CHAIRMAN'S REPORT OF
Track II Network of ASEAN Defence and Security Institutions (NADI)
Workshop on "ASEAN Cooperation in Cyber Capacity Building"
7 – 11 May 2018
Ayutthaya, Thailand

1. The Track II Network of ASEAN Defence and Security Institutions (NADI) Workshop on "**ASEAN Cooperation in Cyber Capacity Building**" was organized by Strategic Studies Center, National Defence Studies Institute (NDSI), at Classic Kameo Hotel & Serviced Apartments, Ayutthaya, Thailand, from 7 to 11 May 2018.

2. Representatives from Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam attended the Workshop. The list of participants is attached in Annex I. Major General Apisak Sombutcharoennon, Director of Strategic Studies Center, The National Defence Studies Institute (NDSI), chaired the Workshop.

<u>Opening Remarks by Lieutenant General Chanin Toliang, Chief of Staff of the National Defence Studies Institute (NDSI)</u>

3. Lieutenant General Chanin welcomed all participants for joining the Workshop. Information technology plays a key role and belongs to human's way of life. Since convenience of data transfer or access is limitless and boundless, it requires more consideration. In aspect of security, information technology is applied as an equipment through social media by terrorist groups for spreading radicalism. This finally creates violence and hence the importance of NADI workshop in cyber capacity building. He wished success of this meeting and asked for recommendations to ensure joint effort to safeguard ASEAN people effectively.

<u>Adoption of Agenda</u>:

4. The workshop adopted the agenda and the programme, which are attached in Annex II and Annex III respectively.

<u>SESSION ONE:</u>

Keynote Speaker:

Major General Chartchai Chaigasam, Director General, Royal Thai Armed Forces Cybersecurity Center (RTARF CSC)

5. He pointed out that with Internet of Things (IoT) and Internet of Everything, cybersecurity has become more important to prevent 'bad guys' from hacking into system. Threats consist of actors, vectors and methods. Actors, including cybercriminals and hackers, hacktivists, nation states and non-state actors, and end users, apply several methods such as virus and malware to hack into the system. Without vulnerability, hackers can do no harm because cyberattack is about cyber technique and vulnerability. They start from reconnaissance, scanning, gaining access, maintaining access, and covering track. For known threat, the related parties should put physical and technical control into network and system. For unknown threat, the related parties should apply National Institute of Standards and

Technology (NIST) Cybersecurity Framework, which includes five steps namely identify, protect, detect, respond, and recover.

6. For monitoring and detection, the related parties need to connect assets in their system and monitor them. RTARF CSC uses AI to detect suspected IPs and is ready to work with ASEAN countries. Each country needs a Computer Emergency Response Team (CERT), whose members understand the situation. According to recent cybercrime statistics, USA has the most cybercrime, followed by China. Thailand was ranked 35th. With increasing cybercrime, cyber warfare has become the 5th domain. So, Thailand needs to secure its cyberspace domain.

7. Lastly, he would like cyber intelligence to detect threats in networks. Most IPs come from USA, followed by China. ASEAN countries can help one another block those IPs and hunt them back to identify them. They need to share knowledge. Cybersecurity academy is very necessary. RTARF CSC has an academy and works with many experts in Thailand. Because the cost of cybertechnology is high, ASEAN members should share technologies, conduct joint exercise, exchange students, and cooperate with one another.

Group Captain Professor Dr. Prasong Praneetpolgrang, Professor, Navaminda Kasatriyadhiraj Royal Air Force Academy (NKRAFA)

1. Many reports warned that Southeast Asia is at risk of cyberattacks. Therefore, ASEAN issued The ASEAN ICT Masterplan 2015 and 2020 as well as Joint Media Statement at 12th ASEAN TELMIN. The Global Risks Report 2018 from World Economic Forum (WEF) ranked cyberattack as risk number three and showed that it became a serious concern. Therefore, ASEAN has to be prepared to ensure cyber resilience.

2. **Information Security Forum (ISF) reported that g**lobal cyber threats in 2018 include Crime-As-A-Service (CaaS) expanding tools and services, IoT adds unmanaged risks, supply chain remaining the weakest link in risk management, and regulation adding complexity of critical asset management. Cybersecurity challenges consist of botnets, DDos attacks, defacements, phishing, ransomware, data bleaches, APT, and insider threats. Group Captain Professor Dr. Prasong also explained recent cyber threats in Thailand. In addition, Thailand is the hub of ASEAN cybersecurity training to improve the skills of 1,200 trainees of the security-related agencies of 10 countries by 2021. However, to deal with these threats, ASEAN-Japan Cybersecurity Capacity Building Centre was established and offers various courses such as Cyder, forensic, and malware analysis. Cybersecurity skills are a core soft infrastructure needed to cope with increasing cyber threats and to jointly resolve new cyber threats when they spread through the ASEAN.

3. Group Captain Professor Dr. Prasong also showed EU's 10 major take-away points to work together on cybersecurity and critical success factors for ASEAN cooperation on cyber capacity building. Lastly, he pointed on various challenges to be dealt with such as stronger cooperative strategy on cybersecurity, developing ASEAN cyber collaboration centre, ASEAN cybersecurity masterplan, smart cybersecurity workforce development. This is an

opportunity to share expertise and resources in order to establish cyber resilience for ASEAN.

<u>SESSION TWO: Presentation on "ASEAN Cyber Situations Awareness : Foresights and Perspectives"</u>

Brunei Darussalam

Presentation by Ms. Alina Omarzuki, Acting Assistant Director, Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS), Ministry of Defence, Brunei Darussalam

8. In her remarks, Ms Alina Omarzuki highlighted that, while Cybersecurity is not a new issue, it has over the years, shot up to join terrorism and Weapons of Mass Destruction (WMD) proliferation as higher strategic altitude issues facing the world today. However, Cybersecurity issues are defined and framed differently depending on the experience of individual governments, businesses and users on how and to what extent Cybersecurity issues have directly impacted them. She further opined that interpretations of Cybersecurity will continue to be diverse as innovations in the cyberspace landscape are fast evolving and the risks and vulnerabilities associated with them continue to be unfolding. This will consequently continue to pose challenges to operationalising cooperation of cybersecurity issues. In moving forward, she further highlighted the need to first recognise the triggers or tipping points that has led to the upsurge in Cybersecurity urgency before more practical solutions can be worked upon.

9. Among the operational recommendations that can be undertaken include:
   a) Devise a comprehensive regional delivery chain to establish clearer accountabilities.
   b) Set up regional clusters and champions for incidents that may / will require responses at the regional level.
   c) Utilise existing Programmes and upcoming Centres as the hub of cybersecurity cooperation such as the ASEAN Cyber Capacity Programme (ACCP) and the ASEAN-Japan Cybersecurity Capacity Building Centre.
   d) Create joint research and assessment reports to review progress of ASEAN Cybersecurity Cooperation in "Readiness, Response and Recovery" areas such as:
      i. Policy/Governance aspects.
      ii. Human and Technical competencies.
      iii. Presence of overarching guidelines/frameworks (including vision, strategies, current state of delivery, past and present performances).
      iv. Existing reporting or cross-sectoral coordination mechanisms and any proposed changes
      v. Platforms (if any) to bridge policy and technical gaps.
      vi. Areas of prioritisation via a two- or three-year work plan.
      vii. Legal-Related Requirements.
   e) Set potential targets, timelines, routines and expected outcomes.

Kingdom of Cambodia

Presentation by MG. Kosal Sovanvisal, Deputy Director in charge of ICT and Electronics, Department of Telecommunication, Ministry of National Defense, Kingdom of Cambodia

10. Maj.Gen. Kosal has presented some points regarding the general overview of the cybersecurity challenges since the rapid growth of digital technology and how it might be

happened in the future. According to the internet users in Asia region, there are 45.7% of the internet users of the global internet users. While the average internet bandwidth especially the latest mobile technologies 4G LTE and the up coming 5G speed are going to be 10 to 100 times faster than the existing capacity at the same time it will also boost and facilitate stronger threats such as botnets, DoS, DDoS, or any other bandwidth hungry type of attacks for example, in particular, the recent highest DDoS attack in history with 1.35 terabit per second (Tbps) on February 28, 2018 that took down the world most popular The software development platform GitHub , outflanking the previously record-setting assault of 1 Tbps at French web hosting provider OVH in September 2016.

11. In conclusion, he had recommended some points for considerations as below:
    (1) Continue focus discuss and finalize the road map of ASEAN cyber defense and security.
    (2) Conduct cyber exercise annually within AMS so that we can strengthening the cooperation and capacity of our expertise. Additionally, it will help socialize all the AMS participants so that they know who to call to when problem occur, and this will effectively help reduce the timely documents process via the official channel.
    (3) Cooperation and collaboration within the AMS so that we can share information to each other as well as in response to any incidents within the region, so that we can take actions on time.
    (4) Consider to establish an ASEAN Cybersecurity Operation Center where there will be representatives of related stakeholders.
    (5) Encourage and spread the awareness to all ASEAN leaders about the impact and important of Cybersecurity with the top down approach so all level will agree on same goal.

Republic of Indonesia

Presentation by Brig.Gen. Benny Octaviar, MDA Head of Center for Strategic Studies of Indonesian Armed Forces (CSS, TNI), Indonesia

12. Southeast Asia is one of the largest number of internet users in the world. The internet uses had become a daily necessity of such cyber space. The development of ICT, influences ASEAN not only in economic practices but also in political and security matters. ASEAN Connectivity have to be a vision to unite AMS in achieving cyber security, and as one of ASEAN Centrality implementation.

13. Therefore, AMS have to build their own capability to face cyber threats. ASEAN has to build cooperation that enhanced with Research and Development as well as effective drills within the AMS.

Malaysia

Presentation by Lt Col Ir. Suthan Venkatachalam & Lt Col Suresh K.Vijayaratnam, Malaysian Institute of Defence and Security(MiDAS), Malaysia

14. According to the 2018 Global Risk Report, cyberattacks have been listed as top 10 security risks that are expected to give a huge impact to the international community. Cyberattacks have proven capable of inflicting serious physical damage to critical infrastructures and have a debilitating impact on national security. Regionally, ASEAN digital economy is projected to grow to about USD 200 billion over the next decade, making the region a prime target for cyberattacks. It is also experiencing a large increase in internet subscriptions largely due to social media usage. The AMS are aware and recognise the obligation to securitise their

cyberspace and ICT infrastructure. Regional initiatives are crucial towards addressing cybersecurity threats that transcends borders.

15. Multiple efforts were made by ASEAN and its Dialogue partner since 2001 in order to secure the harmony of cyberspace regionally despite challenges and setbacks faced throughout the process. However, the initiatives should not stop or stall as AMS need to intensify their efforts due to the rapidly evolving security threats in an often-fraught international security environment.

16. Despite having various initiatives, there are a lot more to be done towards greater cybersecurity cooperation. The region must continue to work together relentlessly to prosper together. Some of the recommendations that can be considered by NADI in providing a secured cyber domain for our region in the future are; enhancing AMS Computer Emergency Response Team (CERT) and bridging the gap, optimising ASEAN ICT Master Plan 2020, utilising the Budapest Convention framework in strengthening ASEAN cybersecurity cooperation and acquiring experts beyond AMS - through ADMM-Plus and other partners.

Republic of Singapore

Presentation by Mr. Tan Seng Chye, Senior Fellow, S. Rajaratnam School of International Studies (RSIS), Singapore

17. Mr. Tan Seng Chye highlighted the importance of the use of internet technology and the Information and Communication Technology (ICT) as the means of communication in the public, private and business sectors. ICT enables people and enterprises to interact in a digital world and for the smooth functioning of the nation, and social and business activities. Therefore, the safeguarding of the ICT systems, networks and programmes from cyberattacks and cybercrime is of primary importance to ensure the safe and smooth operation and non-disruption of critical infrastructures. The government of each ASEAN Member State has to establish an effective agency overseeing cybersecurity to ensure network security, and to protect its ICT systems and programmes to ensure the smooth functioning of the critical infrastructures.

18. The Cybersecurity Agency of Singapore (CSA) was established in 1 April 2015 to provide dedicated and centralised oversight of national cybersecurity functions, and work with the sector leads to protect Singapore's critical services. The Singapore International Cyber Week (SICW) in 2016 aimed to build a secure and resilient smart nation. The SICW 2017 had the theme "Building a Secure and Resilient Digital Future Through Partnership" to provide a platform for regional and international policy makers, thought leaders, industry experts and academics to forge partnerships so as to strengthen Singapore's digital future. During SICW 2017, the ASEAN Ministerial Meeting on Cybersecurity agreed on the importance of closer coordination of regional efforts with the aim of adopting basic voluntary cyber norms of behaviour in ASEAN and to guide the responsible use of ICT. Singapore is funding the establishment of a CSA Academy to train cybersecurity professionals in the government and critical information infrastructure sectors. This will enhance capacity building and strengthen institutions in regional countries to enable them to respond more effectively to cyberattacks

and cybercrimes. In view of the importance of cybersecurity, the following recommendations are suggested:

(1) Increase national and regional capacity building in the cybersecurity sectors and promote closer cooperation among the ASEAN countries.

(2) The SICW held in Singapore will be a useful platform for further networking and the enhancing of cooperation in the ICT sectors among regional countries and with the ASEAN Dialogue Partners and other international partners to promote a safer digital domain.

SESSION THREE: Presentation on "ASEAN Cyber Cooperation in Countering Violent Extremism"

Lao People's Democratic Republic

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

19. LTC Thonechanh briefed the participants of the workshop on general cyber and terrorist issues in Laos. He stated that in recent years, there has been a significant increase in the use of ICTs, social media and other new technological means. Despite the positive development, Laos has experienced a series of cyberattacks such as website defacement, denial of service, malware, phishing site, malicious code, fraud, incriminate and spam. These related cybersecurity matters are rooted from internal and external factors such as technology renovation and the lack of awareness, education and training, capacity building, technical expertise, monitoring, knowledge and information sharing, coordination, analysis, assessment, policy and planning and law enforcement. Regarding terrorist threat, Laos is considered insignificant if compared to other countries. However, since the country has opened up to the outside world socially and economically, it could become more susceptible to cyber and terrorist threats in a direct and indirect form in the coming years.

20. To address these non-traditional security challenges, he was of the view that Laos needs to establish cybersecurity mechanisms and work collaboratively with internal and external partners in order to monitor, warn and alarm cyber and terrorist threats; to share and exchange information and technical expertise; and to strengthen ICT capacity for all concerned organisational stakeholders to handle such challenges. In the Lao cybersecurity context, there is still an urgent need to raise awareness and conduct education and training on cyber and terrorist matters for the local citizens in order to enhance their self-consciousness and ethics on the utilisation of social media and ICT means. The government also needs to mobilise necessary resources to help support cybersecurity initiatives, as well as to periodically develop policy and planning that are fitted to changing cybersecurity and terrorist circumstances.

Republic of Indonesia

Presentation by Colonel Dr. Ir. Rudy Gultom, Head of Cyber Sensing for Defense Study Program, the Indonesian Defence University (IDU), Indonesia

21. Nowadays, the extremism, radicalism and terrorism groups have taken advantages the use of Internet access to support their operations, i.e, member recruitment, propaganda, fundraising, cyberattack actions against their targets, etc. This is one of the issues of cybersecurity as a negative impact of internet utilization by the extremism, radicalism and terrorism groups. They know the benefits of the internet services and social media can be used to facilitate the control of information in their organizational command and control system.

22. In order to tackle this cybersecurity issue, the internet users in ASEAN member countries should get more understanding as well as protection from their government against the danger of cyber extremism, cyber radicalism or cyber terrorism activities over the Internet. Therefore, this paper explains the need of an ASEAN Cybersecurity Framework standard in order to countering violent extremism activities via cyberspace.

23. The ASEAN countries must be aware and prepare of the cybersecurity issues as a negative impact of internet utilization by the extremism, radicalism and terrorism groups, because they know the benefits of the internet services and social media that can be used to facilitate the control of information in their organizational command and control system. To countering cyber extremism activities via internet within the region, ASEAN countries need to cooperate and collaborate in the use of cyber space with several strategic recommendations:
    - To build the ASEAN Cybersecurity Strategy and Policy and Master Plan.
    - To consider building an ASEAN Cyber Command and Control Center (ACCCC or AC4) and infrastructure.
    - To define a common ASEAN Cyber Critical Information Infrastructures and protect it against cyberattack or cyber terrorism actions.
    - To unify Vision of the ASEAN countries in countering violence extremism activities over the cyber space.
    - To share Information regarding Countering violence extremism activities over the Internet.
    - To create ASEAN Cybersecurity Cooperation Reference Model Handbook.
    - To create ASEAN Cybersecurity Framework standard such as the Six Ware Cybersecurity Framework (SWCSF) concept (IDU proposal).

24. The SWCSF concept is just an initial proposal or concept to enhance ASEAN countries cybersecurity environment. In the future, the SWCSF concept needs to be developed and implemented more in-depth through further research (ASEAN joint research) on specific areas especially in countering cyber extremism activities via internet.

Republic of the Union of Myanmar

Presentation by Brig. Gen. SOE MIN OO, Commandant of the Defense Services Institute of Nursing and Paramedical Science

25. Brig. Gen. SOE MIN OO indicated that cybersecurity is one of priorities for the ASEAN because the region is becoming more digitally connected and cybersecurity threats have become more pronounced. Cyberattacks and cyber bullying are much more common as technologies become more developed and advanced. The AMSs should promote and discuss a plan of reaction to distribution of extremist propaganda in politics and other areas.

26. He suggested that AMSs should (1) establish computerized cyber emergency management expert team to handle and monitor cyberattacks and to respond immediately, (2) monitor social media carefully and need to stop and counter to every circumstance that can transform to cybercrime, (3) establish own cyber operation center and should cooperate each other to exchange knowledge, experience, and expertise, and (4) cooperate closely in cyber capacity building and information sharing.

Republic of the Philippines

Presentation by Brigadier General Rolando G Jungco AFP (Ret), Executive Vice President, National Defense College of the Philippines

27. In his presentation, Brigadier General Jungco discussed the relationship between cyber space, particularly social media, and violent extremism. Presenting a more robust and real-time two-way communication process compared to traditional media, social media is revolutionary

because of three characteristics of social media. First, provided there is easy access to the internet, social media can be accessed almost everywhere using computers, mobile phones, and tablets. Second, social media is a marketplace of ideas. People can comment or express their opinions real time on current events, leading to discussions with other people whom they have not personally met. Third, social media provides instant and unfiltered sharing. Such online posts and information can also be shared to other people in real-time, hence dissemination of information can happen more rapidly compared to other conventional forms of media. Mindful of these characteristics, Brigadier General Jungco argued that the social media is being exploited by terrorists for four major purposes: propaganda, recruitment, fund raising, and communication.

28. Thereafter, Brigadier General Jungco discussed some of the key ASEAN initiatives which may serve as basis for cyber cooperation in countering violent extremism (CVE) among ASEAN member-states. In particular, Brigadier General Jungco identified some of the salient points of the ASEAN Convention on Counter-Terrorism (2007), and the ASEAN Comprehensive Plan of Action on Counter Terrorism (2009). Recent ASEAN declarations have explicitly mentioned the role of social media in CVE. For example, the 2017 "East Asia Summit Leaders' Statement on Countering Ideological Challenges of Terrorism and Terrorist Narratives and Propaganda," the leaders expressed concern for the distorted narratives peddled by terrorist through the internet and social media. In conclusion, Brigadier General Jungco proposed the following policy considerations: 1) implement existing agreements; 2) use social media to promote a common counter-narrative; and 3) Cooperation between government and academe/think tank.

Republic of Singapore

Presentation by Mr. Henrick Z. Tsjeng, Associate Research Fellow, S. Rajaratnam School of International Studies (RSIS), Singapore

29. Mr Tsjeng highlighted that, in the fight against terrorism, one major issue that has gained much attention is the usage of the internet to radicalise people using violent extremist content as a tool to recruit potential militants. An effort to counter such violent extremist narratives therefore involves not only enforcement measures, but also the development and online circulation of counter narratives to discredit violent extremist propaganda. But given the transnational nature of violent extremist content, ASEAN Member States (AMS) should also work collectively to counter them but be mindful of social and cultural sensitivities. A possible way forward is the establishment of a working group for moderate religious scholars to discuss the most appropriate counter-narratives, arrive at points of agreement and circulate these areas of common ground using appropriate online tools.

30. Given the foregoing, he recommended the following for consideration:
    (1) The AMS should work together, possibly through a working group, to develop common counter-narratives against violent extremism, while taking into account the unique social and cultural conditions of each country.
    (2) Given the propagation of violent extremist content online, the AMS should collaborate to utilise the online sphere to provide common counter-narratives.

<u>SESSION IV: Presentation on “Possible Models for ASEAN Cooperation in Cyber Capacity Building”</u>

Malaysia

Presentation by Associate Professor Dr. Adam Leong Kok Wey, National Defence University of Malaysia (NDUM) (CDISS), Malaysia

31. ASEAN today is faced with a multitude of cyber threats from cyber criminals to recreation hackers to cyber terrorists. Although there are a few responses launched by ASEAN as a unified front against cyber threats, this article argues for a more targeted response based on classifications of threats and setting up a new regional centre for cyber defence. While cyber-crime and hacking should be countered by policing actions, cyber terrorists must be countered by cyber military action. Hence the need for a concerted cyber-defence approach in cyber anti- terrorism operations. This presentation suggests the formation of a centralized ASEAN Cyber Defence Centre (ACDC) as a centralized command centre for cyber anti-terrorism activities ranging from intelligence and counter propaganda, capacity building, joint exercises, sharing of cyber resources, cyber defensive measures and cyber offensive activities. This centre can be set up using the ASEAN Coordinating Centre for Humanitarian Assistance on disaster management (AHA Centre) as a template. The ACDC will be able to provide ASEAN with an additional organization for joint collaboration and cooperation in countering regional terrorism issues in a coherent manner and with clear strategic direction.

Republic of the Philippines

Presentation by Captain Florante N Gagua, Assistant Chief, Office for Strategic Studies and Strategy Management (OSSSM), Armed Forces of the Philippines

32. Captain Gagua provided an overview of the cybersecurity challenge facing the region. The world is becoming more interconnected in the digital space, as evidenced by the expansion of e-commerce, the increasing number of users, and the phenomenon of the Internet of Things, wherein the internet and network connectivity will be an essential component and feature of more and more vital sectors apart from consumer electronics, such as air, land and sea transport, medical services, industry, energy and power, among others. It is therefore vital to protect the digital space, especially in a cybersecurity context with a wide variety of methods of attack, and an intricate web of possible sources of cyber-attack, from lone individuals including nation-states.

33. He then outlined the Philippines’ efforts to address the cybersecurity challenge, starting with the National Cybersecurity Plan 2022, a multi-agency and multi-sector initiative aimed to achieving the key imperatives of: protection of critical infrastructure, protection of civil and military government networks, protection of businesses and supply chains, and protection of individuals. For its part, the Armed Forces is institutionalizing a Cyber Group which will conduct cyberspace operations through planned, coordinated, integrated, and synchronized efforts. Apart from national efforts, the private sector is also actively contributing, both via proprietary corporate initiatives as well as non-profit organizations such as the Cybersecurity Philippines-Computer Emergency Response Team (CSP-CERT). Moving forward, the following recommendations were proposed for enhancing regional cybersecurity:
    - Using ADMM+ Experts Working Group as a jumping point for further cooperation, not only between ADMM+ military cyber forces, but also with ADMM+ based private cybersecurity entities such as CSP-CERT and its equivalents.

- Consider possible ADMM-Plus wide agreement with Microsoft to provide access to its Global Security Program (GSP);
- Collaborate with other regional frameworks such as ASEAN Regional Frameworks such as ASEAN Regional Forum (ARF), Asia-Pacific Economic Cooperation (APEC), East Asia Summit (EAS) and other relevant international organizations; and
- Increased cross-training and regular network penetration testing/prevention exercises between ASEAN military cyber forces.

Republic of Singapore

Presentation by Mr. Eugene EG Tan, Associate Research Fellow, S. Rajaratnam School of International Studies (RSIS), Singapore

34. Mr. Tan emphasised the need for collective responsibility for cybersecurity in all of ASEAN and highlighted the capacity issues among ASEAN Member States (AMS). While governments are aware of the importance of cyber capacity building in ASEAN, the effectiveness of cyber capacity building measures in ASEAN should not be measured in the short term; instead, cyber capacity building should be seen as a strategic endeavour to ensure that cyberspace remains resilient and stable for economic and social progress. Singapore is committed to cyber capacity building but cannot stand alone in the fight for cyber resilience and stability. There is a need for all AMS and other stakeholders such as private corporations to discuss ways to build cyber capacity in ASEAN. Possible ways forward are: first, to improve information sharing among AMS to keep ahead of cyber threats and cybercrime; and second, to determine binding norms of behaviour for states on an ASEAN level to ensure stability and security in cyberspace.

35. Given the challenges for AMS in cyberspace, the following capacity building measures are recommended for consideration:
    (1) Focus on the ASEAN ICT Masterplan 2020 as a framework for cyber capacity building and development in the ASEAN region;
    (2) Coordination and cooperation among AMS is necessary for building cyber capacity in the region, and enables states to tackle the issues of cybercrime and cyberattacks, while allowing the region to use technology as a growth lever; and,
    (3) AMS should work together to form binding norms of behaviour specific to the ASEAN region to prescribe and proscribe activities for the stability and security of all stakeholders in cyberspace.

Socialist Republic of Vietnam

Presentation by Lieutenant Colonal Canh Van Hoang, researcher, Institute for Defense Strategy (IDS), Ministry of National Defence, Vietnam

36. Cybersecurity poses a big challenge and it attracts a great attention of countries in the region particularly and the international community generally due to the consequences brought by its hackers. The immense opportunities that information technology and technical innovation provide human at this present, on the one hand, has changed the world in terms of space and time, especially cyber technology has allowed human to expand their activities, shorten the world gap, create many patterns as well as technology sectors in cyberspace and entering the 4.0 era. On the other hand, information technology also poses challenges and dangers to the security and development of every nation, places a new problem to be solved in the relationship and cooperation in cybersecurity.

37. The increasing dangers and threats of cyberattacks, transnational cyberspace crimes, cybersecurity issues impact not only on one country solely, cyber criminals can commit crimes at remote distance, using up-to-date technology to penetrate into information systems, aiming at modifying, stealing or disseminating information data, especially critical information related to national defense and security, or destroy the network systems. Those have left unpredictable consequences, making it great concerns and deeply affecting the people's psychology and government's upset. This problem requires ASEAN countries to develop a cooperation mechanism and information sharing to address this issue in order to ensure information security, continuous connectivity and its widespread.

Kingdom of Thailand

Presentation by Colonel Pratuang Piyakapho, Director of Regional Studies Division, Strategic Studies Center (SSC), The National Defence Studies Institute (NDSI), Thailand

38. He stressed that nowadays, increasing rates of cyber situation, in terms of frequency and severity, have sharply increased. These problems drastically impact on stability and security of ASEAN members, which much more complex from many dimensions such as economics, socials, politics, technologies and securities etc. This complex issue is very important for only one country to deal with and need the collaboration of all countries. ASEAN also has cooperation framework. For the ASEAN Defence Ministers' Meeting (ADMM), cybersecurity is the 7th EWG under ADMM-Plus.

39. Effects from cyber are divided in two dimensions as follows. ***Positive effects:*** Cyber will improve quality of life, equality and opportunity in societies, apply to support educational system, applying for green environment, applying defence and security, applying industrial and commercial and influence to daily life. ***Negative effects:*** Cyber will increase more stress in communities, affect culture and morality, reduce social participation, violate personal rights, cause a gap between society, crime on cyber network and result in health problems.

40. He pointed that to reinforce ASEAN cyber capacity may implement in two directions. ***1) Direction for innovation development and fortifying cyber capability*** such as development of high efficiency and area coverage for cyber infrastructure, driving economy with cyber, creating equality and quality society by cyber, changing governmental system to be cyber government, preparation of people for cyber economy, creating confidence and satisfaction on using cyber government system. ***2) Reinforcing capacities to prevent cyber threat in ASEAN*** such as strengthening cooperation in cyber among ASEAN members, having cybersecurity policy, coordinating of cyber work among ASEAN's security units, strengthening capabilities to counter cyber threats, strengthening capabilities about investigation related cybersecurity activities, and having a continuous cybersecurity plan.

Recommendations

41. In order to enhance cyber capacity of ASEAN member states (AMS), which has become more important these days, the following recommendations are proposed for consideration:
    a) Given that AMS have different cyber capacity levels, cybersecurity capability building should be given added priority in order for AMS to effectively address cybersecurity threats in the region.
    b) AMS can optimize the existing platforms such as ADMM-Plus Experts Working Group on Cybersecurity, ASEAN - Japan Cybersecurity Capability Building Center (AJCCBC) (in Thailand) and Singapore International Cyber Week (SICW) for further cooperation.

c) Some aspects of capacity building can be implemented as priorities:
   - Development of human resources such as IT personnel and cybersecurity experts
   - Design, develop, and conduct collaborative activities such as courses and training, joint research and publication
   - Forum to discuss narratives to counter violent extremism in social media

d) In the future, ASEAN could consider creating a new platform for enhanced cooperation.

Other matters

42. Forthcoming NADI activities

    The meeting noted the updates on upcoming NADI activities:

    a) RSIS will host a NADI Workshop on "Counter-Terrorism, Counter-Radicalisation and Cybersecurity" on 25 – 29 June 2018 in Singapore.

    b) IDU will host a NADI Workshop on "Transnational Organized Crime" in mid-August in Bogor, Indonesia (to be confirmed).

Conclusion

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

44. The NADI participants expressed their appreciation to the SSC for their warm hospitality and successful hosting of the workshop.