Co-Chairs' Summary Report of the
ARF Workshop on Measures to Enhance Cyber Security
– Legal and Cultural Aspects
Beijing, China, 11-12 September 2013

Introduction

1. Pursuant to the decision of the 20th ASEAN Regional Forum (ARF), held in Bandar Seri Begawan on 2 July 2013, the ARF Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects was convened in Beijing on 11-12 September 2013. The Workshop was co-chaired by Mr. Jia Guide, Deputy Director-General of the Department of Treaty and Law, Ministry of Foreign Affairs of the People's Republic of China, and Mr. Md Shah Nuri Md Zain, Undersecretary, Cyber and Space Security Division, National Security Council of Malaysia.

2. Representatives from all ARF participants, except Brunei Darussalam, Cambodia, the Democratic People's Republic of Korea, Mongolia, Pakistan, Papua New Guinea, Sri Lanka, and Timor-Leste attended the meeting. A representative of the ASEAN Secretariat and speakers from the United Nations Office of Drugs and Crime (UNODC) and the Council for Security Cooperation in the Asia Pacific (CSCAP) were also present. The List of Participants is attached as **ANNEX I.**

Opening Session - Welcome and Opening Remarks

3. The Co-Chairs welcomed the participants to the Workshop. Mr. Md. Shah Nuri Md Zain outlined the objectives of the Workshop. He looked back at the roots of the ARF and its achievements in contributing to maintaining peace and security in the region. Entering its 20th year, new and emerging security challenges such as cyber threats and cybercrimes demand renewed efforts from all ARF participants to address these challenges collectively. He expressed hope that ARF participants continue to foster dialogue and cooperation to tackle these challenges.

4. H.E. Mr. Zheng Zeguang, Assistant Minister of Foreign Affairs of the People's Republic of China, delivered his opening remarks. He underscored the great importance that the ARF has attached in addressing cyber security issues through the ARF statements and the various meetings and activities in this area. He emphasized the importance of establishing the rule of law as the basic approach to enhancing internet governance and cyber security, indicating that the principles of national sovereignty and non-interference in other's internal affairs enshrined in the UN Charter should be safeguarded. He touched upon the notion of cyber culture. Citing the relevant conclusion of the Information Society Summit in 2003, he highlighted the necessity to recognize the cultural elements behind the Internet public policies and to promote international cooperation in the spirit of mutual respect and inclusiveness. Mr. Zheng also elaborated basic elements to achieve a just and equitable international order in cyber space, including advancing the formulation and implementation of international rules on

cyberspace by giving full play to the role of the UN as the main channel. He expressed hope that the Workshop would enable ARF participants to strengthen communication, enhance mutual trust, and promote cooperation to build a peaceful, secure, open and cooperative cyberspace. His opening remarks appear as **ANNEX II**.

5. H.E. Datuk Mohamed Thajudeen Abdul Wahab, Secretary of the National Security Council, Prime Minister's Department of Malaysia, in his opening remarks expressed appreciation to the Government of the People's Republic of China for co-chairing and co-hosting the Workshop. He underscored the strong reliance of all countries in the world on information and communication technology (ICT) as a means to achieve progress in the digital age. This reliance has presented not only new opportunities but also new challenges and threats. He observed that the majority of cyber security incidents are transnational in nature and therefore cannot be addressed by one country alone. On this note, he emphasized the need to cooperate, collaborate and combine the ARF participants' talents and ideas in order to achieve a viable and credible cyber security approach. His opening remarks appear as **ANNEX III**.

Session I – Recent developments of national and regional practices on cyber security

6. Ms. Shariffah Rashidah Syed Othman, Principal Assistant Secretary of the Cyber and Space Security Division, National Security Council of the Malaysian Prime Minister's Department, outlined Malaysia's cyber threat landscape including online fraud, cyber terrorism, threats to critical national information infrastructure (CNII), and potential leakages or thefts of national confidential information. She emphasized the implications of cyber security threats to Malaysia's national security which prompted the adoption of a National Cyber Security Policy with a main objective of the protection of CNII. She also outlined Malaysia's national cyber security governance under the ambit of the National Security Council which on preservation of national identity, protection of the national digital border, and enhancing education and awareness of positive use of ICT in society. A whole-of-government approach is necessary to implement this policy on a national level. Her presentation appears as **ANNEX IV**.

7. Ms. Michele Markoff, Deputy Coordinator of Cyber Issues, Department of State of the United States, recognised the importance of addressing cyber security threats on a national and international level. She outlined the United States' national policy on protecting its critical infrastructures and pointed out since the majority of critical infrastructures are owned by the private sector, it is imperative that effective public-private cooperation is established and implemented. At the international level, she highlighted the United States' efforts in promoting a robust cyber security culture through various United Nations General Assembly Resolutions on cyber security since 2000. She emphasized the significant achievements of the UN in raising global awareness on cyber security culture but also underscored the importance of other regional and international organizations in this area.

8. Mr. Shi Xiansheng, Deputy Secretary General of the Internet Society of China, outlined the work of the Internet Society of China (ISC) since its establishment in 2001 on promoting internet development in China and providing support to policymakers on internet-related issues. He elaborated on the rapid growth of internet use and dependence in China and highlighted the increased vulnerability from various cyber threats such as malware, Trojan horses, and phishing activities. He updated the Workshop on several bilateral efforts such as the agreement between ISC and the Korean Internet Society Agency (KISA) in combating phishing and other cyber security threats. His presentation appears as **ANNEX V**.

9. Mr. Henry Fox, Director of Cyber Policy, International Security Division of the Australian Department of Foreign Affairs and Trade, informed the Workshop on the efforts in the development of the ARF work plan on cyber security by Australia, Malaysia and Russia. He observed that the ARF's previous efforts on cyber security have focused mainly in criminal and terrorist use of the internet by non-state actors. On that note, he expressed gratitude to ARF participants who have contributed inputs to the work plan. He referred to the ARF's overall confidence building and preventive diplomacy mandate. He noted the mandate provided by ARF Ministers was to "develop an ARF work plan on security in the use of ICTs, focused on practical cooperation on confidence building measures", He also noted a suggestion to add the development of norms of responsible behavior in cyberspace to the objectives of the work plan and asked how did this proposal mesh with the ARF's purpose and with the specific mandate provided by Ministers. The draft work plan may be submitted to the next ARF ISG on CBMs and PD in Myanmar on November/December 2013. He informed participants that the ARF Workshop on Cyber Confidence Building Measures, co-chaired by Australia and Malaysia, will be convened in 2014. His presentation is attached as **ANNEX VI**.

10. Mr. Daniel Holton from the Embassy of Canada in China delivered a presentation on Canada's cyber security strategy. He outlined Canada's Cyber Security Strategy, launched in October 2010, which is built on three pillars, namely securing government systems, partnering to secure systems outside the government, and helping Canadians to be secure online. He informed the Workshop that a separate action plan to implement the Cyber Security Strategy for 2010-2015 was launched in April 2013 with a focus on both domestic and international efforts, including through engagement in international fora such as the ARF. He shared several lessons learned such as the importance of a whole-of-government approach and effort, continuous outreach to other levels of government and the private sector, early development of threats assessment, and a simplified description of the proposed approach. His presentation appears as **ANNEX VII**.

11. Mr. Mattias Lentz from the Delegation of the European Union in China reaffirmed the EU's commitment to a free and secure cyberspace with full appreciation and protection of universal human rights. He also reiterated the EU's support for the ARF's efforts in addressing cyber security issues. The EU is of the view that the Budapest Convention on Cybercrime is the pre-eminent guideline for international

cyber security governance. He underscored the EU's approach to cyber security governance which focuses on protecting and ensuring the freedom of expression and developing norms of respectable behaviour among states in cyberspace.

12. Professor Kwa Chong Guan, Co-Chair of CSCAP, informed the Workshop participants of the outcomes of the CSCAP Cyber Security Study Group in 2011 and the development of the CSCAP Memorandum No. 20 on Ensuring a Safer Cyber Security Environment. He outlined several assumptions which were made during the drafting of the Memorandum. He observed that although ARF participants have declared their intention to be more open and transparent in addressing cyber security threats, this intention is dependent upon states' preparedness to trust others. He shared CSCAP's perspective on the vulnerability of web-based operations and services His presentation appears as **ANNEX VIII**.

13. The Workshop exchanged views on the definition of cybercrime and cyber terrorism within the framework of ARF cooperation. Although individual ARF participants hold different opinions on this subject, the ARF has mainly focused on identifying and combating criminal and terrorist use of the internet.

14. The Workshop also exchanged views on the model of internet governance.

Session II – Capacity building to strengthen cyber security

15. Dr. Soranun Jiwasurat, Director, Office of Security, Ministry of Information and Communication Technology of Thailand, outlined Thailand's efforts in strengthening cyber security through its National Cybersecurity Policy Framework 2013 which consists of three main strategies, i.e. Cybersecurity Governance, Cybersecurity Emergency Readiness, and National Critical Infrastructure Readiness. He identified the lessons learned and remaining challenges in implementing. He invited ARF participants to attend the Connect Asia-Pacific Summit 2013 which will be convened in Bangkok on 18 November 2013. The outline of his presentation appears as **ANNEX IX** .

16. Dr. Du Yuejin, Deputy Chief Technology Officer of the National Computer Emergency Response Team and Coordination Center of China, shared his views on global cyber security trends and requirements. He proceeded to outline China's perspectives and lessons learned in enhancing cyber security and developing the capacity of relevant stakeholders. He emphasized the importance of trust among States and of international efforts to eliminate the digital divide on security. His presentation appears as **ANNEX X**.

17. Mr. Sazali bin Sukardi, Vice President of Research of CyberSecurity Malaysia, Ministry of Science, Technology and Innovation, began his presentation with the various levels of cyber threats that target strategic (state-sponsored cyber-attacks), middle (DDoS), and operational (cyber fraud, online gambling, cyber stalking, etc.) levels. He shared Malaysia's perspectives on cyber threats and reaffirmed the importance of strengthening the individual's cyber security

knowledge and capacity to offset the human factor as the weakest link. He proceeded to elaborate on Malaysia's efforts and initiatives in cyber security capacity building, such as developing a portal for information security professionals and conducting domestic and regional cyber incident drills and exercises. His presentation is attached as **ANNEX XI**.

18. Mr. Choi Su-woong, Deputy Director, Ministry of Foreign Affairs of the Republic of Korea shared the experiences of the Republic of Korea in cyber security capacity building. He proceeded to inform the Workshop participants of the upcoming Seoul Conference on Cyberspace 2013 which will be convened in Seoul on 17-18 October 2013. The Seoul Conference will focus on greater diversification of participating countries, enhancing awareness of cyber issues for developing countries, strengthening public-private partnership, and sharing of best practices in cybercrime, cyber security, and capacity building. His presentation appears as **ANNEX XII**.

19. Dr. Tobias Feakin, Director, International Cyber Policy Centre of the Australian Strategic Policy Institute (ASPI) shared his observation that capacity building, confidence-building measures and norms of responsible behaviour in cyberspace operate along a mutually reinforced continuum; capacity building, transparency and CBMs are short and medium-term activities which in the long run serve the long-term goal of norms building. He offered several recommendations on cyber security capacity building which the ARF could consider, namely 1) sharing approaches to cyber policy making; 2) building regional cyber security baselines and standards, including through an ARF statement on the benefits of raising cyber security standards; 3) conduct trainings and simulations on crisis management and incident response; 4) reinforce existing cybercrime relationships and best practices; and 5) creative utilization of the private sector through the sharing of threat data and best practices as well as conducting joint capacity building. Dr. Feakin's presentation is attached as **ANNEX XIII**.

20. Mr. Liu Song, Director, Cyber Security Issue Management of Huawei Technologies Co. Ltd. offered the private sector's perspective on addressing cyber security threats. He highlighted the different cyber security concerns of the government, operator, vendor and end user and the need to improve cyber security capacity through more cooperation among parties. He elaborated on the comprehensive manner of building the capacity of Huawei staff on all levels. His presentation is attached as **ANNEX XIV**.

21. The Workshop exchanged views on the implementation of public-private sector partnerships. Since governments are responsible for setting laws and regulations, it is crucial for the private sector to maintain very close cooperation with the government where they operate. Participants also emphasized the importance of building trust between the public and private sectors in order to facilitate, among others, the sharing of sensitive and/or confidential information.

Session III – Cultural dimensions in cyberspace

22. Dr. Basuki Yusuf Iskandar, Secretary-General of the Ministry of Communication and Information Technology of the Republic of Indonesia, highlighted Indonesia's cyber security ecosystem and strategy, encompassing not only legal and cultural aspects but also technical measures, organizational structures, capacity building, and international cooperation. He pointed out the social impact of increased dependence on the internet which, in particular, is affecting the younger generation. He informed the Workshop participants on the series of activities leading to the Internet Governance Forum (IGF) 2013 which will be held in Bali, Indonesia on 22-25 October 2013, and he extended an invitation for ARF participants to attend the events. His presentation is attached as **ANNEX XV**.

23. Ms. Michele Markoff delivered the United States' perspective on the cultural aspects of cyber security, namely that cultural considerations should not be reason to limit the expression and protection of basic human rights in the cyberspace. Markoff noted that the international community has affirmed at the UN Human Rights Council that individuals have the same human rights online that they enjoy offline. From the perspective of the United States, cybersecurity refers to the safeguarding of networks and systems and not on controlling content online.

24. Mr. Yang Jian, Vice President of the Shanghai Institute for International Studies, elaborated on the informatisation of Asian societies from a cultural standpoint. He underscored that societies have different adaptability to the reshaping of information and communication technologies (ICT), and that the international community should keep balance between seeking a set of universal norms governing the cyberspace and respecting cultural backgrounds of different countries. He suggested that the creation and acceptance/rejection of behavioral norms in cyberspace is an inherently cultural process. He provided an Asian outlook on the ways to mitigate the potential cultural gaps and conflicts in cyberspace, including narrowing the digital divide in Asian countries and strengthening Internet legal and ethical education that is suitable for local conditions while at the same time in consistency with international practices. His presentation appears as **ANNEX XVI**.

25. Mr. Zulkarnain Mohd Yasin, Head of Monitoring and Enforcement Division of the Malaysian Communications and Multimedia Commission, shared the Malaysian perspective on the cultural dimensions of cyberspace. He emphasized the importance of guarding, protecting, preserving, and promoting national culture and identity particularly in cyberspace. He highlighted examples of differences in interpretation where certain online content was considered offensive and illegal according to one state's laws but considered acceptable by other states' laws. His presentation is attached as **ANNEX XVII**.

26. Mr. Xu Peixi, Associate Professor at the Communication University of China, provided an historical and cultural view on global internet governance. He cited several events which generated online debates and discussions and offered insights into the thoughts of netizens. He introduced some observations from an international communication education project regarding global internet governance. The outlines of his presentation appear as **ANNEX XVIII**.

27. The Workshop exchanged views on the protection of national sovereignty and freedom of expression in the context of cyberspace. Some participants were of the view that freedom of expression in cyberspace should be protected in accordance with international standards. Some participants recognized the great importance of promoting cultural diversity to build an inclusive information society. Views were also expressed to emphasize that the internet governance belongs to sovereign rights of a State, and that the national identity and values should be respected and safeguarded in cyberspace.

Session IV – Regional cooperation in combating cyber crimes

28. Mr. Steve Honiss from the New Zealand Police National Cyber Crime Centre outlined New Zealand's national cyber security strategy and described relevant national agencies responsible for maintaining cyber security. He elaborated on New Zealand's regional cooperation engagements on cyber security, including with ASEAN, Interpol, and the Strategic Alliance Cyber Crime Working Group. He touched on the development of the Interpol Digital Crime Centre (IDCC) which would provide real-time capabilities to respond to cybercrime incidents. More recently he informed participants of New Zealand's dilivery of a ASEAN Cybercrime Workshop which was convened in Singapore on 14-17 May 2013. His presentation appears as **ANNEX XIX**.

29. Mr. Akhil Kumar, Director for Counter-Terrorism at the Ministry of External Affairs of India described the current state of internet use in India and the national laws which govern behavior in cyberspace, most notably the Information Technology Act of 2000. He elaborated on the provisions of the Act and the enforcement framework at the federal and state level. He identified several challenges to international cooperation on cyber security from the jurisdictional, legal, and technical aspects. He expressed hope that the Workshop as well as similar activities would be able to harmonize the various legal and cultural aspects of cyber security. His presentation appears as **ANNEX XX**.

30. Mr. Tsuyoshi Kitagawa, Principal Deputy Director of the International Safety and Security Cooperation Division, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan, presented an overview of Japan's efforts in promoting regional cooperation against cybercrime. He outlined Japan's Cybersecurity Strategy through national measures and international cooperation, particularly in the Asia-Pacific region. He described four common principles for successful international cooperation against cybercrime, and he highlighted how Japan's accession to the Budapest Convention on Cybercrime provided an avenue to fulfill these principles. He touched on various regional capacity-building and information exchange activities, including the upcoming inaugural ASEAN-Japan Ministerial Meeting on Transnational Crime which will be convened in Vientiane in September 2013. Mr. Kitagawa's presentation is attached as **ANNEX XXI**.

31. Mr. Adam Palmer, Senior Expert on Cybercrime and Emerging Crimes at the United Nations Office and Drugs and Crime (UNODC) presented an overview of the UNODC's mandates on cybercrime since 2009. He elaborated on the

UNODC's efforts in supporting international cooperation and capacity-building, such as through an open-ended intergovernmental expert group on cybercrime and a Global Programme on Cybercrime. His presentation appears as **ANNEX XXII**.

32. The Workshop exchanged views on practical cooperation in combating cybercrimes within the ARF context and the barriers to international cooperation. Some participants described the difficulties in determining and liaising with the national points of contact for cybercrime and the slow process of securing and sharing of electronic evidence. Diverse views were expressed in a discussion of the applicability of the Budapest Convention.

Session V – Role of states in cyberspace

33. Mr. Li Chijiang, Director of the Office of Cyber Affairs, Ministry of Foreign Affairs of China, elaborated his views on the role of States in cyberspace, including as the inheritor of cyber sovereignty and the facilitator of international cooperation. He outlined several suggestions on promoting and ensuring the role of States in cyberspace, highlighting that the United Nations should be the major platform to formulate international norms of responsible States' behaviour and that the Draft International Code of Conduct for Information Security (A/66/359) submitted by China, Russia and others to the UN General Assembly in 2011 can serve as a useful basis for relevant international process. He also advanced suggestions on priorities for cyber cooperation within the ARF framework, namely to formulate a regional code of conduct in cyberspace, to strengthen pragmatic cooperation of mutual benefits, and to assist developing countries in cyber security capacity-building. His presentation appears as **ANNEX XXIII**.

34. Ms. Michele Markoff outlined the United States' views on the role of the state in cyberspace, namely that states do not own or regulate cyberspace per se but instead act as one of many caretakers who work with all other stakeholders to ensure that the resource is available so all can benefit. The United States does believe that certain threats in cyberspace can constitute threats to national security and it is this area of work where states have a very important role to play. The United States viewed that states should strive to achieve international cyber stability through the framework of existing international legal norms. Markoff noted that the attributes of IT – no external observables, attribution is difficult, assessing state capabilities is difficult – mean that we need to develop predictability in state behavior. Along with norms, the United States supports the application of a synergistic international framework of practical confidence building measures: transparency measures which provide clarity of states' intentions and actions in cyberspace to avoid misinterpretation; cooperative measures to allow states to work together against common non-state cyber threats and build trust; and confidence and security building measures such as in the form of a self-selected voluntary community of responsibility to define state activities that are inherently destabilizing and which they can pledge to refrain

from. She highlighted the report by the United Nations Group of Governmental Experts (UNGGE) on cyber security, listed as UN document No. A/68/98.

35. Ms. Nadezhda Sokolova from the Department on New Challenges and Threats of the Ministry of Foreign Affairs of the Russian Federation presented an overview of the Russian approach to international information security. Russia, as a firm and consistent proponent of a peace-making approach, is strongly opposing the use of ICTs for military purposes. The initiatives to elaborate universal code of responsible conduct of states in information space such as the draft International Code of Conduct for Information Security presented to the 66th Session of the UN General Assembly by the SCO countries, are increasingly relevant. Russia firmly believes that the United Nations is playing now and should continue to play a leading role in promotion of international information security. Russia welcomes the 2013 report of the relevant UN Group of government experts which enshrines such important points as the key role of UN, the common interest of states in peaceful use of ICTs, the leading role of states in addressing challenges resulting from malicious use of ICTs, the need to continue to study how existing norms of international law shall apply to the state use of ICTs and that additional norms can be developed over time. Russia holds the view that to effectively combat crime in the use of ICTs there is a need to elaborate under the UN auspices a convention that would exclude the most controversial provisions of the Budapest Convention and ensure sovereignty and non-interference into the internal affairs of states. She highlighted that according to the International Covenant on Political and Civil Rights, the exercise of freedom of expression carries with it special duties and responsibility.

36. Mr. Zahri Yunos, Chief Operating Officer of CyberSecurity Malaysia, underscored the shift in cyber threats, particularly the shift from large-scale, widespread incidents to specific, targeted attacks and the shift from benign motivations to economically-driven motivations. He outlined Malaysia's views on the role of states in cyberspace according to four areas of concern, namely economic growth and development, protection of national values, domestic cyber security, and regional cyber security cooperation. He highlighted Malaysia's participation in several regional cyber security cooperation mechanisms, including the ARF, the Asia Pacific Computer Emergency Response Team (APCERT), and the Forum of Incident Response and Security Team (FIRST). His presentation is attached as **ANNEX XXIV**.

37. Participants commented on the changing landscape of the internet and whether governments were becoming more inclined to assume greater control of the internet and move away from the existing multi-stakeholder model such as practiced by the Internet Corporation for Assigned Names and Numbers (ICANN).

38. The Workshop exchanged views on how the ARF can contribute to regional cyber security cooperation in light of differences in national views and capacities and difficulties in harmonizing international practices and conventions with national laws and legislations. In this regard, participants were encouraged to refer to the UN General Assembly Resolution A/RES/64/211 which outlines possible avenues of developing domestic cyber security capabilities.

Closing Session

39. The Co-Chairs summarized and highlighted several key points from the discussions of the Workshop as follows:

    a. Cyber security issues are trans-boundary in nature, and thus should be addressed regionally in a holistic, integrated and comprehensive manner.
    b. The protection of critical national information infrastructure is vital as these critical information systems are vulnerable to various cyber security threats.
    c. Cyber security capacity building in developing countries shall be enhanced, so as to promote balanced progress in global informatization.
    d. Cyber space facilitates the free-flow of information and sharing of cyber cultures. The national sovereignty and internet freedom should be respected and safeguarded in a harmonious and balanced manner.
    e. States have different measures in adapting to cyber cultures. The national identities and values shall be respected in cyber space. It needs to promote cultural diversity in building an inclusive information society.
    f. Cyber crime is a global challenge. The legal issues and technical gaps that exist among States remain significant. Enhanced international cooperation is of great importance in combating cyber crimes.
    g. State has an international obligation and direct contribution towards ensuring the global cyber security and prosperity. The international community may need to adopt good practices of internet governance and norms of responsible behaviour by States such as in the form of international code of conduct as well as enhancing global collaboration in areas of common interest.

40. In closing, the Co-Chairs conveyed their deep appreciation to all participants, moderators, speakers, and the ASEAN Secretariat for their stimulating inputs and their invaluable contribution to the Workshop, which was convened for the first time to address the legal and cultural aspects of cyberspace. The Co-Chairs also expressed hope that the discussions on this topic will be continued to explore suitable collaborative initiatives to strengthen regional cyber security.

41. The Workshop expressed gratitude to China and Malaysia for their effective co-chairmanship. They also thanked the Government of the People's Republic of China for its warm hospitality and excellent arrangements in hosting the ARF Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects.

■■■