CHAIRMAN'S REPORT OF THE TRACK II NETWORK OF ASEAN DEFENCE AND SECURITY INSTITUTIONS (NADI) WORKSHOP ON CYBER SECURITY: EMERGING CHALLENGES AND RESPONSES

20-22 NOVEMBER 2013

TRADERS HOTEL, SINGAPORE

1. The NADI Workshop on Cyber Security: Emerging Challenges and Responses, organised by the S. Rajaratnam School of International Studies (RSIS), was held at Traders Hotel, Singapore on 20-22 November 2013.

2. Representatives from Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam attended the workshop. The list of participants who attended the workshop is attached in Annex I. RSIS Senior Fellow Mr Tan Seng Chye chaired the workshop.

Welcome Remarks by Mr Tan Seng Chye, Senior Fellow, RSIS and Chairman of NADI Workshop

3. Mr Tan Seng Chye welcomed NADI members to the workshop, which is the first meeting of this nature in the ADMM track. He also highlighted the importance of cyber security in the present day and age covering all sectors of commerce and business, finance and banking, transportation including aviation and maritime security, society's daily activities and even in the defence and security sectors. The next decade is likely to witness a 'revolution in information technology' and governments will be concerned with the risks and new cyber threats which could arise. Noting the widespread use of the Internet in today's global landscape, Mr Tan pointed out that according to software company McAfee, cyber attacks have led to between US$300 billion and US$1 trillion dollars of global losses annually. As such, the responsibility to safeguard cyber space cannot be the work of a single country or organisation.

4. Citing Singapore as a case in point, Mr Tan said that the government has set aside S$130 million dollars to enhance the country's cyber security framework. Likewise the Singapore Armed Forces has also established a Cyber Defence Operations Hub to strengthen its cyber defence capabilities. As such, there are opportunities for militaries and security agencies of the Asean countries to enhance information sharing and cooperative initiatives to jointly manage transnational cyber security challenges. The workshop provided a platform for NADI members to present on their countries' national approach and strategy in responding to emerging cyber security threats. The NADI participants could exchange views and make recommendations to the ADMM track on cooperation among the militaries of the Asean countries.

Session One: Presentations by cyber security agencies and experts on cyber security challenges facing the region, as well as governments' approaches and responses to the emerging challenges

Opening Address on "Cyber Security: Singapore's Response to Emerging Challenges" by Mr John Yong, Director (Infocomm Security & Assurance), Infocomm Development Authority, Singapore

5. Mr John Yong highlighted the widespread use of infocomm technology in Singapore at both the business and individual levels and that as a whole the country is highly connected. Nevertheless the Internet is susceptible to attacks which are multifaceted and thus extremely challenging to deal with. As such, there is a need for the government and other stakeholders to be more vigilant and further strengthen the security of Singapore's infocomm infrastructure and systems.

6. On the Singapore's government response, Mr Yong shared that Singapore is actively involved in securing the cyber environment. The National Infocomm Security Committee (NISC) was established in 1997 to set infocomm security policies and strategic directions at the national level. The need to obtain greater public partnership was also reflected in the implementation of the first Infocomm Security Masterplan from 2005 to 2007, which focused on levelling up the capabilities of the public sector to deal with cyber threats. A second five-year Masterplan was put in place in 2008

which widened its focus to include critical infocomm infrastructure. This included the launch of the Cyber Security Awareness Alliance, with partners from both the public and private sectors. The Alliance aims to engage three main segments of the population: (i) school students; (ii) tertiary students and small and medium enterprises, and (iii) the community-at-large.

7. On the recent launch of Singapore's five-year National Cyber Security Masterplan from 2013 to 2018, Mr Yong emphasised three key areas of focus: (i) to enhance the security and resilience of critical infocomm infrastructure; (ii) to increase efforts to promote the adoption of appropriate infocomm security measures among individuals and businesses; and (iii) to grow Singapore's pool of infocomm security experts so as to meet the rising demand for cyber security expertise.

8. Mr Yong shared that the Singapore government has also recently launched a $130 million dollar plan to aid research and development to enhance its cyber security capabilities. This will be funded by the National Research Foundation, the Ministry of Home Affairs and the National Security Coordination Secretariat so as to support research efforts to make computer networks and other IT systems more secure, reliable and resilient, while boosting the pool of qualified personnel to deal more effectively with increasingly sophisticated cyber attacks. Mr Yong also stressed that no country could work in silos on cyber security, and that international collaboration is a key factor for successful cyber security responses.

Presentation on "Cyber Security: Challenges at the Regional Asean Level and Possible Responses" by Ms Caitriona Helena Heinl, Research Fellow, Centre of Excellence for National Security (CENS), RSIS, as an expert in this field

9. Ms Caitriona Heinl highlighted on the need to safeguard both civilian and military fields from cyber threats that could harm its networks and information structure. To do so, international and regional cooperation are required. However, at present, efforts to adopt comprehensive cyber security strategies remained slow. Among the challenges faced include: increasing volume and complexity of threats, problem of attribution, growing number of state and non-state actors, as well as a lack of common understanding of cyber terminology.

10. On the changing cyber landscape in Asean, Ms Heinl pointed out the increasing numbers of Internet users, greater connectivity and higher probabilities of cross-border cyber threats and noted the varying levels of infocomm technologies (ICT) development and adoption among Asean member states. Within the defence sector, there was a need to constantly review the evolving risks, assist in building a resilient cyber security architecture, incorporate principles of usage, as well as having confidence building measures including preventive diplomacy through exchanges among defence and military officials.

Adoption of Agenda

11. The meeting adopted the agenda for the Workshop as attached in Annex II and the programme for the Workshop appears in Annex III.

Session Two: Briefings by NADI member delegations on national strategies and responses to cyber security challenges, including how their militaries can play a role in contributing to the overall national efforts on cyber security

Briefing on Singapore Armed Forces Cyber Defence Operations Hub by Mr Tan Seng Chye, Senior Fellow, RSIS and Chairman of NADI Workshop

12. Mr Tan Seng Chye briefed the meeting on the Singapore Armed Forces (SAF) Cyber Defence Operations Hub (CDOH). Established in June 2013, the CDOH aims to enhance the robustness and resilience of the SAF's networks and systems against cyber threats. It monitors MINDEF/SAF networks on a 24/7 basis, and when faced with cyber attacks, responds swiftly to identify, contain and neutralise threats. The CDOH is comprised of a core planning group, responsible for the planning and management of contingencies and crisis events, as well as three task entities undertaking: (i) cyber security ops monitoring; (ii) cyber incident responses; and (iii) provide engineering solutions to recover from a cyber attack, while guarding against

the recurrence of a similar threat. Complementing the whole-of-government approach, the CDOH works closely with the Singapore IT Security Authority (SITSA) and IDA.

Presentation on "Thailand's Perspective on Asean Cyber Security Strategic Framework: The Joint Asean Cyber Security Center" by Senior Group Captain Poomjai Leksuntarakorn, Director, Regional Studies Division, Strategic Studies Center (SSC), Thailand

13. Senior Group Captain Poomjai Leksuntarakorn elaborated on two types of cyber defence measures. Active defences are electronic countermeasures designed to strike attacking computer systems and shutdown cyber attacks in midstream, while passive defences are the traditional forms of computer security used to defend computer networks, such as system access controls, data access controls, security administration, and secure system design. The most effective way to ward off cyber attacks is to use a layered defence framework of active and passive defences.

14. He added that given the increasingly connected IT systems and infrastructures and the emergence of transnational challenges, there is a need for cooperation among states on cyber security. He proposed that the Asean nations establish a Joint Asean Cyber Security Center to share information and conduct joint training on cyber security issues. He also made four recommendations for joint cooperation at the Asean regional level. First, Asean nations should invest in developing comprehensive core information security technology. Second, risk and vulnerability analysis should be carried out at all levels among Asean nations. Third, Asean should implement an early warning system for cyber threats. Fourth, Asean countries should develop agreements on cyber active defence under international law.

Presentation on "Cyber Security: The Malaysian Armed Forces' Perspective" by Colonel Johnny Lim Eng Seng, Director, Policy Research, Malaysian Institute of Defence and Security (MiDAS), Malaysia

15. Colonel Johnny Lim noted that due to Malaysia's geographical location and plural society, the country is vulnerable to many security concerns which could undermine its security and sovereignty. Although the physical threat of non-traditional adversaries cannot be discarded – as was proven in the recent Lahad Datu incident – it

is the growing threat of cyber attacks which are of concern now. He noted two significant aspects of cyber challenges. First, cyber warfare levels the field for the less technologically advanced states. Second, there is a blurred distinction between the civilian and military domains.

16. He highlighted some of the Malaysian Armed Forces' (MAF) cyber security measures, such as constantly updating, surveillance and monitoring of cyber developments, and exchanging intelligence with regional counterparts on cyber threats. He also suggested that a national-level strategic platform could be established to create awareness on cyber security measures among all relevant agencies. At the regional level, Colonel Lim proposed that the Asean nations could consider holding joint cyber defence exercises, institutionalising regular dialogues on cyber security, and developing a network of Asean cyber security organisations.

Presentation on "Cyber Security Challenges and Responses: Indonesia's Perspective" by Brigadier General Haryoko Sukarto, Chief, Center for Strategic Studies of TNI, Indonesia

17. Brigadier General Haryoko Sukarto briefed the meeting on cyber security challenges and responses from Indonesia's perspective. The digital technologies are great enablers, but they can be misused by actors to conduct criminal actions that may exploit nations, business and individuals. Critical infrastructures, such as government operations, storage and delivery systems, banking and financial markets, as well as military control and command are targets of such cyber challenges. For Indonesia, there are two main challenges that relate to the development of Asean cyber security, namely (i) the lack of awareness among Asean member countries on both national and regional cyber security; and (ii) the limited human resources in the field of cyber security and defence, in both quality and quantity, within each member country.

18. In order to deal with the challenges, Indonesia proposed five steps that Asean member countries should consider to undertake. The first step is establishing agreement to guarantee that cyber space will not be used as a platform for Asean member countries to attack one another. The second step is enhancing cooperation programmes in developing Asean's cyber security awareness. The third step is establishing the Asean's cyber security centre through enhancement of the existing cooperation

programmes. The fourth step is establishing Asean Cyber Rule of Engagement as common guidance. The fifth step is enhancing cooperation programmes through education and training on Asean's cyber security as part of capacity building measures.

Presentation on "Collaborative Efforts on Securing Asean Cyber Space: A Defense Perspective" by Colonel Dr Arwin Sumari, Principal Lecturer of Asymmetric Warfare Study Programme, Indonesian Defense University

19. Colonel Dr Arwin Sumari highlighted that cyber space threats might transfer across borders to neighbouring countries, and therefore Asean nations should establish efforts to increase security measures. Indonesia proposed Asean collaborative efforts in cyber security by including collaborative usage of military information infrastructure, conduct of cyber army exercises, collaborative usage of information resource, control of information network infrastructure, control of information flow and conduct of collaborative cyber space defence.

20. To reduce the risk of cyber crimes and attacks toward the region, Indonesia proposed to extend the collaboration efforts to non-Asean member countries, including Japan and China, to obtain wider cyber space protection. The presentation concluded that because of the transnational nature of cyber security challenges, Asean should protect the wider domain of cyber space by collaborating in military and non-military sectors to minimise the impact of cyber attacks.

Presentation on "The Philippine Cyber Landscape and Government Initiatives to Enhance the Country's Cyber Security" by Colonel Danilo Chad Isleta, Chief, Office of Strategic and Special Studies, Armed Forces of the Philippines

21. Colonel Danilo Chad Isleta's presentation noted the Philippine focus on cyber space as part of its national interest as it is an indispensable tool to support economic growth, equitable development and effective government. However, it is noted that there is an increase of cyber crimes attacking official government websites, conducting web defacement and disturbances. The latest challenge of terrorist recruitment through the Internet highlights cyber crime's close relation to violent crime. To counter cyber

challenges, the Philippines subscribe to the guiding principles set by the international community, including the UN Resolution on Combating Criminal Misuse of Technologies and Asean Cyber Security Initiative. The Philippines cyber strategy is based on the National Security Policy, the Philippine Development Plan and the Philippine Digital Strategy.

22. The Philippine government conducted campaigns to increase digital literacy, consumer protection awareness and enforcing cyber crime laws with effective law enforcers. The guiding principles on cyber space legal conduct continuously evolves to cope with dynamism of cyber threats and appointed government departments to regulate the cyber space. There are lessons learnt from the Philippines that would be useful to Asean's effort on security cyber space. The first lesson is continuous evolution of legal and institutional tools to address and manage the fluidity of cyber space. The second lesson is that cyber crime affects different countries in varying degrees depending on the extent of the legislative enactment of a country. Lastly, cooperation should not be limited to the intergovernmental level, but also be multi-sectoral as cyber security is a shared responsibility among different sectors of the society.

Presentation on "Mapping Brunei Darussalam on the Cyber Security Landscape" by Ms Refana Mohd Juanda, Research Officer, Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS)

23. Ms Refana Mohd Juanda's presentation explored the current cyber security landscape which is confronted by three main challenges: evolution of malware, technology-enabled crimes and the advent of cyber warfare. Out of the three, Brunei Darussalam is particularly affected by the first two challenges. In recent years, the nation has experienced high level of virus infections, spamming and website defacement. With regards to technology-enabled crimes, Brunei Darussalam is concerned with the trend of exploitation of vulnerable groups such as children, as a result of widespread use of the Internet among the population.

24. In response, Brunei Darussalam has introduced laws and various initiatives to mitigate and prevent cyber threats, with the aim of increasing awareness among the public and

deter potential offenders. To overcome future threats, it still needs to build on capacities and strengthen the security of its cyber infrastructure. It seeks to address these limitations through continuous inter-agency and multilateral cooperation, at the same time, contributing towards regional efforts for peace, security and stability.

Presentation on "Cyber Security and Measures to Enhance Cyber Security in Asean Armed Forces Cooperation" by Lieutenant General Nguyen Dinh Chien, Director General, Institute for Defense Strategy, MOD Vietnam

25. Lieutenant General Nguyen Dinh Chien emphasised that the advent and continuous development of the Internet have not only brought about huge benefits to human society, but has also result in a variety of cyber security challenges. Cyber weapons have a number of prominent advantages: (i) they are more effective than conventional weapons; (ii) the costs involved in developing solutions are relatively low compared to other conventional weapons; (iii) it is more difficult to identify the perpetrators of cyber-attacks; and (iv) their destructive consequences can be compared to nuclear, biological, or chemical weapons.

26. In order to effectively enhance cyber security, the armed forces of Asean countries should implement concurrently a number of measures such as properly investing in securing defence and military information; sharing information and training aimed at raising awareness of cyber security threats for not only officers, soldiers, defence staff but also commanders of units at all levels of the armed forces through organising training courses. The Asean countries should also boost cyber security cooperation as well as promote cooperation with the armed forces of the Dialogue Partners in dealing with cyber security challenges. He also stressed that apart from the existing six areas of cooperation, the ADMM-Plus should consider adding cyber security to its areas of cooperation.

Presentation on "Cyber Security of Myanmar and the Role of Defense Services" by Major Naing Lin Aung, Deputy Department Head, Defence Services Computer Department, Myanmar Army

27. Major Naing Lin Aung highlighted that the Myanmar government is in the process of preparing to protect and counter the threats and criminal activities in cyber space. The country also participates in organisations such as TSUBAME (Internet threat monitoring system), IMPACT (International Multilateral Partnership Against Cyber Threats) and APCERT (Asia Pacific Computer Emergency Response Teams) so as to better prepare itself to respond to cyber attacks. He added that cyber attacks represent a threat to the political, social, economic and education activities of the country and that the cooperative efforts among Asean member states are needed.

28. On Myanmar's initiatives, he highlighted the use of E-office application programmes within the defence ministry as well as transferring of information within a military network. He added that although the defence ministry was unable to presently provide effective cyber support at the national level, there are plans to form a cyber security task force.

Presentation on "Lao PDR Perspective on Cyber Security" by Mr Souksan Khaiphom, Deputy Head Office, Department of Military Science-History, Ministry of National Defence, Lao PDR

29. Mr Souksan Khaiphom shared that the Lao PDR government has actively promoted the development of telecommunication in recent years through the provision of 3G and 4G mobile networks to its citizens. At present its Internet infrastructure has enabled Lao PDR to connect to neighbouring countries such as China, Thailand, Vietnam and Cambodia.

30. On the government's policy on cyber security, Mr Souksan said that ICT is being promoted as an engine for social and economic development and that legislation has been established for governing and managing the development and usage of ICT. In addition, the Lao Computer Emergency Response Team (LaoCERT) is designated as the contact point to handle incidents and issues pertaining to computer and Internet security. He highlighted the importance for Asean member states to share experiences in cyber security and for cooperation among governments and national bodies in developing cyber security strategies.

Presentation on "Issues in Cyber Security" by Lieutenant Colonel Sokretya Sowath, Chief of Public Relations, Department of Development, Ministry of National Defence, Cambodia

31. Lieutenant Colonel Sokretya Sowath defined cyber war as leveraging the Internet for political, military and economic espionage activities. Due to its sophistication, it was difficult to prepare for and defend against a cyber war. The more developed a country is, the more it is dependent on technology and thus vulnerable and prone to hackers.

32. He added that cyber space conflicts could arise in three areas: civilian-civilian; civilian-state and state-state. There is a need to measure and weigh the respective priorities accorded to these three perspectives to accurately measure the national-level impact of cyber conflicts. Due to its vast domain, it was difficult to manage and control and as such, there was a need to differentiate between the type of attacks and to look for regional solutions such as those at the Asean level.

Session Three: Consideration of recommendations to enhance cooperation among militaries of the Asean countries and related security agencies in cyber security at the bilateral and regional levels

Exchange of views and consider recommendations to enhance cooperation of the militaries of the Asean countries and related security agencies

33. The NADI participants had an extensive exchange of views following their presentations on national approaches and responses to cyber security challenges which can affect all aspects of their nations' activities and societies as a whole. Today, all activities at the national, regional and global levels are dependent on infocomm technologies. This makes the threats of cyber security and meeting cyber challenges an urgent priority of governments as national activities such as transport, business, commerce, banking and finance, and the people's daily lives, can be disrupted by cyber attacks. Infocomm technologies play an important role even in the defence and security sectors, which can also be seriously threatened by disruptions in the event of cyber attacks. Thus there should be national approaches and responses as well as cooperation at the bilateral and multilateral levels among states to respond to cyber security challenges.

34. The militaries of the Asean countries could play an important role as part of the national efforts to combat cyber security challenges and threats, and to ensure their effectiveness in protecting national security. In view of the growing prominence of cyber security challenges and threats in recent times, the NADI participants recommend to the ADMM track to initiate as a priority, the promotion of closer cooperation at the military level among the Asean countries through the conduct of seminars and workshops to discuss cooperative efforts, share experiences and best practices. This would allow militaries of Asean countries to develop human capacities at the bilateral and multilateral levels. In addition, it was agreed that there was a need to incorporate cyber elements into traditional joint military exercises so as to provide opportunities for the militaries to work together. The ADMM track could also, within the framework of the ADMM-Plus, seek the cooperation of the Plus counties to share their experiences with Asean countries and assist them in developing human capacities and explore ways to combat cyber security threats. Given the different abilities of the militaries of the Asean countries, there was also a need for mutual cooperation to provide cyber security expertise and assistance to member countries affected if requested by them.

Any Other Matters:

Updates on upcoming NADI meetings

35. The meeting noted the updates on upcoming NADI activities presented by hosts of respective NADI workshops as follow:

a. NADI Workshop on "The Role of Military in Enhancing Human Security" would be held on January 19-22, 2014 in Pattaya, Thailand.

b. NADI Workshop on "Future of Asean Community: Challenges and Opportunities Beyond 2015" would be held in the third week of February 2014 in Yogyakarta, Indonesia.

c. 7th NADI Annual Meeting to be held on April 7-9, 2014 in Naypyidaw, Myanmar.

d. NADI Workshop on "Regional Maritime Rules of Engagement" would be held from May 7-11, 2014 in Manila, The Philippines.

e. NADI Workshop on "Integration of the Three Pillars of Asean Community" would be held in January 2015, Chiangmai, Thailand.

Consideration of NADI Workshop Chairman's Report

36. The meeting considered the draft Chairman's Report of the NADI Workshop on Cyber Security: Emerging Challenges and Responses. After examining the Chairman's Report carefully, the meeting endorsed the report.

Concluding Remarks

37. The NADI representatives expressed their appreciation to RSIS for the warm hospitality accorded to them and the excellent arrangements made for the NADI Workshop on Cyber Security.

22 November 2013