as a New Security Threat: Assessing its Implications for National and Global Security
- Session II: Private-Government Partnership and Cooperation in Combating Cyber Terrorism
- Session III: Developing Technologies and Policies against Cyber Threats
- Session IV: Today and Tomorrow of CERTs - Activities and Cooperation
- Session V: Enhancing International Cooperation among ARF Members on Cyber Terrorism

Opening Session

5. The Korean co-chair of the seminar emphasized that with the spread of information technology, cyber terrorism has emerged as a new non-traditional threat to security. He highlighted that as one of the leading countries in information technology, the Korean government has played a proactive role in addressing this transnational issue including the initiative for strengthening cyber security taken up at the Asia-Europe Meeting (ASEM) held last week in Vietnam. In this regard, the Republic of Korea has assumed the co-chair of this seminar with the Republic of the Philippines, which will be significant in addressing the various aspects of this issue within the framework of the ARF for the first time, with the aim to lay the groundwork for future cooperation among ARF participants.

6. The Philippine co-chair expressed the hope that the seminar would enable participants to have a better understanding of the nature, motivation and tools of cyber terrorism, which would lead to better prevention and the building of a level of trust and confidence in the nascent ARF cyber security community. She reaffirmed the commitment of the Philippines to the fight against global terror and cyber terrorism, in particular.

Session 1: Cyber Terrorism as a New Security Threat - Assessing its Implications for National and Global Security

7. The Korean National Cyber Security Center gave a presentation on "Korea's Cyber Terror Response System and Policies." The Korean delegation showed that traditional security threats could be threatened by non-traditional means. In this context, the threat has been addressed by respective governmental institutions that are operating under the guidelines of a cyber security management system. The scope of application is configured with the definition of cyber terrorism in the system and adequate responses are conducted in phases of prevention and recovery.

8. China's Ministry of Public Security presented a paper on "China's Policies on Cyber Terrorism." The Chinese delegation pointed out that cyber terrorism includes two aspects, in which 'cyber' is considered as (1) a 'target,' or (2) a 'tool.' Accordingly, the Chinese delegation introduced its legal aspects as 'cyber' as an object and tool and

emphasized that prevention was essential in promoting its national cyber security. China also presented its national detection, reporting and responding mechanisms, as well as its training and research programmes aiming at promoting its national information infrastructure.

Session 2: Private-Government Partnership and Cooperation in Combating Cyber Terrorism

9. The National Computer Center of the Philippines presented a paper on "Private-Government Partnership" with the aim to protect critical information infrastructure. In this regard, private-government cooperation will be one of the most essential countermeasures for respective ARF participants. Information exchange between the governmental and private sectors should be conducted on a large scale with an assessment of vulnerabilities. Training and education on cyber security will also be a crucial part of cooperation.

10. The Information Security Office of the Cabinet Secretariat of Japan presented a paper to report the functions of the National Incident Response Team (NIRT) as a national CERT. The Japanese delegation also provided helpful information for a CERT collaboration network among ARF participants.

11. It was pointed out that the expansion of the cooperation network of national CERTs would be essential to countering cyber terrorism. Therefore, suggestions included framing out a contact list of the CERTs of respective ARF participants. In order to maximize the security surveillance of ARF participants, the possibility of increasing cooperation on blocking the source of terrorist organization websites was pointed out. However, the counterpoint was also made that blocking websites may not be an effective method due to problems related to ISP and could create a nuisance for some countries in terms of basic rights.

Session 3: Developing Technologies and Policies against Cyber Threats

12. The National Security Research Institute (NSRI) of Korea made their presentation on the recent trend of cyber attacks in 2004. Statistics of recent attacks were presented and a detailed explanation of the threats and comparison between various viruses and worms were provided. The means to protect computers were also introduced, which

reflects the current trend of the cyber attacks. The Korean delegation demonstrated a simulation of actual techniques used in PC hacking, web hacking, wireless hacking and cyber terrorism to stress the importance of preventive measures.

Session 4: Today and Tomorrow of CERTS - Activities and Cooperation

13. The presentations by the Malaysian and Indian delegations introduced national CERT activities including reactive and proactive measures, as well as security management services aiming at enhancing cyber security and providing protection on critical national infrastructure. In particular, the Korea Information Security Agency pointed out some limitations and challenges to CERT activities such as the lack of legal and analytical/technical support, information exchange, and coordination with related national organizations and vendors.

14. With regard to current limitations that exist in national CERT activities, the need to promote cooperation among national organizations and vendors was emphasized in promoting future CERT activities at the national level. Govcert.nl of the Netherlands also presented its views in promoting regional cooperation through its past experience in constructing a CERT network in Europe.

Session 5: Enhancing International Cooperation among ARF Members

15. The evolving nature of recent cyber attacks have limited the activities of national CERTs in effectively responding to threats to their cyber security. The National Cyber Security Center (NCSC) of the Republic of Korea proposed to examine the possibilities of constructing a CERTs network within the framework of the ARF, which would help ARF participants minimize the damaging effects of cyber terrorism through information exchange and technical support.

16. With regard to promoting cooperation in combating cyber terrorism in the Asia-Pacific region, the Ministry of Information and Communication Technology of Thailand proposed to establish a 'World Cyber Alert System,' which would provide essential information on current security issues, vulnerabilities, and cyber attacks. The representatives of the Russian Federation pointed out the need to establish universal legal frameworks in countering cyber terrorism activities, and for this purpose, to

explore ways of harmonizing the relevant national legislation of the ARF participants, in particular, by holding legal experts meetings.

General Discussions

17. The participants discussed possible methods in reaching a consensus on a definition for cyber terrorism. Several participants referred to the absence of a definition of cyber terrorism as an inhibiting factor in identifying measures in combating it. Discussion on the definition of cyber terrorism continued within the context of the motivation, means of cyber terrorism, and the scope and extent of damage caused by acts of cyber terrorism.

18. Some participants pointed out the necessity to establish common regulations on cyber security among the members. It was also noted that there are different levels of IT development in member countries and there was a need to bridge these gaps.

19. The seminar exchanged ideas on the positive and negative aspects of information technology. Some concerns were expressed on the possibility that some organizations might be involved in building up an asymmetrical information warfare capacity. Different perspectives were expressed on whether to focus on the control of hacking tools or on capacity-building measures to prevent hacking.

20. The participants shared their experiences on the interaction between public and private sectors of CERTs. The seminar also explored the possibility of sharing information and setting up a regional network of CERT within the ARF framework.

21. Member countries recognized the need to educate organizations and the public on the realities of cyber threats and cyber terrorism. Workshops, seminars and similar forums could be held for this purpose.

22. Various opinions were raised on whether or not the meeting should discuss common cyber crimes in general or focus on terrorism-related cyber crimes.

Suggested Recommendations

(1) The issues dealt with in this seminar will be reported for consideration at the ARF Inter-Sessional Support Group Meeting on CBMs (ISG), the Senior Officials' Meeting (SOM), and the Foreign Ministerial Meeting (FMM). The proceedings and outcomes of the seminar will also be briefed to ARF CTTC Meetings.

(2) Recognize the importance of dealing with the issue of cyber terrorism within the ARF framework and recommend holding further formal discussions on a regular basis with a view to promoting trust and confidence building in the ARF cyber community.

(3) Efforts will be made by the ARF participants to examine possible harmonization of domestic laws and regulations on cyber terrorism.

(4) Consider ways and means to improve coordination among ARF participants including the creation of ARF national contact points and the establishment of an 'ARF National CERT Network' with the following illustrative functions, in a manner complementing to existing networks:

- Strengthening ties among member CERTs for the purpose of reducing the possibility of cyber terrorism
- Sharing analysis and countermeasures for latest hacking techniques, worms and viruses
- Consultation on investigation cooperation to trace suspects of cyber terrorism
- Policy and technology support for member countries to set up their own CERTs, as well as assist newly established CERTs