CO-CHAIRS' SUMMARY REPORT

2nd ASEAN REGIONAL FORUM INTER-SESSIONAL MEETING ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ARF ISM ON ICTs SECURITY)

Singapore, 28-29 March 2019

INTRODUCTION

1. Pursuant to the decision of the 25th ARF held in Singapore on 4 August 2018, the 2nd ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ISM on ICTs Security) was held in Singapore on 28-29 March 2019. The Meeting was Co-Chaired by Mr. Ng Hoo Ming, Deputy Chief Executive Operation, Cyber Security Agency of Singapore; Ms. Shariffah Rashidah Syed Othman, Director of Cyber Security Policy and International Cooperation, National Cyber Security Agency, Malaysia; and Mr Yusuke Arai, Minister and Deputy Chief of Mission, Embassy of Japan in Singapore. The Meeting was attended by representatives from all ARF Participants except Bangladesh, Brunei Darussalam, Democratic People's Republic of Korea (DPRK), Myanmar, Mongolia, Pakistan, Papua New Guinea, Sri Lanka. Representatives of the ASEAN Secretariat were also in attendance. The List of Delegates appears as **ANNEX 1**.

AGENDA ITEM 1: OPENING REMARKS BY CO-CHAIRS

2. In their opening remarks, the Co-Chairs expressed condolences to the Government of New Zealand and to the victims of the terrorist incident in Christchurch. Recognising the nature and complexity of the rapidly changing cyber security environment, the Co-Chairs reiterated the importance of confidence building measures (CBMs) in reducing conflicts and promoting trust in cyber space. As threats to security in the use of ICTs transcend geographical boundaries, the Co-Chairs also emphasised the need to enhance cooperation with governments as well as with the private sector. Recalling the objective of the ISM as a platform for more focused

dialogue on security in the use of ICTs among ARF Participants and in efforts to implement the ARF Work Plan on the Security of and in the Use of ICTs, the Co-Chairs further underlined that this ISM is in itself a meaningful example of confidence building in the ARF. The Co-Chairs further commended the successful convening of the 4th Open-Ended Study Group on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies (OESG) and expressed hope that the implementation of CBM#2: Sharing of Information on National Laws, Policies, Best Practices and Strategies as well as Rules and Regulations at this Meeting will contribute to the success of the ISM. In this regard, they looked forward to the fruitful discussions.

AGENDA ITEM 2: ADOPTION OF MEETING AGENDA

3. The Meeting adopted the Agenda, which appears as **ANNEX 2**.

AGENDA ITEM 3: CONSIDERATION AND ASSESSMENT OF PROPOSALS BY THE STUDY GROUP

3.1. Immediate Activities

4. On the implementation of CBM#4: Awareness-Raising and Information Sharing on Emergency Responses to Security Incidents in the Use of ICTs, the Meeting noted that Cambodia, Singapore and China as proponents will be developing a concept paper to convene a workshop to implement this initiative. The Meeting further took note that the Concept Paper will be submitted to the ARF Inter-Sessional Support Group Meeting on Confidence Building Measures and Preventive Diplomacy (ISG on CBMs and PD) scheduled to be held in Seoul in May 2019 and submitted to the ARF Senior Officials' Meeting (SOM) later that month for consideration. The Meeting noted that upon adoption by the 26th ARF, the proposed activities are intended to be convened in conjunction with the 5th ARF OESG in Malaysia in January 2020.

5. On the implementation of the ARF Workshop on Principles of Building Security in the Use of ICTs in the National Context, the Meeting noted that the Workshop, which aims to facilitate dialogue among ARF Participants and enhance understanding of the principles of building security in the use of ICTs security, is scheduled to be held in Singapore on 25-26 June 2019. The Meeting further noted that inputs and comments to the draft agenda of the Workshop, which appears as **ANNEX 3**, should be submitted to Singapore and Canada as the Co-Chairs of the Workshop.

3.2. Priority Areas for ARF ISM on ICTs Security

6. The Meeting noted that the proposed CBM #1: Establishment of ARF Points of Contact Directory on Security of and in the Use of Information and Communication Technologies by Malaysia and Australia, aims to provide a platform for communication among ARF Participants in the event of ICTs security incidents, to reduce tension and risk of conflict arising from misunderstanding and misperceptions. It was further reiterated that as countries may have different approaches in governing security in the use of ICTs, participation in the Directory was voluntary and non-binding. The Meeting also took note of the additional proposed paragraphs on the processes and procedures for the Directory. In this regard, the Meeting expressed in-principle support towards the proposal whilst noting that some ARF Participating Countries would need to seek confirmation from their respective capitals and will submit their confirmation and/or further inputs directly to the Co-Sponsors by 8 April 2019. The Concept Paper appears as **ANNEX 4.**

7. The Meeting deliberated on Singapore and the EU's proposal on workshop entitled Protection of Critical Infrastructures which was meant to serve as a practical avenue for ARF Participants to share information on the modalities and mechanisms in protecting the ICT-enabled critical national infrastructures. It was further noted that inputs to the proposal are being considered and that the updated proposal will be further circulated in due course. Taking into consideration the concerns raised by one delegation regarding the application and definition of the term CBMs within the context of this ARF ISM on ICTs Security, the Meeting noted the Co-Chairs' recommendation to seek guidance from the ARF ISG on CBMs and PD regarding the usage of the term CBMs in the ARF. The Concept Paper appears as **ANNEX 5.**

3.3. Other Proposals

8. The Meeting noted that no other proposals were tabled at this juncture.

AGENDA ITEM 4: DISCUSSION ON EMERGING ISSUES

9. New Zealand briefed the Meeting on the outcome of the 4th ADMM-Plus Experts' Working Group on Cyber Security (EWG on CS) which was held in Auckland, New Zealand in November 2018. The Meeting took note that the ADMM-Plus EWG on CS have established a Cyber Points of Contact Directory and that at present, 32 Points of Contacts from 16 ADMM-Plus countries have been identified and included in the Directory.

10. The Meeting took note that Russia would be organising an International Cybersecurity Congress (ICC) in Moscow on 20-21 June 2019, which was intended to be an international cross-industry platform dedicated to facilitate collaboration and discussion among government officials, business leaders and experts on security in the use of ICTs in combating current digital threats as well as to establish key areas of development aimed at escalating the global level of resilience to information threats. It was also noted that the event, scheduled during the Global Cyber Week, would highlight an extensive global online simulation exercise on computer attacks to critical financial institutions such as banks and its risk mitigation.

11. The Meeting also took note of the briefing on discussions on security of and in the use of ICTs under the auspices of the United Nations (UN) including the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) established by the resolution entitled "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" and the UN Open-Ended Working Group (OEWG) established by the resolution entitled "Developments on the Field of Information and Telecommunications in the context of International Security". The Meeting noted that the UNGGE was meant to examine existing and potential threats in the information sphere and identify the possible cooperative measures to address these threats, and that the UNGGE is required to produce consensus reports to be reported to the UN General Assembly (UNGA). It was further noted that to date, five UNGGEs have been convened wherein the first and fifth sessions were not able to produce consensus reports. Topics discussed within the UNGGE include a number of norms of responsible behaviour of states, confidence building measures, the need for capacity building and the applicability of international law to information space. It was further noted that the UNGGE was also intending to hold consultations with countries and organisations which were not members of the UNGGE, including the ARF, to provide inputs on the UNGGE process. It was reiterated that such consultations with the ARF was not intended to seek the combined views of the ARF but rather to have discussions with ARF Participants and seek the views of individual ARF Participants on issues that should be addressed at the UNGGE, which would be reported to the UNGA in 2021.

12. Meanwhile, an Open-ended Working Group (OEWG) on international information security (IIIS) is for the first time being created within the UN. It means that all the UN Member States without exception will be able to participate in its work. The OEWG will be authorised to consider a whole range of IIS-related issues. It pays special attention to further work on norms, rules and principles of responsible conduct in information space, to the issues of applicability of international law and to building digital capacity of developing countries; and to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United

Nations. Such a mandate is granted to the UN structure negotiating IIS issues for the first time. The Open-ended Group will allow each country to make its contribution to the discussion of these topics and adoption of the relevant decisions. The OEWG is a fully fledged UN General Assembly body that may develop any documents and recommend them to Member States, including draft international treaties. OEWG will held inter-session consultations with non-State actors – business, non-governmental organizations and scientific community, for exchanging views on the issues covered by the group mandate. It was underlined that despite their differences, both the UNGGE and OEWG were intended to remain complimentary towards one another and promote international discussions on security in the use of ICTs. On the issue of the use of ICTs in criminal purposes, whilst recognising that this threat continues to be on the rise, the Meeting also took note that there was yet to be a common understanding on the definition of this phenomenon nor a common approach to address this issue.

13. The meeting took note of the presentation of the Russian side on elaboration of unified glossary on security in the use of ICTs.

AGENDA ITEM 5: COUNTRY PRESENTATIONS OF CBM#2

14. The Meeting took note of Australia's briefing on the implementation of Australia's International Cyber Engagement Strategy, which was published in 2017. Since then, Australia has implemented the strategy which focuses on a number of chapters including digital trade, cyber security, cybercrime, international security and cyber space, internet governance, human rights, and technology for development. The Meeting also noted Australia's position on the application of international law to cyber space, wherein Australia was of the view that there was a need for the international community to have a dialogue on how international law applies in cyber space. The Meeting further took note of Australia's cyber cooperation programme which was launched in 2017 and now has a budget of AUD 44 million, encompassing five pillars, including international cyber stability framework, cybercrime, cyber incident management, best practices use of technology for development, and human rights and democracy.

15. The Meeting noted that Canada had recently reviewed its 2010 national cyber strategy, which was now designed to be flexible and adaptable to the changing environment, in consultation with the Canadian public. Launched in June 2018, the updated strategy focuses on three objectives: (i) secure and resilient Canadian systems, (ii) innovative and adaptive ecosystems, and (iii) effective leadership, governance and collaboration, with a budget of over CAD 500 million. To deliver on

the first objective, Canada had dedicated CAD 160 million over the course of five years to support the creation of the National Cybercrime Coordination Unit, which was aimed to expand on the capacity of the Royal Canadian Mounted Police (RCMP) to investigate and respond to cybercrime and establish a coordination hub for domestic and international cybercrime investigations. On its second objective, Canada intends to work with partners to drive investment and foster cyber research and development. Finally, Canada aimed to take a leadership role domestically and internationally, through effective governance and collaboration to advance cyber security in Canada and shape the international security environment, including through the creation of the Canadian Centre for Cyber Security, which was meant as a single source of expertise, guidance and support for government, private sector and the Canadian public. Canada's presentation appears as **ANNEX 6.**

16. The Meeting took note that China released its "International Strategy of Cooperation on Cyberspace" in 2017 which includes four principles: peace, sovereignty, shared governance and shared benefits; six strategic goals: safeguarding sovereignty and security in cyber space, developing a system of international rules, promoting fair internet governance, protecting legitimate rights and interest of citizens, promoting cooperation on digital economy, and building platforms for cyber culture exchange; and action plans: (i) peace and stability in cyber space; (ii) rule-based order in cyber space; (iii) partnership in cyber space; (iv) reform of global internet governance systems; (v) international cooperation on cyber-terrorism and cybercrimes; (vi) protection of citizens' rights and interests including privacy; (vii) development of digital economy and sharing of digital dividends; (viii) global infrastructure development and protection; and (ix) exchange of cyber cultures. China's presentation appears as **ANNEX 7.**

17. The Meeting noted that in response to the changing cyber environment, Japan had updated its cyber security strategy in 2018 which includes Japan's basic visions of cyber security, termed as Cybersecurity Ecosystem. These consist of three efforts: Mission Assurance, Risk Management, and Participation, Coordination and Collaboration. To achieve these visions, Japan applied a cross-cutting three pillar policy approach, namely: (i) Enabling socio-economic vitality and sustainable development; (ii) Building a safe and secure society for the people; and (iii) Contribution to the peace and stability of the international community and Japan's own national security. On the first pillar, Japan was advancing cyber security as a value creation driver, achieving a supply chain that creates values through diverse connections, and building secure Internet of Things (IoT) systems. In order to build a safe and secure society for the people, the Meeting noted that Japan was implementing a number of measures including strengthening and improving security in governmental bodies and related entities, building an information sharing

framework, strengthening incident readiness against massive cyberattacks, as well as increasing protection of critical infrastructures through public and private sector cooperation. On the third pillar, Japan was committed to ensure a free, fair and secure cyber space as well as make concerted efforts to strengthen their capabilities for defence, deterrence and situational awareness, and to strengthen their international cooperation and collaboration on cyber security. Japan's presentation appears as **ANNEX 8.**

18. The Philippines briefed the Meeting on its cyber security laws, best practices and strategies. It was noted that in efforts to govern cyber security, the Philippines issued the Electronic Commerce Act in 2000, a Cybercrime Prevention Act in 2012 and established the Department of Information and Communication Technologies (DICT) in 2016. It was noted that in the Philippines, cyber security matters are undertaken by different departments according to their major responsibilities, i.e. the Department of Justice for law enforcement, DICT for protection, and protection of military networks by the Department of National Defense. The Philippines had also developed a National Cybersecurity Plan 2022 with the objectives of ensuring cyber resilience and protecting critical infrastructures, government networks, businesses and their supply chains as well as the public through, among others, the establishment of the National Computer Emergency Response Team (CERT) and the implementation of programmes embedded in the Plan. The Philippines' presentation appears as **ANNEX 9.**

19. The Meeting took note of Russia's briefing on its national efforts in the firled of security in the use of ICTs including through the establishment of its 2012 National Computer Incident Response and Coordination Center (NCIRCC), tasked to secure the critical information infrastructure facilities in the Russian Federation and the creation of its national CERT. It was noted that the services provided by the NCIRCC include proactive services, security management services and reactive services. The Meeting further noted Russia's experience in countering computer attacks, which occurred during major events such as the Winter Olympics, President's Press Conference and Presidential Elections. It was underlined that there was a need to promote cooperation, information sharing and inter-agency coordination as these elements were key to the successful disruption of computer attacks. The Meeting also noted that the NCIRCC was the single point of contact for computer incident response in Russia and would be included in the ARF Points of Contact Directory on Security of and in the Use of Information and Communication Technologies. Russia's presentation appears as **ANNEX 10.**

20. The United States briefed the Meeting on its National Cyber Strategy, released in September 2018, which outlined the steps undertaken by the U.S. government to

advance an open, interoperable, reliable and secure Internet. It was noted that the Strategy was structured around four pillars, which include a number of priority actions to enhance capabilities in the cyber space. The first pillar, Protecting the American People, the Homeland, and the American Way of Life, sought to secure federal networks and information, secure critical infrastructures as well as combat cybercrime and improve incident reporting through capacity building, enhancing international cooperation and sharing of best practices. Pillar II: Promoting American Prosperity, sought to foster a vibrant global technological ecosystem and innovation as well as develop stronger cybersecurity workforce through education and improvement. Under Pillar III: Preserving Peace through Strength, the strategy sought to counter disruptive, destructive or otherwise destabilizing acts in cyberspace through the promotion of responsible state behavior, ensuring the application of consequences for irresponsible state behavior, and countering malign online influence and information operations. On Pillar IV: Advancing American Influence, the strategy seeks to promote an open, interoperable, reliable and secure Internet by urging countries to promote internet freedom, advance a multi-stakeholder model of internet governance, and building international cyber capacity. The United States' presentation appears as **ANNEX 11.**

AGENDA ITEM 6: CONCLUSION AND WAY FORWARD

21. The Meeting noted the suggestion for discussions in future ISMs on ICTs Security to include issues of data flow protection and related international laws, cybercrime, and updates on UN processes i.e. the UNGGE and OEWG. Recognising the importance of these issues whilst, at the same time, noting that these issues were also being discussed in other ASEAN-led mechanisms, some ARF Participants were of the view that discussions at this ISM should avoid duplication and could perhaps be deliberated on a case-by-case basis. The Meeting also noted the request for proposals to be tabled at future ISMs on ICTs Security be circulated in advance to allow ample time for ARF Participants to consult their respective line agencies. Moving forward, the Meeting noted that the tenure of the current Co-Chairs would expire in April 2020. In this connection, the Co-Chairs encouraged other ARF Participants to consider expressing their interests to co-chair this ISM to ensure continuity of discussions in this area of cooperation.

AGENDA ITEM 7: CLOSING REMARKS BY CO-CHAIRS

22. In their closing remarks, the Co-Chairs reiterated that while there were differing views on a number of issues, the ARF ISM on ICTs Security remained as a useful

platform for dialogue and confidence building among its Participants. It was further noted that the successful implementation of CBM#2 reflected the positive indication of confidence among ARF Participating Countries and had paved the way for the implementation of other initiatives.

ACKNOWLEDGEMENT

23. The Co-Chairs thanked all delegates for their active contribution to the Meeting and looked forward to continued cooperation in this area. The Meeting expressed appreciation to the Co-Chairs for the effective co-chairmanship and thanked the Government of Singapore for its hospitality as well as the excellent arrangements of the Meeting.

ISSUES REQUIRING FOLLOW-UP ACTION

No.	Key Decision/Issues	Timeline	Follow-up By
1.	ARF Participants to provide comments/inputs to the Concept Papers of the proposed initiatives for submission to the ARF ISG on CBMs and PD and the ARF SOM.	8 April 2019	The Proponents of the initiatives and all ARF Participants.
2.	To seek guidance from the ARF ISG on CBMs and PD regarding the definition and application of the term CBMs.	3 May 2019	Co-Chairs of the ARF ISM on ICTs Security.

■■■