CO-CHAIRS' SUMMARY REPORT
ARF SEMINAR ON OPERATIONALIZING CYBER CONFIDENCE BUILDING MEASURES
REPUBLIC OF SINGAPORE, 21-22 OCTOBER 2015

Introduction

1. Pursuant to the decision of the 22nd ASEAN Regional Forum (ARF) in Kuala Lumpur, Malaysia on 6 August 2015, the ARF Seminar on Operationalizing Cyber Confidence Building Measures (CBMs) was held in Singapore on 21-22 October 2015. Mr Wong Yu Han, Director, Cyber Security Agency of Singapore and Ms. Michele Markoff, Deputy Coordinator for Cyber Issues, U.S. Department of State co-chaired the Seminar.

2. Representatives from 19 of 27 ARF participants, attended the Seminar, along with a representative of the ASEAN Secretariat and experts from international organisations and academia, including Organisation for Security and Cooperation in Europe, International Institute for Strategic Studies, the Australian Strategic Policy Institute, and S.Rajaratnam School of International Studies 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

2. Mr David Koh, Chief Executive of the Cyber Security Agency of Singapore said that it was important for countries to foster strong cybersecurity cooperation with each other through platforms such as the ASEAN Regional Forum, given the transboundary nature of the cyber threat. To do this, it was important for countries to work towards build strong networks between agencies and officials at all levels. Events like the present seminar were helpful in fostering a common understanding on cybersecurity issues. He said that Singapore strongly supported ASEAN efforts to foster regional cybersecurity cooperation and advance cyber capacity building efforts.

3. H.E. Kurt Wagar, Ambassador of the United States of America to the Republic of Singapore, thanked the delegates for their outstanding, broad participation. He said that long term peace and international growth depends on respect for international law and norms, including respect for human rights. The U.S. is committed to promoting the ARF as a bulwark of stability and security in the region. The Ambassador commended the ARF on the adoption of the work plan on security of and in the use of information and communication technologies (the 'ARF ICT Work Plan'). The ARF ICT Work Plan emphasizes issues of

common concern. Cyber norms and CBMs can contribute greatly to international security. Now is a good time to fulfill the recommendation to produce a regional contact group for information sharing and communication on cybersecurity.

Session I: Update on the ARF ICT Work Plan

Co-chairpersons: Michelle Markoff, Deputy Cyber Coordinator, U.S. Department of State, and Wong Yu Han, Director, Cyber Security Agency of Singapore.

4. Mr. Henry Fox, Director Cyber and Space Policy, International Security Division, Department of Foreign Affairs and Trade, Australia provided an update on cybersecurity in the context of ARF. He noted that ARF has a long-standing tradition of work on regional security and confidence building measures in many areas. In 2012 the SOM approved the development of a plan which was adopted at the ARF Ministers meeting on 6 August 2015. The plan focuses on 1) promoting transparency to reduce risk of conflict; 2) raising awareness on threats; 3) enhancing practical cooperation on cybersecurity; and 4) improving cooperation, including improving capacity, to deter criminal and terrorist use of ICTs. The plan provides practical suggestions for focus, including CBMs, raising awareness for non-technical personnel, developing points of contact network and capacity building. Mr. Fox also reviewed the March 2014 ARF cyber CBM workshop. The overall goal was to reduce the risk of state on state miscalculation and conflict in cyberspace. The workshop identified a need to identify cyber leads within government; noted internal and regional coordination and communication were essential; found that cyber incident response should be coordinated with broader national security mechanisms; noted technical and policy communities needed to be connected; concluded building capacity was a concern as regional capacity varied widely; and encouraged communication between governments and the need to develop a regional contact network. Mr. Fox thanked Singapore and the U.S. for organizing the seminar.

5. Mr. Bernard Low, Consultant, with the Security Policy Standards and Regulation Division, Infocomm Security Group, Infocomm Development Authority of Singapore, spoke on cybersecurity initiatives for the Infocomm sector. He said cybersecurity was important because disruptions of ICTs could have disastrous consequences since the Infocomm (Information and Communications) sector is an integral part of the economy and government. Advanced persistent threats (APTs) will continue to evolve. In Singapore, regulations require and encourage cooperation between government and the private sector through information sharing and cyber exercises. iDA was mindful of adopting a proportionate regulatory approach that expected more from large incumbents with higher potential risks and impacts, and less compliance costs from smaller operators

with less potential risk and impact, so as to not impose an undue burden on smaller companies.

6. Mr. Md Shah Nuri Md Zain, Undersecretary Cyber and Space Security Division, National Security Council, Malaysia spoke on the Malaysian lessons learned from previous events and key takeaways on the ARF ICT Work Plan. ROK and Malaysia held an ARF CBM workshop in 2012. China and Malaysia held a workshop on measures to enhance cyber security legal and cultural aspects in 2013. Australia and Malaysia held a CBM workshop in 2014. China and Malaysia held an ARF workshop on cyber security capacity building in 2015. Mr. Zain said the 2014 workshop focused on baseline CBMs like cyber points of contact and transparency measures and conducted a practical desktop exercise. The 2013 workshop focused on link between legal and cultural perspectives and cyber security; the adaptability of cyber cultures; domestic law and cultural diversity; and national sovereignty and Internet freedom. He also reviewed the common themes for cyber issues in workshops co-hosted by Malaysia. He noted gaps Malaysia sees, including: poor follow-up to the workshop and need for ARF mechanisms to ensure the effectiveness of the workshop; less discussion on deep technical and enforcement issues; less participation from industry and private sector; and not enough participation from necessary government entities.

7. Co-Chair Markoff noted that technical officers will not make decision about what to do about an incident, will not be making attribution, will not be determining the policy responses to respond to incidents. This is the role of policy-makers. She urged attendees to think about how they can operationalize the recommendations from the seminar and take them back to technical and policy counterparts.

Session II: ARF Cyber CBMs - Moving Forward

8. Ms. Jessica Woodall from the Australian Strategic Policy Institute (ASPI) spoke about the categories of cyber CBMs and how they might be implemented in ARF, using lessons from the UNGGE, the ARF ICT Work Plan, and ASPIs work. The region’s challenges are its diversity and differing priorities. Some countries have low capacity. Some have too much capacity and/or internal organizational confusion. Efforts such as the Global Forum for Cyber Expertise, CERT community, APNIC, and policy training can be helpful. The recent UN GGE report highlighted recommendations, four of which are highly relevant: 1) development of cyber points of contact; 2) adoption of voluntary national arrangements to classify the scale and seriousness of cyber incidents for information sharing; 3) voluntary provision by states of categories of critical infrastructure; 4) exchange of personnel in areas like incident response and law

enforcement and encouraging exchanges between think tanks and academic institutions. The ARF ICT Work Plan can be best implemented by sharing of information on national laws policies, best practices and strategies; raising awareness for non-technical personnel and policy makers on threats and countermeasures through technical training for policy experts, training programs in local languages; conducting surveys on lessons learned in dealing with threats by tapping into the large capacity and expertise of the private sector which has a stake in online security.

9. Kohei Kawaguchi, National Security Policy Division, Foreign Policy Bureau, Ministry of Foreign Affairs, Japan spoke on the UN GGE efforts and Japan's efforts. The consensus report adopted July 2015 focused on existing and emerging threats; the applicability of international law; norms, rules and principles for the responsible behavior of states; CBMs; international cooperation and capacity-building; and recommendations for future work. The GGE had similar opinions on CBMs. Japan will promote policy dialogues with relevant states through multilateral and bilateral dialogues, through holding cyber workshops with ASEAN and through promoting CBMs. Japan engages in a large number of bilateral and trilateral dialogues. He noted that CBM capacity building requires focus on laws and standards, building human resources and public-private partnerships in the context of the human resources of each country, in addition to technology.

10. Caitriona Heinl, Research Fellow, Centre of Excellence for National Security, S Rajaratnam School of International Studies (RSIS), Nanyang Technological University Singapore spoke on OSCE CBM efforts and translating international agreements into action plans. She reviewed the points in #2 of the ARF ICT Work Plan. She noted the OSCE recommended that states have domestic legislation promoting information sharing. She said we need a way to take recommendations from the seminar and create a mechanism for moving them forward after the meeting. We also need to capture lessons learned, but the difficulty may be in how to make this knowledge intelligible and useful. She argued that more communication and understanding of ongoing activities might allow states to leverage this work and avoid duplication. More discussion should be had on cultural differences, but this doesn't mean that norms on human rights can be ignored. Ms. Heinl recommended a number of steps to build confidence: informal solutions like joint task forces are a good way to overcome challenges; there is an absence of agreed terminology, consider the OSCE decision of 2013 to create a glossary; need to consider manpower concerns on how the contact database will be maintained; there is a need to meet regularly and account for staff rotations and the fact that there may not have been MFA contact points for all countries.

11. Ms. Enekin Tikk-Ringas, Senior Fellow for Cyber Security, The International Institute for Strategic Studies Middle East, spoke on military cyber issues. She noted it's important to ensure countries developing military cyber capabilities produce doctrines and publicly acknowledge the creation of these capabilities. The development of military capabilities isn't as much of a concern as the use of these capabilities in ways that increase the risk of conflict. Military capabilities are increasingly transparent, and the existence of these capabilities are not necessarily destabilizing. They can be useful for increasing security. The use of these technologies for lethal effects are the concern and require countries to abide by their international obligations. Non-state actors, which work under the appearance (officially or non-officially) of their national governments for personal or political gain, are a high concern both to other countries and to the countries in which they operate. Non-state actors' abilities to operate usually results not from state permission, but from a lack of cybersecurity and lack of agreement on norms. Attack maps don't even demonstrate adversaries, instead they represent attack routing schemes. (map.norsecorp.com map).

12. Ben Hiller, Cyber Security Officer, OSCE Secretariat, Transnational Threats Department spoke about the OSCE experience and lessons learned on cyber CBMs. OSCE states follow the recommendations of the UN GGE in operationalizing CBMs. PC.DEC/1106: is the initial set of OSCE CBMs to reduce the risks of conflict stemming from the use of ICTs. OSCE CBMs fall into three areas: 1) those which allow states to read another State's posturing making cyberspace more predictable; 2) CBMs which offer opportunities for timely communication and cooperation to defuse tensions during incidents; and 3) CBMs which promote national preparedness and due diligence to address cyber/ ICT challenges. He said CBMs are important because they can help states put down their guard and cooperate on common solutions; it is the start of additional engagement. CBMs will not stop intentional conflict but they can stop unintentional conflict; and non-implementation does not shine a good light on a State. 66% of the OSCE countries have implemented CBMs. Key challenges are 1) overcoming internal constraints, e.g. difficult political environments; maintaining cyber as a diplomatic/foreign policy topic; simple things like creating POC lists are challenging. 2) Overcoming regional fragmentation: strategically the UN GGE is the focus but there should be inter-regional exchanges e.g. OSCE - ARF discussions; 3) overcoming capacity constraints for countries which don't have the right tools to engage in the CBM process. OSCE focused on transparency first. Next are cooperative measures for processes and capacity building and then focusing on stabilizing measures.

13. Ivan Minaev, Expert, Federal Security of the Russian Federation spoke on the Russian experience with cybersecurity. The Islamic State in the Levant has been compromising Russian sites for their purposes. The Russian malware

library has 17 million examples. Malware is increasingly found in things like mobile applications and some malware on desktops cannot be removed. Methods like botnet control are becoming much more sophisticated, as some attacks use over 2 million devices. The Internet of Things (IOT) will increase the number of vulnerable network devices. Malware must be outlawed and heavily prosecuted in all countries. Mr. Minaev called for states to build stronger domestic legislation and international cooperation, coordinate our efforts and develop a secure information environment.

14. Mr. Md Shah Nuri Md Zain, Undersecretary Cyber and Space Security Division National Security Council, Malaysia spoke on how to move forward with ARF cyber CBMs. He reviewed the six major areas of cooperation on the ARF ICT Work Plan with possible areas for implementing these areas. Two major areas of effort for implementation have been the study group and the workshops/seminars for supporting the study group's work. The ARF work plan is closely guided by the work of the UN GGE. He suggested 1) focusing CBMs at the regional level to produce practical outcomes 2) aligning with the UN GGE and 3) establishment of the study group and continuing seminars and workshops to support CBMs.

15. Ms. Michelle Markoff noted the UN GGE work to share national cyber strategies and plans for resolving cyber incidents, sharing points of contact for managing cyber incidents, and creating stability measures and standards of restraint for cyberspace.

Session III: Cyber Incident Management - National and Regional Lessons Learned

16. Mr. Loh Phin Juay, Deputy Director, Cyber Security Agency of Singapore, spoke about CSA's cyber incident management approach. He mentioned that CSA was established in April 2015 under the Prime Minister's office and provides dedicated and centralized oversight of national cyber security functions. Some of CSA key focuses include critical information infrastructure protection, partnership and outreach, research and analysis, cyber incident response, capability development, and industry engagement. He shared about the incident reporting and response framework of the Critical Information Infrastructure sectors in Singapore. In addition, CSA also operates the National Cyber Security Centre which oversees the handling of incidents across all sectors and is in charge of the National Cyber Incident Response Team which can augment/pool resources to respond to threats.

17. Bridget Walsh, Joshua Kim and Sheila Flynn from the U.S. government spoke about U.S. cybersecurity organizations. Ms. Walsh from the Department of

Homeland Security noted that the Department of Justice and FBI lead for investigation and enforcement of cybercrime, the Department of Homeland Security leads protection of non-military government networks and critical infrastructure and the Department of Defense leads on national cyber defense. The Department of State coordinates international engagements. DHS focuses on prevention, mitigation and recovery from cyber incidents and works closely with the private sector. DHS operates the national CERT and the National Cyber Integration Center which integrates technical and policy responses. Policy level groups work with their respective agencies to organize whole of government responses to incidents. The U.S. has 16 critical infrastructure sectors and DHS engages with the leadership of these sectors regularly and works with them on incidents. DHS is working with government agencies to provide a common baseline and best practices for cybersecurity. DHS also focuses in information sharing and incident response.

18. Mr. Joshua Kim from the Federal Bureau of Investigation (FBI) spoke about the FBI which is responsible for detecting, disrupting, investigating and prosecuting cybercrime. The FBI has worldwide partnerships with national law enforcement and with agencies like Interpol. FBI incident response strategies rely on partnerships with the private sector and other agencies who detect the activity. FBI does not mitigate incidents but does publish notifications for industry about malware and adverse actors. Law enforcement cooperation internationally is primarily through the MLAT process. International challenges are consent monitoring, data retention policies in other countries, whether countries have data sharing legislation and technical/ capacity limitations. DOJ has a 24/7 call center which can preserve evidence.

19. Ms. Sheila Flynn from the Office of the Secretary’s Coordinator for Cyber Issues spoke about the State Department (DOS) role. She noted the U.S. interest in working with foreign partners on incidents as they occur, ranging from routine information sharing on incidents to response on major events. DOS uses diplomatic channels to supplement technical law enforcement requests for assistance to reinforce the requests and communicate the seriousness of the incident to policy-makers.

20. Mr. Masanori Sasaki, Deputy Counsellor, National Center for Incident Readiness and Strategy for Cybersecurity (NISC), Japan spoke about lessons learned from cyber incident management. NISC handles information on law, policy and strategy, situation information on incidents, threats, actors and best practices, as well as technical information on malware and vulnerabilities. NISC communicates domestically with the Government Security Operation Coordination team, agency CSIRTs, JP-CERT/CC and other partners, law enforcement and the private sector. Internationally NISC works through formal

channels like bilateral cyber dialogues, multilateral frameworks like FIRST, informal meetings and communications. It also has an email (poc@nisc.go.jp) for any issue. GSOC monitors networks and warns CSIRTS of threats. CSIRTS respond and report back. Cyber Incident Mobile Assistance Teams provide technical assistance and advice to Ministry CSIRTs when requested. NISC also has channels with the private sector and international partners but is still developing practical means to work with them.

21. Mr. Park Ji Yong, Senior Research Associate, KrCERT/CC, Korean Internet and Security Agency, spoke about Korean incident response and KrCERT's experience. He described a number of cyber incidents which KrCERT had seen and responded to over the last several years. KrCERT has developed a system for fighting zombie PCs where it works with the ISPs to identify the Zombie PC through the IP address. Then it sends a popup with remedial software to the zombie PC

22. Ms. Angela Marie De Gracia, State Counsel, Department of Justice (DOJ), Philippines spoke about cyber incident management in the Philippines. The Cybercrime prevention act passed in 2012 is the first comprehensive cybercrime law in the Philippines. The Philippines has expressed an interest and has been invited to participate in the Budapest Convention on Cybercrime. The DOJ Office of Cybercrime is responsible for all domestic and international cooperation on cybercrime. DeGracia noted that there are challenges in developing capacity, as well as in designating lines of effort. Further, there is a lack of capacity among the legal community who understand the technology, as well as how to deal with evidence.

23. Mr. Harme Mohamed, Malaysia Communications and Multimedia Commission (MCMC) spoke on the Malaysian experience. MCMC regulates all matters relating to information and communications. MCMC operates the SKMM Network Security Sector (SNSC). This is the sector lead for information and communication sector (one of 10 critical infrastructure sectors). As an example, SNSC works with the Internet Banking Task Force, Malaysian ISPs and the global CERT community to combat online banking phishing. They collect phishing emails and websites, and work to take down the websites. They also work within the MCMC to raise awareness about cybersecurity among the public. SNSC also organized an IASP cyber drill where mock threats are handled by the IASPs CERT with SNSC as the coordination entity.

24. Mr. Michael Debolt, Digital Crimes Officer, Interpol spoke about the consistent themes from the presentations. The Digital Crime Center could serve to coordinate points of contact among states, as well as for capacity building. Interpol's Digital Crimes Center has three pillars: capacity building, training, and

a digital crime center. The digital crime center has a digital investigative support unit and a digital forensics laboratory. The digital investigative support unit has representatives from member countries who leverage private and academic partnerships to identify emerging cyber threats, and they respond to requests from member countries. The cyber fusion center is a gateway for global cyber threat intelligence sharing and a secure and neutral workspace where law enforcement the private sector can tackle cybercrime together. It is the point of initial assessment for cyber threats, it conducts intelligence analysis and it is the focal point for intelligence sharing on threats and incidents. They issue Purple Notices which are emerging threats or modus operandi criminals are using and Cyber Activity Reports which are tactical, actionable intelligence. The Cyber Fusion Centre can be contacted by countries at (cfc@interpol.int) for international law enforcement coordination and reporting of attacks.

25. The Seminar further discussed how to move forward toward implementing CBMs. A number of states noted that they are committed to implementing the ICT Work Plan and that events such as this seminar were useful in the implementation process. Some states, such as Australia and the United States noted that the group should consider developing points of contact, while others, such as Russia, argued for further studies on how workshops could improve implementation.

Table Top Exercise

26. This exercise was conducted in the form of a facilitated discussion exercise and used an escalating cyber security incident scenario which enabled inputs from the Seminar participants. The focus of this exercise was on the whole-of-government responses to cyber security incidents and on communication between governments, involving both technical and policy aspects. The participants were required to consider questions and issues on operational responses including law enforcement, collaboration with private sector, information sharing, as well as coordination and cooperation at operational and policy levels. During this exercise, participants demonstrated their whole-of-government understanding of their respective national systems for identifying, managing and responding to cyber security incidents of national security significance. Additionally, the groups were encouraged to discuss how communication among governments might best achieve their goals.

Table Top Exercise: Managing/ Responding to a Serious Transnational Cyber Incident

27. The Table Top Exercise focused on information gathering, coordination, mitigation, law enforcement and technical capabilities in the context of a multi-

nation cyber incident. Participants were required to consider gathering a comprehensive picture of the incident, consider which actors would be involved at the national and international levels, as well as potential technical and public communications issues. Participants discussed the roles of ministries, regulators, CERTS, and the private sector, as well as among states, to share information, reduce tensions, mitigate damage, support law enforcement, etc. The groups also discussed which ministries should lead efforts on mitigation, law enforcement and communication. Lastly, States discussed what technical capabilities they might employ during such events to assist in mitigation, reducing tension, and law enforcement.

28. Important discussions were raised during this session, including:

a. Public communication: working to reassure the public.
b. Coordination: ensuring all relevant agencies have a role and which should lead efforts.
c. Mitigation: all relevant bodies should work together to stop further damage to systems
d. Gathering information: understanding which agencies need what information and how to disseminate.
e. Technical: ensuring all relevant organizations with technical capability are working together.
f. International cooperation: working with foreign government counterparts at all levels to share information, mitigate and coordinate: how can ARF help with this? What agencies should reach out to their foreign counterparts? At what level?

29. The exercise allowed participants to consider lessons learned, such as:

a. The importance of contact points, and knowing who to communicate with ahead of time;
b. The importance of technical capabilities, such as CERTs, and with law enforcement;
c. The need to have strong links among policy and technical officers and organizations in order to best deal with crises;
d. The value of exchanging information among ministries, and working together to communicate to the public.

30. Challenges identified during the exercise were:

a. Lack of preparation and cyber strategies;
b. Lack of capacity in some states;
c. Varying levels of capacity among states;

d. The large role of privately owned infrastructure in dealing with a potential crisis;
e. Attribution;
f. Understanding fast changing technology;
g. Clearly defined roles for government ministries during an attack;
h. Communication among governments.

31. Further questions among participants included:

a. Is there a procedure through ARF for technical assistance during crises?
b. Are there existing regional institutions that could coordinate response plans?
c. What roles would international organizations such as Interpol or the IMF play in such a crisis?
d. What is the appropriate level for coordination?
e. At what point is it appropriate to reach out to foreign governments?

32. Participants discussed a number of takeaways during the conclusion of the exercise:

a. It is better to have broad regional communication, across a range of professionals (law enforcement, technical, political) during crises;
b. Policymakers should consider discussing attribution to attempt to avoid blaming one another which could lead to escalation;
c. Understanding among technical, political and foreign counterparts is critical in ensuring communication is effective;
d. Clear lines of effort and leads are necessary to ensure effective responses to crises;
e. ASEAN and/or ARF could play an important coordination role in assisting communication or information dissemination among members;
f. Understanding who and at what level to contact in which ministries, before a crisis begins, is necessary;
g. Legal structures for enforcing cyber crimes and sharing information can help mitigate attacks and allow for cooperation;
h. CERTs have an important role in limiting the damage of attacks, if they are linked to one another;

33. Ms. Markoff concluded the wrap up session by noting the strong desire among members to address these issues. There is recognition that this is a common concern and that responding to them multilaterally can give us more impact than working alone. She was heartened by the level of interest and hoped that can move us forward towards operationalizing these efforts.

Session VI: Discussion on the Way Forward on ARF Cyber CBMs: What and How to Implement

34. Mr. Fox noted an impressive level of understanding among the group about the challenges we face with operationalizing CBMs. He believed the group felt it was time to launch the POC directory. The point isn't to develop a telephone book of everyone who is involved in cyber within a government. The objective is to list the types of contacts who would be useful in helping to prevent a cyber incident from spiraling out of control. The list should be focused on specific responsibilities, not agencies since governments organize each other in different ways. Australia will submit this proposal through the normal ARF process and launch it when there is sufficient consensus. The representative from Malaysia looked forward to working with Australia and ARF to implement this initiative.

35. The Indonesian representative noted that ICTs can be a great benefit to development but present challenges. Indonesia proposes establishment of cooperation between CERTs either through the ASEAN mechanism or another mechanism. Wants to promote cooperation via exercises for CERTs. National CERTS have a key role to play in incident response but this requires significant capacity which is lacking in some countries. We should build the capacity of partner countries in critical infrastructure protection and work to build collaboration and cooperation. One of the best ways to promote cooperation is to bring countries together. The exercise will promote CERT readiness.

36. Mr. Pierre Louis Lempereur, First Counsellor at the EU Delegation to Singapore noted that the EU has developed a cybersecurity strategy. The goal is to ensure the domain remains free, open and secure. The international community is in the midst of developing norms in cyberspace. He wanted to acknowledge the work by the UNGGE to analyze the impact of international law in cyberspace and craft norms. The EU believes regional fora have a key role to play in building effective CBMs. The EU will organize a workshop with Malaysia and the Netherlands 2-3 March in Kuala Lumpur to focus on more concrete and practical steps and integrating international cooperation into international incident response. The EU representative commented that they would like to integrate political cooperation for incident response into the technical cooperation already underway.

37. The Russian representative was surprised there was not more discussion of the study group and urged the speedy establishment of the study group which will research practical measures for CBMs.

Concluding Remarks by Co-Chairs

38. Ms. Markoff said we've come a long way and we have a shared awareness of the challenges and importance of cooperating on cyber incidents. She commended the commitment to a follow on workshop and thanked the attendees for spending the time to come to the event. She thanked the co-chair Singapore for the venue, lovely food and patience in organizing the conference.

39. Mr. Wong Yu Han thanked everyone for their patience and attendance at the conference. He noted the persistence the group has shown in engaging with these difficult issues. He urged continued steady progress so we can move into the implementation of confidence building measures. He thanked Michelle and all the organizers of the event and said he looked forward to the next workshop by our Malaysian and EU partners.

■■■