CHAIRMAN'S REPORT OF THE TRACK II NETWORK OF ASEAN DEFENCE AND SECURITY INSTITUTIONS (NADI) WORKSHOP ON "COUNTER-TERRORISM, COUNTER-RADICALISATION AND CYBERSECURITY" 25-29 June 2018 Singapore

1. The Track II Network of ASEAN Defence and Security Institutions (NADI) Workshop on "Counter-Terrorism, Counter-Radicalisation and Cybersecurity" was organised by the S. Rajaratnam School of International Studies (RSIS), Singapore, at the Novotel Singapore on Stevens, from 25 to 29 June 2018.

2. Representatives from Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, the Philippines, Singapore, Thailand and Vietnam attended the Workshop. The list of participants is attached in Annex I. Ambassador Ong Keng Yong, Executive Deputy Chairman, RSIS, chaired the Workshop.

OPENING REMARKS BY AMBASSADOR ONG KENG YONG, EXECUTIVE DEPUTY CHAIRMAN, RSIS, CHAIRMAN OF THE NADI WORKSHOP

3. Ambassador Ong Keng Yong warmly welcomed all delegates, distinguished and keynote speakers to the NADI Workshop. He noted the challenges posed by terrorism, radicalisation and cyber threats to the peace and security of ASEAN. The transboundary nature of these threats underscores the need for cooperation at both the bilateral and multilateral levels. In addition, a whole-of-government approach involving the military, police and other related security forces, is needed. He stated that, at the Track II level, NADI ought to make its contribution through thoughtful and innovative recommendations.

KEYNOTE SPEAKER I: PROFESSOR ROHAN GUNARATNA, HEAD OF INTERNATIONAL CENTRE FOR POLITICAL VIOLENCE AND TERRORISM RESEARCH (ICPVTR), RSIS

4. Professor Rohan Gunaratna said that today, more than ever before, the scale, magnitude and the intensity of terrorism is overwhelming the region's law enforcement, military and intelligence services. To contain, isolate and eliminate the threat of terrorism, the challenge is for Southeast Asia to work together. The region's borders are imaginary and unless governments work together, ideological extremism and violence will grow and expand affecting the entire region. The threat is most dominant in peninsular Southeast Asia but is also present in mainland Southeast Asia.

5. The contemporary threat of terrorism within Southeast Asia is a national, regional and a global threat. The threat groups are operationally and ideologically linked and derive support from segments of their vulnerable communities. The current and emerging threat cannot be eradicated by any single state. With globalisation, the global threat became the regional and the regional threat became the domestic threat. Although there are groups with national agendas, increasingly Southeast Asian terrorists operate cross border and link up with groups with regional and global agendas. Although governments have made progress,

traditional mistrust made them resistant and reluctant to exchange personnel, build common databases, conduct joint training and operations, and share expertise, experience and resources. The siege of Marawi in 2017 demonstrated how the region was unprepared.

6. The terrorist attacks in Surabaya in 2018 demonstrate that the threat is expanding from politically motivated violent groups to communities. The ideologies radicalise groups, networks, cells, individuals including entire families to fight. To deter and defeat the threat, governments need to develop a full spectrum response. They range from downstream rehabilitation to midstream, lethal and kinetic operations and upstream community engagement. Motivated by ethno-political, politico-religious and left and right wing ideologies, in pursuit of their goals, the terrorists seek to kill innocent people or destroy property. To detect and disrupt terrorist preparations to strike, governments should build capabilities.

7. To effectively manage the rising threat, governments should develop a whole-of-society approach to prevent exclusivism, counter the threat of extremism and rehabilitate and reintegrate terrorists. In the counter-terrorism spectrum, community engagement and rehabilitation are two of the three components in the fight against exclusivism, extremism and terrorism. The three are: (i) prevent and counter the radicalisation of communities; (ii) interdict to detect and disrupt attacks; and (iii) rehabilitate and reintegrate former terrorists back to society.

ADOPTION OF AGENDA

8. The Workshop adopted the agenda and the programme, which are appended in Annex II and Annex III respectively.

SESSION I: COUNTER-TERRORISM

Indonesia (CSS TNI)

Presentation by Brigadier General Benny Octaviar, Head of Center for Strategic Studies, Indonesian Armed Forces, CSS TNI

9. Brigadier General Benny Octaviar highlighted the importance of enhancing the cooperation of ASEAN by promoting information exchange, best practices and lessons learnt between ASEAN Member States (AMS) in preventing and countering cyber terrorism. AMS should regulate the prevention and treatment of cyber terrorism and the exchange of evidence. This will include the activation of extradition based on bilateral agreements for cyber crime practices.

10. He recommended to strengthen capabilities and cooperation between governments, telecommunication network operators, cybersecurity specialists, law enforcement agencies, and civil society by raising awareness to enhance cybersecurity. AMS should multiply joint training in the field of counter-terrorism, both regionally and internationally.

Indonesia (IDU)

Presentation by Colonel Dr Pujo Widodo, Lecturer of Asymmetric Warfare, Indonesia Defense University

11. Colonel Dr Pujo Widodo presented on the sudden attacks in Surabaya, Indonesia, by terrorists bombers. The attacks on churches and police headquarters are difficult to identify. These terrorists have changed their strategy to use groups of family as bombers. In overcoming the terrorist threat posed by the Islamic State of Iraq and Syria (ISIS), the Indonesian Armed Forces (TNI) and police have been supported by the Indonesian government through improving the legal system.

12. He also stressed that ASEAN defence and security institutions should work together more intensively, rather than work alone. An agreement similar to the Indonesia-Malaysia-Philippines Trilateral Maritime Patrol (IndoMalPhi), is needed to guard against family bombers of ISIS.

Lao PDR

Presentation by Major Phaivanh Vongsaikham, Military Science and History Department, Ministry of National Defence

13. Major Phaivanh Vongsaikham highlighted that in a joint declaration issued at the end of the ASEAN Defence Ministers' Meeting (ADMM), the ASEAN Ministers emphasised the need "to enhance regional cooperation through intelligence and information sharing, increasing surveillance, and promoting awareness among the public about the threat of radicalism". They also vowed to collectively combat terrorism "in all its forms and manifestations in accordance with the ASEAN Convention on Counterterrorism and ASEAN Comprehensive Plan of Action on Counterterrorism as well as identify ways to strengthen counterterrorism cooperation among ASEAN defence establishments".

14. ASEAN Defence Ministers have noted with grave concern the rise of terrorism in our region, perpetrated by individuals and groups with increasingly sophisticated and deadly tactics and weapons. Major Phaivanh condemned in the strongest terms the attacks carried out by terrorists in Southeast Asia and around the world, and expressed deepest condolences to the families of the many innocent victims of these attacks. In this regard, he is heartened by the strong collaboration among ASEAN and external partners, through the ADMM-Plus Experts' Working Group (EWG) on Counter-Terrorism, the Trilateral Cooperative Arrangements, the Our Eyes Initiative, and efforts under other sectorial bodies such as the ASEAN Ministerial Meeting on Transnational Crime. These exemplify the ASEAN spirit of regional cooperation and friendship.

Philippines (AFP-OSSSM)

Presentation by Lieutenant Colonel John Paul David Trajano, Chief, Strategy Management Division, Office for Strategic Studies and Strategy Management, Armed Forces of the Philippines

15. Lieutenant Colonel John Paul Trajano underscored that a year after the Marawi crisis, there was a stark realisation that terrorism remains a looming problem in Southeast Asia. Despite of it being a local terror attack, there were reports that Foreign Terrorist Fighters (FTFs) joined the Maute to fight for the advancement of ISIS ideology and establish a regional caliphate in the Philippines. These foreign terrorists have capitalised their networks with local terrorist groups in the Philippines and they play a big role in the operations of local terrorist groups (LTGs). The Armed Forces of the Philippines (AFP) adopts programmes, which are inter-agency in nature that runs across a spectrum of different initiatives to address terrorism in a more holistic approach.

16. The Marawi City campaign exemplifies the strong commitment of the AFP, in collaboration with other government agencies, to counter terrorism. The significant gains made by the AFP in the operations to liberate Marawi City need to be sustained by implementing military and non-military solutions to address the problem. However, such initiatives should transcend beyond the confines of the military and domestic domain; it should be treated as a regional issue. It is recommended that ASEAN's existing frameworks on counter-terrorism are reinforced, particularly: (i) enhance the capabilities and cooperation among AMS, particularly on matters related to combatting terrorist financing; (ii) work on ASEAN counter narrative against ISIS' global caliphate narrative; (iii) improve the security of immigration and other travel documents issued by ASEAN; (iv) support the full implementation of the Mindanao peace process; and (v) develop an integrated surveillance and movement control methods at vulnerable areas along common borders in ASEAN, and the commencement of coordinated patrols to prevent infiltration.

Singapore

Presentation by Dr Jolene Jerard, Deputy Head, International Centre for Political Violence and Terrorism Research (ICPVTR), RSIS

17. Dr Jolene Jerard said that security is amongst the foremost tasks of governments. It is vital that states remain robust in their effort to isolate, contain and mitigate security threats. The transformative power of technology, continued radicalisation and recruitment, steadfast innovation within groups and dense cross-pollination of ideas have resulted evolving trends and new tradecraft and tactics within transnational terrorist groups in Southeast Asia. The sustenance of networks of trust is at the heart of a regional response to the threat of terrorism.

18. The transnational security threats are diverse, borderless and afflict ASEAN in a multiplicity of ways. In crafting an effective direction forward, it is important to ensure that security debates do not get in the way of positive cooperation. Building on foundations of understanding and a resolve to work together, the

transnational terrorist threat requires dynamic cooperation. Within the parameters of NADI, these objectives can be summarised as — *Head, Heart and Hand*. The 'head' to explore, evaluate and understand strategies and policies undertaken, the 'heart' to appreciate a sense of belonging within the ASEAN brotherhood; and finally the 'hand' emphasising the necessity for visionary leaders and institutions who can help create an effective way forward and contribute towards the promotion of resilient networks of trust.

Vietnam

Presentation by Senior Colonel Pham Ngoc Thanh, Director of International Studies, Institute for Defense Strategy

19. Senior Colonel Pham Ngoc Thanh noted that, thanks to the efforts of nations as well as regional and international cooperation, the fight against terrorism in Southeast Asia has achieved positive results. However, terrorism has changed significantly both in forms of organisation and operation thus introducing new challenges for the fight against terrorism in Southeast Asia. There are no longer large, hierarchic, multi-level organisations. Instead, there are now smaller and loose organisations with few branches and cells. Terrorism has expanded its targets beyond Western countries to developing countries with broader and more diversified targets, including civilians. Moreover, the mode of terrorist action has also become more diversified and dangerous, difficult to prevent and combat, especially with the exploitation of cyberspace and economic liberalisation.

20. Vietnam regards terrorism as one of the most serious challenges to national security. The Vietnam government places great importance on prevention and cooperation with countries in and beyond the region. Vietnam's opinions and experiences on the fight against terrorism include: (i) steadily keeping political stability, security and social order in the country; (ii) bringing into full play of people in the protection of national security generally and the fight against terrorism particularly; (iii) combining economic cooperation with strengthened security measures and management of cyber domain; and (iv) enhancing the effectiveness of regional and international cooperation, especially ADMM and ADMM-Plus.

DISTINGUISHED SPEAKER: AMBASSADOR MOHAMMAD ALAMI MUSA, HEAD, STUDIES IN INTER-RELIGIOUS RELATIONS IN PLURAL SOCIETIES PROGRAMME, RSIS

(Ambassador Alami shared three of his recent published commentaries and these are found in Annexes IV, V, VI.)

21. Ambassador Mohammad Alami Musa said that individuals who choose pathways towards radicalisation and violence are increasingly the successful members of society. There is, however, a different kind of impetus to motivate these successful individuals of functional states to take the leap into religious based radicalism. The narrative that is used to attract them is closely tied to their fundamentalist orientation in understanding and practicing religion. Fundamentalism is on the rise in many parts of the world including in this region. One significant cause of this is their disenchantment that many things have gone

wrong because they believe that the societies they live in have departed from the dictates of religion and have become evil. The narrative is built on the notion that there needs to be radical action to reform society and bring it back to the straight path and this can only be achieved through religion, not the mainstream version but some obscurantist version.

22. Fundamentalism becomes the slippery road to radicalism when fundamentalists combine the antiquated religious experiences derived from a literal reading of sacred text with the strains of violence which are found in the deepest level of religious imagination. These motivations to conjure a lethal formula for solution through acts of violence provide the radicals with what they believe as the divine mandate to destroy "evil" through violent acts of terror to "clean up" society.

23. To counter fundamentalism, even in its mild form, is therefore the strategy needed to fight radicalisation. If left unchecked, such mild form of fundamentalist behaviour can lead to a more aggressive form that will then fester into the dangerous, radicalised type. States in this region must step in and work with religious leaders as well as faith communities to contain the current rise in religious fundamentalism before it becomes a threat to national security, social peace and unity of the nation.

KEYNOTE SPEAKER II: ASSISTANT PROFESSOR MOHAMED BIN ALI, STUDIES IN INTER-RELIGIOUS RELATIONS IN PLURAL SOCIETIES PROGRAMME, RSIS

24. Assistant Professor Mohamed bin Ali said that the threat posed by violent Islamist groups such as ISIS requires a strategic approach that deals with terrorist motivation and ideology. This is due to the fact that ideology has been used as an important tool in terrorist propaganda which has spread worldwide. Terrorism is a by-product of extremism and radicalism. Extreme and uncompromising views on religion has led individuals to conduct terrorist attacks and commit violence in the name of religion. Extremist groups have used Islamic teaching and concepts such as *Jihad (struggle), Al-Wala; wal Bara' (Loyalty and Disavowal), Khilafah (Caliphate)* and many others to justify their attacks and for the purpose.

25. He also highlighted that young Muslims from many countries have been swayed into subscribing extremist narratives and hence radicalised. Since at least a decade ago, extremist narratives and propaganda have spread widely across the globe via various platforms especially the Internet and social media. Countering extremist narratives and radicalism thus becomes an important and effective strategy to combat the current wave of terrorism and extremism.

26. Several countries have developed programmes to eliminate the ideology that has been deep-rooted in the minds and hearts of the extremists and replace it with positive ones. The presentation highlights the strategic approach in countering radicalisation as an important long term strategy to fight global violent extremism In particular, it highlights Singapore's unique experience in countering extremism and radicalisation and the lessons that could be learnt from it. This include the country's unique terrorist rehabilitation programme which started in 2003 and other initiatives by both the government agencies and civil society to counter extremism and radicalism.

SESSION II: COUNTER-RADICALISATION

Brunei

Presentation by Ms Ampuan Yura Kasumawati Dato Paduka Haji Mohd Adnan, Senior Research Officer, Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies

27. Ms Ampuan Yura Kasumawati shared Brunei's outreach in countering radicalisation that focused on a comprehensive whole-of-government and nation approach. This lies in its enforcement, religious governance and education aspects. In this regard, the National Security Committee oversees security matters at the national level in which a working group on anti-terrorism has been established under the Committee. At the same time, various legal instruments and framework are also in place to address and mitigate terrorism, violence and extremism. The central authority of religious matters by the Ministry of Religious Affairs, the Brunei Islamic Council and State Mufti Department plays an important role to uphold and defend the Islamic faith and teachings in accordance to *Ahli Sunnah Wal Jama'ah* as embedded in the Constitution. Further to this, education and awareness centred on the youth also acts as preventive measures to build resilience and strengthen understanding of the nation.

28. She added that online radicalisation including self-radicalisation is an increasing concern for Brunei. It poses a high risk in a majority Muslim population where its youth have accessibility to social media and the Internet. There is recognition on the need to constantly recalibrate strategies including in enhancing cybersecurity capacity and capability at bilateral and multilateral levels.

Cambodia

Presentation by Major Vithyea Phann, Deputy Training Officer, National Counter Terrorism Special Forces

29. Major Vithyea Phann said that combatting transit terrorism is the key to counter-radicalisation in Cambodia. ISIS is like a water balloon. Once the balloon has been popped by the hand — the international community — the water not only stays on the hand, but spatters all over your body. The balloon pop is an illusion that ISIS collapsed. But on the contrary, a collapsed ISIS will expand all over the world. Cambodia being a relatively peaceful and stable country, but with limited security resources, has provided returning or fleeing terrorist groups with an adequately safe haven. The creation of breeding grounds for local extremists who are vulnerable to radicalisation is an important issue that Cambodia is facing. For instance, with funding from abroad, terrorist leaders were able to operate a religious school in Cambodian Cham villages throughout the country. Sheltering terrorists gives adequate time and resources to them to spread a misguided and flawed ideology to Cambodia's Cham population.

30. Cambodia is encountering many difficulties in counter-radicalisation. The lack of capability to control and track cyber threats makes the country vulnerable to the spread of and outbreak of radicalisation. A fast-growing economy with limited

security capability also allow for safe transaction of funds. Funds are not only entering the country as recruitment resources; Cambodia is also being use as a middleman and a transit point for funds to be distributed elsewhere. Remnants of past armed conflicts also present another issue that Cambodia is facing when it comes to counter-radicalisation. Remnants of our past provide adequate hardware which can be used to train, radicalise, and weaponise terrorists. Cambodia uses the unity of its people to combat terrorism and radicalisation. Cooperation with the people allows for an effective form of security network that leads us to successfully suppress extremist activities and eliminate some sources of radicalisation. Peace, stability, and prosperity has led us to the rejection of extremism and ultimately radicalisation.

Malaysia (NDUM)

Presentation by Professor Dr B.A. Hamzah, Director, Centre for Defence and International Security Studies, National Defence University of Malaysia

31. Professor Dr B.A. Hamzah said that certain quarters are apprehensive of Southeast Asia becoming a new hotbed of militancy and terrorism, post-Syria conflict. Although a mass exodus of militants from Iraq, Syria, Libya and Afghanistan is unlikely, some mercenaries have returned to the region to seek safe havens. Why the region has attracted militancy remains a question mark. While most studies show no one single factor can adequately explain the preference for militancy, the World Bank believes the recent militant uprising at Marawi, the Philippines, was caused by poverty and underdevelopment.

32. He also highlighted the importance of regional collaboration to address the shared challenges of militancy and violent extremism. Apart from the existing bilateral and region-wide mechanisms of sharing intelligence on militant activities, policy planners need to continuously engage the members of the civil society and the people to educate them on the menace of militancy and terrorism and its adverse impact on peace and stability in the region. Uncontrolled terrorism, militancy and radicalism, can undermine economic development in the region as well as stifling the much needed foreign investment.

Philippines (NDCP)

Presentation by Mr Mico Galang, Defense Research Officer II, National Defense College of the Philippines

33. Mr Mico Galang discussed the Philippines' counter-radicalisation efforts. Based on the academic literature, radicalisation is largely governed by the dynamics of grievances, ideology, and mobilisation. As such, the Philippines' counter-radicalisation efforts include addressing grievances by implementing peace agreements forged with insurgent groups, as well as through a host of political and socio-economic programmes. Manila likewise fights radicalisation by debunking the ideology of terrorists by exposing their atrocities, and through information campaigns. To address the mobilisation initiatives of terrorists, Philippine authorities have initiated steps in promoting community policing as well as by continuing intelligence efforts. Manila also supports international

counter-radicalisation efforts. Under the Philippines' 2017 Chairmanship, ASEAN adopted various declarations/statements to address radicalisation, including the "Manila Declaration to Counter the Rise of Radicalisation and Violent Extremism" by the 11th ASEAN Ministerial Meeting on Transnational Crime, the "Joint Statement of Special ASEAN Defence Ministers' Meeting on Countering Violent Extremism (CVE), Radicalisation and Terrorism", the "East Asia Summit Leaders' Statement on Countering Ideological Challenges of Terrorism and Terrorist Narratives and Propaganda", among others.

34. To further strengthen counter-radicalisation efforts at the regional level, Mr Galang recommended the following initiatives for the consideration of the ADMM. First, enhance existing cooperative efforts in counter-terrorism and counter-radicalisation. Second, sustain the cooperation with the Plus countries, especially with the upward momentum in cooperation after the ADMM-Plus has been annualised. Third, pursuant to the "Concept Paper on Streamlining ASEAN Defence Ministers' Meeting (ADMM)-Plus Experts' Working Groups (EWGs)" adopted by the ADMM in 2017, review and assess ADMM-Plus EWGs, particularly the EWGs on Counter-Terrorism and Cyber-Security, in order to improve regional cooperation.

Singapore

Presentation by Ms Nur Azlin Mohamed Yasin, Associate Research Fellow, ICPVTR, RSIS

35. Ms Nur Azlin highlighted that online extremism in Southeast Asia seemed to have lost its vibrance in the last quarter of 2017. Recruiters are hardly seen and supporters are losing interest. This is a stark difference as compared to the period from 2014 to early 2017. Terrorist operatives in Syria and Iraq, and later on in Marawi were vigorous in their propaganda dissemination and recruitment activities in open platforms. They were powerful magnets in attracting recruits and supporters, and were creating interlinked networks in this region. In the last quarter of 2017, with the increasing number of terrorists' deaths in battlegrounds, loss in territorial strength, and removal of terrorist materials on social media, their online dominance too declined. Avid supporters who are active propagandists, now recycle old propaganda releases notably those written by Aman Abdurrahman. Terrorists and recruiters on the other hand, are absent from open platforms, and linger on encrypted platforms to cover their communication footprints.

36. Despite this dwindle, and separation between the terrorists and their supporters, the presence of the online extremist community still persevered. Real-world events are especially observed to be key in rekindling the online 'jihad' spirit. They have led to spikes in online activities that allow for like-minded individuals to reinforce and revive their radicalisation processes in an effective group context. This could lead to the creation of online cells that have shown to provide fertile grounds for real-world terrorist activities. Examples of terrorist cells which had its genesis imprinted on online activities are ISIS Batam cell Katibah Gonggong Rebus (KGR), and ISIS Malaysia group, Al Qubro Generations. Keeping an eye on trends and developments on online extremism and terrorism

remains imperative. Doing so not only provide us with clues on terrorist operations. It also provides a treasure trove of materials essential to understanding our adversary's mindset and beliefs important in the creation of updated counter and alternative messages and narratives.

Thailand

Presentation by Colonel Pratuang Piyakapho, Director of Regional Studies Division, Strategic Studies Center (SSC), National Defence Studies Institute (NDSI), Royal Thai Armed Forces Headquarters (RTARF HQs)

37. Colonel Pratuang Piyakapho highlighted that nowadays, radicalisation situations correlating with terrorism still exist. Although the intensity of global terrorism has decreased annually from 2014, according to the Global Terrorism Index 2017 by the Institute for Economics and Peace, the threat continues to spread to an increasing number of countries. As for the Asia Pacific including ASEAN, in recent years, the region had the third lowest impact from terrorism. Nevertheless, there has been a 720 percent increase in the number of terrorist attacks over the last 15 years. Additionally, the United Nations Security Council's resolution 2178(2014) states that "preventing radicalisation is one of the solutions in need for preventing violent extremism, which can be conducive to terrorism". Consequently, counter-radicalisation is an important issue to be considered in intercepting conditions conducive to violent extremism. There are three root causes. Firstly, political causes are composed of a lack of political opportunities, poor governance, corruption, unfair behaviour threatened by the states and their agents and violation of human rights or the ineffective rule of law. Secondly, socio-economic causes consist of poverty, unemployment, low quality of life, marginalisation, alienation and discrimination. Lastly, social media is another cause that accelerate distribution of many ideas of radicalisation to individuals and groups via social networks.

38. Recommendations for counter-radicalisation consist of: (i) finding out root causes to effectively solve the problems; (ii) building up economic equality focusing on adjusting economic structure for thorough development and sustainability; (iii) preventing abuse of social media through coordination among government and private sector; (iv) applying measures for attracting and reparation of people who are misguided by groups of radicalism, as well as give them opportunities to return to the society; and (v) applying existing ASEAN cooperation frameworks, such as ADMM's three-year work programme 2017-2019 and ASEAN Convention on Counter-Terrorism (ACCT) to coordinate in terms of, information sharing, warning, prevention, exchange knowledge and intercepting financial support to terrorism.

GUEST SPEAKER: MS GWENDA FONG, DIRECTOR, STRATEGY DIVISION, CYBER SECURITY AGENCY OF SINGAPORE

39. Ms Gwenda Fong highlighted that the Cyber Security Agency (CSA) of Singapore was set up in April 2015 to provide centralised oversight of the state of cybersecurity preparedness at the national level especially where it relates to critical information infrastructure (CII), and to better engage with the private sector. In the three years that CSA has been formed, its mission has expanded

to cover other areas beyond CIIs. This is in response to the changing cyber threat landscape — for instance, the scale and severity of impact of cyber attacks have greatly increased, and the proliferation of Internet-of-Things (IoT) devices compounds the challenge of maintaining cybersecurity.

40. Singapore recognises that the cyber threat is real, and it is here to stay. Four trends of concern are — the rise of ransomware, massive data breaches, attacks on IoT vulnerabilities, and Advanced Persistent Threats.

41. In response to the complex cyber threat landscape, Prime Minister Lee Hsien Loong launched a national Cybersecurity Strategy in October 2016 that aims to build a resilient and trusted cyber environment for Singapore. The strategy comprises four pillars:
    (i) Building a resilient infrastructure — A key initiative under this is the introduction of the Cybersecurity Act that was passed in Parliament in February 2018;
    (ii) Creating a safer cyberspace — Beyond working with CII owners, we have also introduced a number of initiatives aimed at improving the overall hygiene of Singapore's cyberspace as well as improving public awareness of cybersecurity best practices;
    (iii) Developing a vibrant cybersecurity ecosystem — In recognition that cybersecurity is a growth opportunity for Singapore, we have introduced a number of manpower and industry development initiatives to create economic opportunities and good jobs for Singaporeans; and
    (iv) Strengthening international partnership — Cyber threats are borderless; as such, we have various bilateral cooperation agreements with partner countries. Singapore also plays an active role in promoting dialogue on cyber norms and supporting confidence and capacity building measures regionally.

BRIEFING BY COLONEL TEOH CHUN PING, DIRECTOR (POLICY), DEFENCE CYBER ORGANISATION, MINISTRY OF DEFENCE (MINDEF), SINGAPORE

42. Colonel Teoh Chun Ping said that as MINDEF/Singapore Armed Forces (SAF) continues to leverage technologies to achieve operational, administrative and logistical effectiveness, it will also be exposed to an expanding attack surface, where the risk of cyber threats is exacerbated by the increasing complexity of information technologies and operational technologies networks and systems. The increasingly sophisticated methods employed by Advanced Persistent Threat actors and the potential shift towards attacking defence-related networks across the entire defence eco-system, outside of the traditional defence establishments, further compound the cyber defence challenges.

43. The Defence Cyber Organisation (DCO) was established in 2017 to: (i) drive cybersecurity efforts across the entire defence sector; (ii) develop cyber defence capabilities for MINDEF/SAF; and (iii) contribute to the whole-of-government cybersecurity efforts, when called upon, especially in response to national level cyber incidents. To effectively fulfil these roles, DCO seeks to: (i) build up capable and ready cyber forces through the implementation of multiple service schemes; (ii) develop cutting-edge capabilities, working closely with the defence

technology community; (iii) mainstream cyber defence with the rest of MINDEF/SAF's commanders, planners and operators; (iv) contribute to the whole-of-government's cybersecurity efforts; and (v) strengthen international cooperation with like-minded defence establishments. These key strategic goals have led DCO to embark on cyber initiatives, such as the Cyber National Service Full-Time Scheme, the MINDEF Bug Bounty Programme and the Cyber Defenders' Discovery Camp.

44. Moving ahead, DCO will continue to break new grounds, working closely with partners in the defence sector, across the whole-of-government and with industry and international partners to build up a strong cyber defence capability for MINDEF/SAF and for Singapore.

SESSION III: CYBERSECURITY

Brunei

Presentation by Ms Selina Farahiyah Muhammad Safwan Teo, Research Officer, Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies

45. Ms Selina Farahiyah Teo discussed Brunei Darussalam's strategies to manage its cyber challenges where she highlighted numerous national mechanisms put in place in the past 15 years and the country's ongoing initiatives including the promotion of cyber awareness among the society and the drafting of the National Cyber Security Framework.

46. She also highlighted the mapping of cybersecurity cooperation mechanisms around the region across the Track I, Track 1.5 and II and technical components in cybersecurity and the presence of gaps within the same track and across different tracks. In addressing the gaps, she highlighted the importance to engage multi-stakeholders in cybersecurity dialogues and practical initiatives at all levels to ensure initiatives across the various sectors are complementing each other, while avoiding duplication including to bridge the gap between the policy and technical components in the cybersecurity ecosystem. At the regional level, there is a need to devise a comprehensive regional plan to ensure continuity of cybersecurity cooperation. On this note, a stocktake on existing cybersecurity cooperation is required to develop future plans across the various sectors and tracks in order to strengthen national and regional cyber capabilities and resilience. In this regard, Track II can support Track I by raising awareness on all the work done across various sectors through international cooperation and discussion where Track II can: (i) map out laws and regulations, policies, doctrines in ASEAN; (ii) track and report ongoing unclassified cyber activities; and (iii) provide support to the ASEAN Secretariat in their cybersecurity agenda throughout succeeding chairmanships.

Cambodia

Presentation by Mr Sovanvisal Kosal, Deputy Director, Department of Telecommunication, Ministry of National Defence

47. Mr Sovanvisal Kosal said that ASEAN region is now a prime target for cyber attacks. The digital economy in ASEAN has the potential to add $1 trillion to gross domestic product over the next 10 years. However, cyber risks could prevent trust and resilience in this digital economy and prevent the region from realising its full digital potential. Cyber resilience is generally low, and countries have different levels of cyber readiness. Specifically, there is a lack of a strategic mindset, policy preparedness, and institutional oversight relating to cybersecurity. The absence of a unifying framework makes regional efforts largely voluntary, which leads to an underestimation of value-at-risk, and results in significant underinvestment.

48. The situation will escalate over time: the increase in trade, capital flows, and cyber linkages across ASEAN countries imply that the cyber threat landscape will generate even greater complexity in the future which will further escalate the region's cybersecurity challenges. An urgent call for action to response to these challenges must be comprehensive, engaging an array of stakeholders to deal with the scale of the threat and to ensure that ASEAN's leap into the digital economy is unobstructed. Because cybersecurity is a continuously evolving challenge, the region must build the next wave of cybersecurity capability by cultivating the future generation of security professionals and driving research and development around innovative technologies that can address emerging and unforeseen threats. Given the magnitude and complexity of the region's challenges and its unique context, ASEAN must embrace a game-changing approach, based on greater cohesion and a collective use of resources, to achieve a cyber resilient future.

49. In response to that, Cambodia has sped up developing and expanding cybersecurity-related works, namely the finalisation of the Cyber Law, and increase awareness and information sharing campaigns for government agencies, academia and the public. Capacity building and collaborations have improved the readiness of all stakeholders in responding to the cyber incidents. The ICT Masterplan 2020 have been actively discussed at both the senior and operation levels, and is on its way to the implementation phase with the involvement of all government agencies and private sectors.

Indonesia (IDU)

Presentation by Colonel Dr Pujo Widodo, Lecturer of Asymmetric Warfare, Indonesia Defense University

50. Colonel Dr Pujo Widodo said that future battlefronts will involve cyberspace in equatorial zones including Indonesia. Meanwhile, non-state actors are increasingly using cyber terrorism to attack a country.

51. Therefore, AMS need a security system to counter cyber terrorism with institutionalised mechanisms and procedures. Finally, AMS should agree on joint norms and rules against cyber terrorism.

Lao PDR

Presentation by Lieutenant Colonel Thonechanh Tongvongkham, Deputy Director, ASEAN Political and Security Division, Foreign Relations Department, Ministry of National Defence

52. Lieutenant Colonel Thonechanh Tongvongkham stated that in recent years, there has been a significant increase in the use of information and communication technology (ICTs), social media and other new technological means. Despite the positive development, Laos has experienced a series of cyber attacks such as website defacement, denial of service, malware, phishing site, malicious code, fraud, incriminate, spam and vulnerability report. He was of the view that these cybersecurity issues are rooted from internal and external factors such as technology renovation and the lack of the local people's awareness on cybersecurity matters, education and training, capacity building, technical expertise, monitoring, information sharing, coordination, analysis, assessment, policy and planning and law enforcement.

53. To address these non-traditional security challenges, Laos needs to enhance the existing cybersecurity mechanisms, as well as to establish new working groups within relevant organisations in order to deal with cybersecurity threats. In the Lao cybersecurity context, there is also a need for the country to develop its people in the areas of ICT capacity building, education and training on cybersecurity matters in order to enhance their knowledge, self-consciousness and ethics on the utilisation of social media and ICT means. The concerned organisations also need to mobilise necessary resources to help support cybersecurity initiatives, especially policy and planning measures, which are developed from time to time to meet the needs of the changing circumstances, and work collaboratively with external partners to handle cybersecurity challenges more effectively.

Malaysia (MiDAS)

Presentation by Captain Rosli Abd Ghani, Director, Traditional Military Affairs, Malaysian Institute of Defence and Security

54. Captain Rosli Abd Ghani indicated that Malaysia's Vision 2020 marked the country's journey towards becoming a developed nation by embracing the knowledge-based economy as a mean of achieving it. Consciously the government utilised the information and communication technology as a tool for development, hence resulting in the increasing use of digital information systems throughout the nation. However, the dependency on digital information systems brings with it escalating vulnerabilities and risks.

55. Acknowledging the growth of cyber threats that are endangering the e-sovereignty of the nation, a cybersecurity policy was put in place. The National

Cybersecurity Policy is a comprehensive cybersecurity implementation plan which was done in an integrated manner to ensure the national interests are protected to a level that commensurate the risks faced. Through a holistic approach which cut across the government machinery, the implementation has drawn in various ministries and agencies to work together to meet the envisaged vision.

56. Cybersecurity issues are not one-man fights because they do not conform to the physical boundary of a nation. Thus, the region must continue to work together relentlessly to prosper together. Sharing the challenges and success story with AMS is worth the salt in making this region a better place. Some of the recommendations that can be considered by AMS in providing a secured cyber domain for our region in the future are: (i) cyber capacity building; (ii) corporation and collaboration with regional and international partners; and (iii) confidence building measures among member states.

Malaysia (NDUM)

Presentation by Professor Dr B.A. Hamzah, Director, Centre for Defence and International Security Studies, National Defence University of Malaysia

57. Professor Dr B.A. Hamzah said that combatting cyber crimes and risks requires cooperation from all in the region. NADI should engage other like-minded Track II organisations in AMS and those from the civil society and non-governmental organisations to develop coordinated programmes on cybersecurity. We need to step up collaboration in cybersecurity as a matter of urgency for economic survivability. Southeast Asia is the world's fastest growing Internet economy — from 260 million users now to 480 million users by 2020. The Southeast Asian Internet economy is estimated to grow from $50 billion in 2017 to $200 billion in 2025.

58. He also highlighted the need to introduce an ASEAN Code of Responsible Conduct for the Cyber Space in support of the ASEAN Leaders' Statement for "voluntary and non-binding cyber norms, as well as the development of a peaceful, secure and resilient rules-based cyberspace that will contribute to continued economic progress, enhanced regional connectivity within and improved living standards across ASEAN". Finally, he wished to appeal to the Singapore Government to put aside from its $10 million cyber capacity programme fund in the form of Fellowships at RSIS for NADI delegates to learn, conduct research and advocacy on cybersecurity.

Singapore

Presentation by Mr Benjamin Ang, Senior Fellow, Centre of Excellence for National Security (CENS), RSIS

59. Mr Benjamin Ang highlighted that in our modern, highly connected societies, cybersecurity touches every aspect of our lives. Even countries at early stages of digital development have critical infrastructure — power, telecommunications, airports — that is dependent in some way on technology. Many of these potential

targets are owned and controlled by the private sector or the civilian public sector. They are also vulnerable to attacks conducted through their suppliers, customers, or insider threats.

60. He also said that unlike conventional threats, cyber attacks are often kept below the level of armed conflict, therefore limiting the role of military defence. Instead. governments, businesses, and individuals need to cooperate to respond to these attacks. Academics help to advance the understanding of cyber threats, propose best practices and policies, and train skilled responders. Ethical hackers help organisations to identify weaknesses before they are exploited. Civil society helps to mobilise people at different levels. Countries need to cooperate to develop voluntary norms of behaviour in cyber operations (cyber norms), pursuant to the ASEAN Leaders' Statement on Cybersecurity Cooperation, so that they can cooperate to prevent attacks, catch perpetrators, and avoid escalating conflicts. Therefore, a successful strategy must encompass the whole-of-society.

Thailand

Presentation by Lieutenant Colonel Tamrongchai Noonpugdee, attached to Regional Studies Division, Strategic Studies Center (SSC), National Defence Studies Institute (NDSI), Royal Thai Armed Forces Headquarters (RTARF HQs)

61. Lieutenant Colonel Tamrongchai Noonpugdee said that cyber threats currently affect society, economy and national security widely. The threats come in many forms such as hacking, spyware, sniffing, ransomware, malware, distribute Denial of Service (DDoS) attack, etc. So far, the Thai government has been trying to make a concrete implementation on cybersecurity policy, for example, an establishment of the national committee for preparation of national cybersecurity in 2017. This committee has to work accordingly with a 2017-2020 national strategic plan in cybersecurity. In addition, Thailand has also been working together with ASEAN in efforts to foster greater cybersecurity cooperation and capacity building in the region. As for ASEAN, there are a number of cooperation with dialogue partners in the field of ICT for the implementation of the ASEAN ICT Master Plan 2020 (AIM 2020). One of the ongoing cooperation is the ASEAN-Japan Cyber Capacity Building Centre (AJCCBC) with the objective of developing cybersecurity workforces and critical information infrastructure operators in ASEAN.

62. Recommendations for cybersecurity consist of: (i) governments should provide knowledge about cyber threats and how to deal with them to the public in order to build up awareness; (ii) governments should support cybersecurity concept in general, facilitate cybersecurity agencies' operations in specific instances, build up cybersecurity personnel's ability, and promote the cybersecurity's Public Private Partnership cooperation idea; and (iii) ASEAN members should take advantage of ASEAN's existing cybersecurity framework to develop workforces, share knowledge, techniques and experiences, as well as utilise implementation activities for more understanding and realisation of ASEAN cybersecurity coordination and collaboration.

Vietnam

Presentation by Senior Colonel Pham Ngoc Thanh, Director of International Studies, Institute for Defense Strategy

63. Senior Colonel Pham Ngoc Thanh indicated that the fourth industrial revolution has brought about benefits to human beings and at the same time introduced serious threats to cybersecurity of a country as well as the whole region. This may cause tension between countries, increase the risk of cyber war, threaten the safety of critical infrastructures, organisations and individuals, and exacerbate crime and terrorist threats.

64. In the coming time, with the dynamic development, wide application of state-operated services and technologies. In order to protect a secured and trusted cyberspace for the interest of all countries, it is necessary to strengthen the security measures including: (i) promoting education to increase awareness of cyberspace and cybersecurity; (ii) building and improving the laws on security and cybersecurity; (iii) increasing the investment on the cyber infrastructure and human resources; (iv) promoting interagency cooperation on cybersecurity; and (v) enhancing international cooperation.

65. Cybersecurity is not only a security of a single country but also a global issue; not only an issue of organisations or governments but also of all individuals in the society. Therefore, it is very urgent to enhance the roles of each government, entrepreneurs, agencies and individuals, combined with promoting international cooperation including cooperation of armed forces in cybersecurity.

EXCHANGE OF VIEWS AND RECOMMENDATIONS

66. The keynote speeches on terrorism and radicalisation, and the presentations by the Cyber Security Agency of Singapore and the Defence Cyber Organisation, Ministry of Defence, Singapore, as well as the presentations of NADI member institutions, and discussions, have all highlighted the continuing threats and challenges posed by terrorism, radicalisation and cybersecurity to AMS.

67. AMS are increasingly concerned about terrorism and radicalisation in some ASEAN countries due partly to the returning fighters who had earlier joined ISIS in the Middle East, and their supporters. AMS are also concerned about ISIS spreading its ideology globally and into Southeast Asia over various platforms, in particular, through social media and the Internet.

68. There is growing concern that the terrorists are using the cyber domain to spread their extremist ideology, resulting in self-radicalisation of individuals and groups that in certain instances have resulted in terrorist attacks and suicide bombings. The threat posed by violent groups such as ISIS requires a strategic approach that deals with terrorist motivation and ideology, particularly as ideology has become an important tool in terrorist propaganda spreading worldwide.

69. The NADI delegates noted that the issues of radicalisation and extremism are not about religion, but about individuals who have been radicalised with extremist

ideologies. Any counter-radicalisation efforts should be towards rehabilitation and reintegration of these individuals.

70. The NADI delegates agreed that enforcement agencies in AMS face many challenges in countering terrorist narratives. In particular, it was highlighted that the predominantly top-down approaches used to propagate counter narratives often fail to resonate with the wider public. Therefore, cooperation between government agencies and civil society organisations is crucial for introducing community engagement programmes to prevent radicalisation and extremism.

71. AMS should better manage cybersecurity to prevent potential disruptions as most critical infrastructures in AMS are ICT operated. AMS should contribute to global governance in cybersecurity by developing a shared set of voluntary norms that are consistent with those recommended by the ASEAN Leaders' Statement on Cybersecurity Cooperation.

72. The NADI delegates shared the view that AMS should have a national strategy and a whole-of-nation approach to counter terrorism, radicalisation and cyber threats through closer coordination and cooperation and sharing of information among the military, police and related security agencies in responding to these threats and challenges. A review of the existing enforcement structure, including legal provisions and prosecution of terrorists, could be considered. Moreover, mere law enforcement action is insufficient, as action must be taken to rehabilitate detainees and ensure that detainees, once released, do not return to terrorist activities.

73. The NADI delegates also agreed that more education and training of ICT experts should be conducted in order to enhance the effective response to cyber threats. It was recognised that aside from cooperation at the national level, there should be cooperation and sharing of information at the bilateral, trilateral and other multilateral levels to counter terrorism, radicalisation and cybersecurity challenges in the region.

74. The Workshop also recognised that there are differences in the level of capabilities and capacities among AMS to deal with terrorism, radicalisation and cyber threats. In view of this, priority should be given to the sharing of experiences and in the building of human capacity and technical expertise.

75. Aside from ASEAN cooperation, AMS should also cooperate with other countries outside the region to share experiences and information. In this regard, international conferences like the Singapore International Cyber Week (SICW) and the ASEAN Ministerial Conference on Cybersecurity Cooperation (AMCC), provide an important platform for the sharing of information and promoting cooperation and networking.

76. In view of the foregoing and taking note of the joint declaration of the 11th ADMM held in October 2017, which emphasised the need to enhance regional cooperation through intelligence and information sharing, increasing surveillance, and promoting awareness among the public about the threat of radicalisation, as well as identifying ways to strengthen counter-terrorism

cooperation among ASEAN defence establishments, the Workshop proposed the following recommendations:

(i) At the national level, the Defence Ministry should strengthen its role as part of the whole-of-nation approach to foster closer cooperation on counter-terrorism and radicalisation, and cybersecurity. A Track 1.5 meeting with the participation of related government agencies, the private sectors as well as academic institutions with the relevant expertise could be organised.

(ii) At the regional level, the ADMM-Plus through their EWGs on Counter-Terrorism and Cybersecurity, could hold workshops or seminars to enhance capacity building and human resource development and information sharing in strengthening cooperation in counter-terrorism and cybersecurity. They could also conduct more joint field or table top exercises to promote closer cooperation among AMS.

(iii) Each AMS should strengthen its national strategy to deal with terrorism, radicalisation and cybersecurity, and where necessary, establish a national coordinating centre to undertake this task.

(iv) ISIS has been active in using social media and the Internet to spread their ideology and narratives. Hence, there is a need for AMS to organise meetings to identify, discuss and develop counter as well as alternative narratives. This will enable a more coordinated strategy to deal with terrorism and extremism.

ANY OTHER MATTERS

Forthcoming NADI Activities

77. The meeting noted that Indonesia (IDU) will host a NADI Workshop on “Transnational Crimes” in Bogor, Indonesia, on 27-30 August 2018.

78. The meeting agreed to consider the schedule of NADI meetings and workshops for 2019/2020, at the NADI Workshop held in Bogor, Indonesia, in August 2018.

CONCLUDING REMARKS

79. The Chairman of the NADI Workshop extended his sincere appreciation and thanks to all the delegates for their participation in and constructive contribution to the Workshop.

80. The NADI delegates expressed their appreciation to RSIS for their generous hospitality and excellent arrangements made for the NADI Workshop.