Co-Chairs' Summary Report of the
ARF Seminar on Confidence Building Measures in Cyberspace
Seoul, Republic of Korea, 11-12 September 2012

Introduction

1. Pursuant to the decision of the 19th ASEAN Regional Forum (ARF), held in Phnom Penh, Cambodia on 12 July 2012, the ARF Seminar on Confidence Building Measures in Cyberspace was held in Seoul, the Republic of Korea, on 11-12 September 2012. Mr. Jeong-sik Kang, Deputy Director-General, International Organizations Bureau of the Ministry of Foreign Affairs and Trade of the Republic of Korea and Ambassador Raja Nazrin Aznam, Deputy Director-General (Political-Security) of the ASEAN Malaysia National Secretariat of the Ministry of Foreign Affairs of Malaysia, co-chaired the Seminar.

2. Representatives from all ARF participants, except Bangladesh, the Democratic People's Republic of Korea, India, Japan and Papua New Guinea attended the Seminar. A representative of the ASEAN Secretariat and experts from international organizations and academia, including the OSCE, UNGGE, CSIS, GCSP and ICT4Peace Foundation were also present. The Programme of the Seminar appears as **ANNEX A**, and the List of Participants as **ANNEX B**.

Opening Session - Welcome and Opening Remarks

3. Mr. Jeong-sik Kang, Deputy Director-General of the Ministry of Foreign Affairs and Trade of the Republic of Korea delivered his opening speech. He welcomed the participants to the ARF Seminar on Confidence Building Measures in Cyberspace and briefly elaborated on the benefits and challenges brought about by the use of ICTs and the need for confidence building measures (CBMs) in cyberspace to mitigate misperception and conflict. Mr. Kang put the Seminar in the context of the internet and ICT contributing to free flow of ideas, freedom of expression and enhancing accountability of governments. He also expressed hope that the Seminar will be able to thrash out a potential set of CBMs applicable in the region by building on the existing ideas and concepts that has been sorted out in previous ARF meetings and other international fora.

4. Amb. Raja Nazrin Aznam, the Malaysian Co-Chair, in his welcoming remarks expressed appreciation to the Government of the Republic of Korea for co-chairing and arranging the Seminar. He highlighted that CBMs were directed more specifically to issues related to cyber warfare rather than cyber crime. He further noted that a cyber attack on one country would have a spillover effect on another and that distrust exists among states with regard to the use of Information and Communications Technologies (ICT). He reiterated the need for ARF participants to cooperate in order to implement the previous statements and recommendations set forth in the ARF. He also underscored the importance of exchanging information, trust, standard norms, code of conduct, public-private

partnership and human capacity building, which was to be addressed in the Seminar.

Session 1 – Identification of Existing and Potential Threats in Cyberspace

5. Dr. Eneken Tikk-Ringas, Advisor to the Board of the ICT4Peace Foundation, discussed the problems arising from the differing approaches and terminologies related to cyber issues with focus on identifying the concepts from a technical, legal and political perspective. She emphasized the need to scrutinize the terms, definitions and concepts related to cyber issues. She viewed the term 'cyber security' as overly vague and pointed out that the diverse interpretation of the notion often blurs the immediate issue and related interests. She reiterated that there are numerous practices and instruments that can be assessed and applied to achieve the prioritized goals. The international community has put in place well established mechanisms for international peace and security including mechanisms established by the UN Security Council. She therefore suggested that relevant practices and instruments be set forth to clarify what needs to be addressed and that existing mechanisms first need to be considered. Dr. Tikk-Ringas' presentation outline appears as **ANNEX C.**

6. Dr. Intaek Han, Associate Research Fellow of the Jeju Peace Institute of the Republic of Korea addressed the correlation between growth and vulnerabilities in cyberspace. He explained the types and method of cyber threats and their trends and geographical distribution. He mentioned the strengths and shortcomings of national strategies and noted the negative impact of mistrust and uncertainty on cyber security. Three pillars of cyber peace were introduced: capacity building, confidence building and norm building. He pointed out that there is a lack of legal framework on cyber security and that more needs to be done to establish the norms. Such efforts may include developing legal documents. The presentation appears as **ANNEX D**.

7. Mr. Zahri Yunos, Acting Chief Executive Officer of CyberSecurity Malaysia delivered his presentation on a collaborative model toward achieving security and safety in the cyber environment. He addressed cyber threats including hacktivism and attacks on critical infrastructure, and made three recommendations to enhance cyber security: public-private partnership, regional and global cooperation, and establishment of legal and policy framework. He also elaborated on collaboration with other frameworks such as ITU, CSCAP, ARF, OIC CERT, FIRST and APCERT. He introduced Malaysia's experience of establishing governance structure in cyber security management, and its national cyber security policy. He also addressed technology related threats and cyber content related threats. He highlighted the challenges related to content-related threats in particular and the need to achieve harmonization of laws. His presentation appears as **ANNEX E.**

8. The Seminar deliberated on whether there is a lack of a cyber security legal framework and on a related note discussed how to build norms. Some participants noted that the existing international laws on conflict and humanitarian matters have evolved to encompass different forms of threats and challenges. On

the other hand, other participants suggested that the norms should be enlisted in a form of a legal document. The Seminar also discussed the possibility of cyber operations triggering an armed conflict that would necessitate application of the aforementioned existing international legal framework.

9. The Seminar also exchanged views on the ranks of the cyber threats. The Seminar observed that content-related crimes such as fraud, defamation and infringement of privacy, state's cyber attacks using proxy actors, attacks on critical infrastructure, disturbance of social norms, cyber espionage and sabotage, and cyber war are the threats to be contended with by each individual and government.

10. The Seminar discussed the impact of political relations on cyber attacks. Countries in political disputes would be inclined to make a more aggressive attack on each other. The Seminar also emphasized the need to consider the human aspects and capacity building.

Session 2 – Confidence-Building Measures in Cyberspace

11. Mr. Nemanja Malisevic, Cyber Security Officer of the Organization for Security and Cooperation in Europe (OSCE) delivered his presentation on CBMs to reduce the risks of conflict stemming from the use of ICTs with a focus on the OSCE experience. He noted that CBMs have been identified as a useful way forward to address the concerns related to cyber security and stressed that trust and confidence go hand in hand. He introduced the OSCE's work on developing CBMs in the cyber security context. He expressed hope that a final document produced will be adopted at the end of this year. He also identified the trends and tendencies with regard to potential CBMs that have emerged during discussions thus far. The focus was on transparency and cooperative measures. The CBMs discussed included best practices, exchanging information on national strategies and terminologies, joint exercises, developing national and international agreements and other legal documents. He recognized that the idea of joint exercise and developing international legal documents brought about some differences in opinions and levels of support from the participants. He added that the first set of CBMS need not be perfect and underscored the need to translate commitments into actions. The outline of his speech appears as **ANNEX F**.

12. Mr. Young-hyo Park, Director for International Security Affairs, Ministry of Foreign Affairs and Trade of the Republic of Korea discussed developing CBMs in cyberspace within the ARF framework. He briefly updated the participants on the recent discussions on cyber CBMs in the ARF and other international fora such as the UNGGE and the London Conference on Cyberspace. He reviewed the previous work of the ARF. The ARF has a decade-long history of discussing cyber security issues and in the process has already identified possible CBMs to a certain degree. He emphasized that the ARF now needs to focus on implementation of practical measures. In the same context, he addressed the two Ministerial Statements adopted by the ARF and highlighted that the recent statement adopted in July 2012 encourages participants to develop an ARF work

plan on security in the use of ICTs. He suggested that the ARF craft a feasible work plan by setting specific goals and tasks to ensure cyber security. His presentation appears as **ANNEX G.**

13. Mr. Wang Lei from the Department of Arms Control and Disarmament of China's Foreign Ministry noted that the discussion on CBMs should start from defining elements that may undermine confidence. He highlighted the three factors undermining confidence, i.e. the increasing dependence on cyberspace, the trend of regarding cyberspace as a new battlefield and the lack of rules and norms in cyberspace. He pointed out that the most important CBM the current stage is to establish international norms which would guide behaviours of all actors in information space and thus increase confidence for all. He introduced a document of the International Code of Conduct (A/66/359), which was submitted to the UN General Assembly. He pointed out that the document aims at building a peaceful, secure, open and cooperative information space. The document is politically binding and could serve as a basis for future international consensus. Furthermore, there is a need to recognize the differences between different regions and differences between the CBMs in the cold war era and those in the post-cold war era; and whether it is possible to compare conventional CBMs and cyberspace CBMs. He reiterated that the ARF participants should avoid simply copying the modalities in other areas or fields, and that more discussions regarding the international norms of behaviour need to be carried out in the region as it is the most important CBM. He stated that he wished to share the document of the International Code of Conduct (CoC) with the rest of the participants. The paper appears as **ANNEX H**, and the presentation as **ANNEX I.**

14. Ms. Michele Markoff, Senior Advisor of the U.S. Department of State, elaborated on the UNGGE report adopted in 2010 and the U.S. submission to the UNGGE this year. She introduced three categories of risk reduction activities that could build synergy in building ICT stability, namely transparency measures, cooperative measures and stability measures, and stressed that transparency measures is the most fundamental element. These three categories should be developed within the context of a voluntary, cooperative effort whose objective is to enhance international ICT stability and thereby reduce the risk of conflict. She envisioned the concept of cyber stability as a peaceful, stable and sustainable operating environment where the economic and social benefits of ICTs can be enjoyed by all states, and where the prospects for conflict are diminished through collaborations designed to remove incentives for destabilizing the cyberspace. While there is a need to recognize that differences in different regions exist, cyber is international and application of CBMs developed in certain regions could also apply to others. Ms. Markoff also shared her belief that all participants will benefit from cyberspace CBMs. The U.S submission to the UNGGE this year appears as **ANNEX J.**

15. The Seminar deliberated on the distinction between regional-specific measures and measures applied internationally. Some participants reiterated that when devising regional CBMs, it is necessary to diagnose the types and forms of cyber threats that the region often encounters, and take into consideration the different level of experience in dialogue and cooperation. Others were of the view that the

CBMs being discussed in certain regional forum such as the OSCE are of a general and practical nature rather than something that would apply regionally. It was noted that certain measures are applicable both at the regional and international levels. Establishing crisis management mechanism is such an example.

16. The Seminar also debated on the applicability of the Convention on Cybercrime, which was drafted by the Council of Europe, to the region. While some believed that the Convention could be useful for other countries as well, others expressed reservations with the Convention. It was suggested that the UN should be the principle and core body where a general legal framework should be discussed. It was noted that the Council of Europe Convention was open for non-European membership and certain Asian countries had already joined.

Session 3 – Norms of Acceptable Behavior in Cyberspace

17. Dr. James Lewis, Senior Fellow and Director of the Center for Strategic and International Studies (CSIS) began his presentation by explaining the strategic context for cyber security. Cyberspace is not a unique environment. States will behave in this environment as they do in any other. He stated that to date, 41 nations are developing cyber military capabilities and that of them, 12 are developing offensive capabilities. He pointed out that obstacles to reaching an agreement, even non-binding ones, include state's unwillingness to allow their sovereign rights to be impinged upon as well as competing political agendas. He further deliberated on the International Code of Conduct submitted to the UN. The Code is not politically neutral and it is inconsistent with existing international practices and agreements such as the Universal Declaration of Human Rights. He underscored the importance of building norms before working on a treaty. He defined a norm as an expectation about responsible behavior by a state. The most important norms would establish state responsibility for actions in cyberspace that originate in their territory, which could be mainly achieved by extension and application of existing international law to cyberspace. If new norms are needed then it is important to specify where they are necessary. What is developed in the regional context need to be compatible with those adopted in other regional fora. He also looked forward to more progress within the ARF. His presentation appears as **ANNEX K.**

18. Dr. Nils Melzer from the Department of Security and Law of the Geneva Centre for Security Policy (GCSP) suggested three things to be addressed when figuring out a way to develop an international code of conduct: the encountered problems, the political environment, and the ultimate goal. With regard to the ways forward, he emphasized that the question is not whether but how the existing norms apply. States should agree on how far we can take existing laws to apply in cyberspace and not "cyberize" the problem. Where legal interpretation is not enough to cover the problems, new precise rules should be discussed. It is about time that the international community agrees on a preliminary code of conduct. He suggested that a first decisive and realistic step toward establishing the rule of law in cyber space would be to encompass the binding and non-binding aspects of norms into a single code of conduct. The first part, the binding part, may be restricted to

restating the basic rules of existing international law. The second part, the non-binding part, could comprise a compilation of best practices. He also invited participants to focus on forging a common goal of developing norms instead of merely promoting their political interests. A summary of his presentation appears as **ANNEX L.**

19. Mr. Nick Haycock, the UK representative and advisor to the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) introduced the history, membership and works of the UNGGE, and elaborated on the UNGGE mandate, which is to study existing and potential threats and possible cooperative measures with regard to information space. The current UNGGE topics include the applicability of existing international law in cyber space, approaches to developing norms and the role of the UN in developing CBMs. He discussed the ideological divide within the UNGGE and concerns over some content of the International Code of Conduct. Some parts of the CoC, if misused, could allow for the freedom of expression to be hindered. He also stressed that cyber CBMs could replace speculation with certainty and allow for greater predictability and avoid unplanned escalation of incidents. He suggested that the international community start small and build up and emphasized the importance of the role of regional security organizations such as the ARF and OSCE in their endeavor. His presentation appears as **ANNEX M.**

20. Mr. Alexander P. Minaev, Senior Counsellor from the Russian Embassy to the Republic of Korea, discussed how to deal with the information security issue more effectively. The issue of maintenance of international information security is global and thus can be addressed more effectively by utilizing an open and representative international forum like the UN. It was viewed that much of the modern realities were not reflected in the system of contemporary international law. The international community needs to agree upon a set of rules, standards or principles of conduct in the sphere of ICTs. Concrete proposals on this topic have already been introduced in the International Code of Conduct (CoC) for Information Security and Convention on International Information Security. He stressed that it doesn't matter what form a code of conduct takes. What matters is to reach consensus and establish common grounds. He further pointed out the regional efforts being taken by the Shanghai Cooperation Organization (SCO), OSCE and ARF. His speech appears as **ANNEX N**.

21. The Seminar deliberated on the correlation between CBMs and norms. Norms of behavior and CBMs are inseparable as developing norms are a crucial element in building confidence. Some participants stated that document-based discussions are requisite and encouraged the other countries to make a comment on the CoC so that it can be developed in the way that all the countries could agree upon. Other participants mentioned the need to accumulate understanding and experience to figure out the risk involved.

22. The Seminar also exchanged views on balancing the principles of sovereignty and universal rights, agreeing that human rights should be respected. The Seminar debated whether the CoC reflects the balance. Some participants

underlined that the CoC includes a similar language that was used in the International Human Right Declaration, with respect to human rights and the rules of law. Others expressed concern about the provisions of CoC, which circumscribe human rights on the premise of complying with relevant national laws. It was also suggested that the countries should try to find the common denominator and formulate the basic principles related to the issue.

23. The Seminar discussed the need to address laws of the armed conflict in dealing with cyber security. It was pointed out that in future conflicts, cyber attacks can be used as subsidiary strategies. Some participants viewed that it is very unlikely that states will give up on the use of cyber attacks, and emphasized that the international community should focus on how cyber operations are used and managed. Other participants pointed out that rushing into discussions on how to regulate the cyber operations by existing international law on armed conflict might mislead the international community to believe that states are seemingly preparing for cyber warfare, which is unacceptable. The Seminar also discussed the possible impact of cyber attacks on national critical infrastructure and national security.

24. On the issue of holding states responsible for any offensive action originating from their territories, participants discussed various cases relating to the scope of state responsibility. The Seminar observed that the states' willingness to take responsibility was an important factor and cited the example of Somalia and that it was considered a failed state due to its failure to address the issue of piracy off its coast.

Session 4 – Capacity-Building Measures in Cyberspace

25. Mr. Henry Fox, Director for Cyber Policy of the Department of Foreign Affairs and Trade of Australia noted that a precondition for developing confidence between states in cyberspace is good national cyber security policies and practices. He stressed the responsibilities of governments in providing cyber security that meets the standard and noted the importance of cooperation between governments, the private sector and civil society. He emphasized awareness-raising within governments, developing appropriate government policies and structures, and developing national capacities for incident response. Improved government coordination is also key to confidence building. He also introduced the results of the ARF Cyber Incident Response Workshop held in Singapore in September this year and proposed developing a work plan on cyber security. His speech appears as **ANNEX O**.

26. Mr. Bambang Heru Tjahjono, Director of Information Security of the Ministry of Communication and Information Technology of Indonesia explained the impact of ICTs and the interactive relationship between cyberspace and the real world. He further elaborated on the actors related to cyber security and the global legal framework. He suggested that the countries make and share a list of illegal activities and contents in cyberspace. He also elaborated on the national and international measures taken to expand Indonesia's capacity. He also reiterated that making good use of international and regional bodies is important and

introduced some of the proposals made by Indonesia to the International Telecommunication Union, World Conference on International Telecommunications and the UN General Assembly. His presentation appears as **ANNEX P**.

27. Mr. Muhammad Amir Malik from the Ministry of Information and Technology of Pakistan started his presentation by introducing the ICT profile of Pakistan and highlighted the need to promote capacity building in order to develop a sustainable and proactive culture in ensuring cyber security. He noted that capacity building involves understanding the obstacles that inhibit people, governments, international organizations and non-governmental organization from realizing their developmental goals while enhancing the abilities that will allow them to achieve measurable and sustainable results. He further diagnosed the current cyber security status in the Asia Pacific region and Pakistan, and enumerated efforts made at the national level. He also recommended that the ARF establish a working group at the technical level to develop a database of threats and possible remedies thereto; close the gap in human/institutional capacity building and experience among countries; fund scholarships for developing countries' government officers serving in the information security sector; continue holding seminars and workshops; introduce video conferences to provide training; and designate Point of Contacts and share the list. The presentation appears as **ANNEX Q.**

28. Mr. Jinhyun Cho, Senior Research Fellow of the Korea Computer Emergency Response Team Coordination Center (KrCERT/CC) of the Korea Internet and Security Agency of the Republic of Korea introduced various bilateral and multilateral cooperation measures to respond to cyber incidents and build confidence among the countries, including information sharing and confidence building. He also elaborated on the assistance programs carried out by KISA such as the APISC Security Training Course, which was launched in 2005. He highlighted the need to approach capacity-building activities from the perspective of the developing countries and prioritize the tasks to be undertaken rather than follow the examples of the developed countries. The presentation appears as **ANNEX R**.

29. Mr. Hoang Ngoc Quynh Lam, Police Officer of the Ministry of Public Security in Vietnam elaborated the concept and benefits of capacity building. He defined capacity building as a process of strengthening the ability of individuals, organizations and societies to make effective use of all resources in order to ensure the national and international information security. He recommended that the ARF participants enhance cyber security awareness of governments, businesses and Internet users; build a national legal framework on cyberspace that is consistent with international law; accumulate human capital in the cyber security area; strengthen the cooperation between law enforcement agencies and Internet management organizations; and launch and enhance international research on cyber security. His presentation appears as **ANNEX S.**

30. Mr. Ryan Jay Roset, Attorney of the Department of Justice of the Philippines addressed the legislative capacity building efforts of the Philippines with a focus

on preventing and addressing cyber crimes. He elaborated on the Philippines' national laws enacted to address cyber crimes including hacking, child pornography, offenses against confidentiality and privacy. He also explained the Philippines' framework including the roles of domestic departments dealing with cyber security. Creation of special task forces and training programs for law enforcement agencies were cited as examples of the Philippines' efforts to build capacity at the national level. His presentation appears as **ANNEX T.**

31. The Seminar deliberated on how to develop best practices and models in capacity building. Some participants believed that information exchanges could help developing countries establish new legal framework and enhance human capacity. Cooperation on training, digital forensic, monitoring and management were cited as possible measures. The Seminar also recognized that shared responsibility should be the main driving force for supporting capacity building of developing countries

32. The ASEAN Secretariat introduced various activities conducted at the ASEAN level. ASEAN is cooperating with countries like Japan and EU on conducting training workshops on cyber crime and legislation. ASEAN has a CERT network, which carries out drills to share information and focal points, foster closer relationships, and sharpen investigation coordination to deal with malware incidents. ASEAN CERT incident drills have been conducted 7 times thus far.

Closing Session – Wrap Up and the Way Forward

33. Mr. Jeong-sik Kang discussed some conclusions from the Seminar. He recognized the need to enhance ARF cooperative efforts to secure a safe, resilient and reliable cyberspace and develop CBMs. He noted that this Seminar provided a good opportunity for the ARF to discuss and assess how far we have come and where we need to go. He emphasized that the ARF participants must continue to work closely together through bilateral channels, the ARF and other international fora.

34. Mr. Nazrin noted that a wide range of issues were addressed in the Seminar and the exchange of frank and sensitive views among the participants reflected the maturity of the ARF process. He expressed the hope that more concrete proposals would be made by participants that could be more readily implemented. He stressed that the projects need not be many, but should be those that are useful to ARF participants. While he acknowledged the need to make a regional-specific approach to deal with cyber security, he was also of the view that we need to consider adapting existing measures to suit regional needs rather than starting anew.

35. Following the informal request of Timor Leste, participants were also urged to share their lessons learnt. In this regard, Malaysia was pleased to share with Timor Leste and with interested participants its lessons learnt from drafting its National Cyber Security Policy which has been implemented since 2006. Malaysia was also pleased to share its experiences in conducting cyber crisis exercises involving various organizations related to the critical national

information infrastructure. Cyber crisis exercises were designed to assess and improve the readiness of its critical national information infrastructure against cyber attacks.

36. In closing, the Co-Chairs conveyed their deep appreciation to all participants, experts and the ASEAN Secretariat for their cooperation and invaluable contribution to the Seminar, which was convened for the first time to address the specific topic of confidence building measures in cyberspace.

37. The Seminar noted the following specific recommendations as a way forward for the ARF to effectively implement confidence building measures in cyberspace :

    a. Review previous discussions carried out within the ARF Framework and consider the suggestions and recommendations made by the ARF participants;

    b. Review discussions in other international and regional fora related to cyber security including the UN, Conference on Cyberspace, Shanghai Cooperation Organization, OSCE, APEC, etc and consider those within the regional context;

    c. Cooperate and exchange information to develop best practices and assist capacity-building of developing countries in the area of Cyber Security;

    d. Continue to discuss developing acceptable norms of state behavior and CBMs in cyberspace;

    e. Promote implementation of the ARF Statement on Cooperation in Ensuring Cyber Security; and

    f. Explore the possibility of holding a follow-up workshop or seminar on cyber issues in 2013.

38. The Seminar expressed gratitude to the Republic of Korea and Malaysia for their co-chairmanship of the ARF. They also thanked the Government of the Republic of Korea for their warm hospitality and excellent arrangements in hosting the ARF Seminar on Confidence Building Measures (CBMs) in Cyberspace.

■■■