CHAIRMAN'S REPORT OF
Track II Network of ASEAN Defence and Security Institutions (NADI)
Workshop on
"Cyber Threats and Their Impacts on National and Regional Security in Southeast Asia"
6th – 7th September 2022
via Video Teleconference

1. The Track II Network of ASEAN Defence and Security Institutions (NADI) Workshop on "**Cyber Threats and Their Impacts on National and Regional Security in Southeast Asia**" was organized by the Republic of Indonesia Defense University (RIDU), via Zoom Meeting, on the 6th – 7th September 2022.

2. Representatives from Brunei Darussalam, Kingdom of Cambodia, Republic of Indonesia, Lao People's Democratic Republic, Malaysia, Republic of the Union of Myanmar, Republic of the Philippines, Republic of Singapore, Kingdom of Thailand, and the Socialist Republic of Vietnam attended the Workshop. The list of participants is attached in Annex I. Major General TNI Jonni Mahroza, Ph.D., Vice Rector I for Academic and Student Affairs of the Republic of Indonesia Defense University (RIDU), chaired the Workshop.

Opening Remarks by Major General TNI Jonni Mahroza, Ph.D., Vice Rector I for Academic and Student Affairs of the Republic of Indonesia Defense University (RIDU).

3. Major General Jonni Mahroza welcomed all participants to the Track II Network of ASEAN Defence and Security Institutions (NADI) Workshop organized via video teleconference. Peace, security, and prosperity are fundamental and ultimate goals of any international cooperation. And it is very true for ASEAN when the leaders of our countries founded it more than five decades ago, during the cold-war security environment, where threats to peace and security, especially prosperity were so real. They had a common dream of lasting peace and security, and prosperity among ASEAN Member States (AMS). We should thank the founders and the leaders of ASEAN for its various achievements and the benefits that our nations have been enjoying in the last fifty years or so. NADI is one of the various instruments of cooperation in ASEAN, that focuses on intellectual exchanges to share knowledge and experiences and to build consensus on common ideas. NADI's contribution has been important in assisting our ASEAN leaders in the ASEAN Defence Ministers' Meeting (ADMM) to make that very common dream of lasting peace, security, and prosperity in our region fully become, or continue to be a reality.

4. Chairman said, today's NADI topic about cyber threats is also vitally important. It is the very key to multi-dimensional or multi-domain security. Every domain of security, both traditional and non-traditional security, is now vulnerable to cyber threats, be that cyber-crimes or cyber-attacks, or its combination of threats as currently familiarized in the term of irregular warfare. There are several interchangeable terms for this, but the point is, that cyber threats can start their attack from any domain, which then may evolve and end in different domains. The main problem is that no country in the world can contain cyber threats within its territorial boundary, due to its transnational nature. So, international cooperation, which also includes government-private partnerships, and the whole sector approaches, has to be strengthened. All nations have to work together closely and intensively.

5. Before ending his remarks, the Chair of the 2022 NADI Workshop hereby stated that the Network of ASEAN Defense Institutions (NADI) Track II Workshop on "Cyber Threats and Their Impact on National and Regional Security in Southeast Asia", from 6 – 7 September 2022, officially opened.

Keynote Speakers

Keynote speech on the "Regional Cyber Defence Cooperation: A Proposal from the Republic of Indonesia Defense University" by Vice Admiral Prof. Dr. Ir. Amarulla Octavian, M.Sc., DESD., ASEAN Eng., Rector of the Republic of Indonesia Defense University (RIDU).

6. Prof. Dr. Ir. Amarulla Octavian mentioned that the complexity of handling cyber threats in Southeast Asia is quite complicated. The transnational security issues originating from cyber threats seem to be endless. ASEAN countries acknowledge that cyber systems are vulnerable to cyber threats.

7. Cyber security threats have escalated on many levels, and it has complexified the threat to global, regional, and national security. These serious cyber security and defence problems have also led to "Cyber War" which needs cyber security and defence policy coordination, strong military infrastructure, and reliable human resources for cyber defence.

8. Military domain cybersecurity, consists of developing military infrastructure communications among AMS, strengthening the existing military mechanism to be implemented by bolstering the regional cyber military readiness, standardizing cyber defence infrastructure capabilities among AMS, conducting joint cyber defence exercise among AMS, and improving human resources on cyber defence in the region. Civilian domain cyber security consists of establishing a regional control centre to monitor any possible cyber-attacks in the region, evaluating the existing mechanisms that have not been implemented by AMS in dealing with military and non-military cybersecurity threats, standardizing cyberinfrastructure capabilities among AMS, and improving the existing mechanism to address with the future challenges of cybersecurity cooperation by establishing a joint communication protocol

Adoption of Agenda:

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

SESSION I: Presentation on "What are the challenges of cyber threats and their impacts on the security of Southeast Asia?"

Brunei Darussalam

Presentation by Nor Azriah Binti Dato Seri Setia Haji Abdul Aziz, Research Officer, Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS).

10. In her presentation Ms. Azriah said, that there is undoubtedly a growing dependence on our society in the cyber domain for personal and professional use in the Region. Moreover, the embracement of the Fourth Industrial Revolution (4IR) in the region, has opened more challenges to the region's cybersecurity. Having a fair share of the victims of cyberattacks, Southeast Asia is considered a prime target for cyber-attacks,

where it has been used as launchpads for attacks, either as vulnerable hotbeds of unsecured infrastructure or as well-connected hubs to initiate attacks.

11. Brunei Darussalam identified cyber threats as another urgent threat to national security. According to a statistic released by Cybersecurity Brunei (CSB), it was recorded that cyber-attacks have increased by 38% in 2018 compared to previous years. As part of the efforts and initiatives, Brunei Darussalam has established major digital security services such as National Digital Forensics Laboratory (NDFL), Cyberwatch, BruCERT, and CSB to deter and combat the growing cyber risks and threats within Brunei Darussalam. In the defence and military sector, the Cyber Defence Unit (CDU), Royal Brunei Armed Forces (RBAF), has played a proactive and substantive role in ensuring RBAF information communication technology (ICT) system and operations are well-protected from any cyber threats and attacks. This unit is also a focal point in RBAF to support CSB for national coordination, and initiatives on cyber security.

Kingdom of Cambodia

Presentation by Brigadier General Phorn Rithysak, Deputy Director of Department of Telecommunications, Ministry of National Defence.

12. BG. Phorn Rithysak reminded us how Cybersecurity still stands as one of the most challenging issues, especially with the fast-changing technology environment in the Southeast Asia region. The Covid-19 pandemic has demonstrated the importance of the internet and has ultimately changed the way we work; this has resulted in an increase in cyberattacks in the region in both the private and public sectors. The general trend of cyberattack activity is carried out in various ways such as ransomware, phishing, business email compromise (BEC), crypto-jacking, and e-Commerce data interception.

13. As Cyber criminals continue to use different and more sophisticated means to target various industries, the cost of such attacks is costly and becoming more difficult. Businesses are spending more on Data Infrastructure and Cybersecurity, yet on the other hand, the general population is becoming more attracted to cyber threats through non-technology focused, by exploiting human vulnerabilities that can be carried out through various Scams, messengers' platforms, social networks and so on, to steal personal data and impersonation. These entail more challenges for national as well as regional security, particularly in the Southeast Asia region. Strengthening existing mechanisms within the ASEAN framework whilst also exploring other possible areas of cooperation and programs may help ease the challenges in defending ourselves against cyber threats.

Republic of Indonesia

Presentation by MG. Army A.Z.R. Dondokambey, S.E. M.Han., Head of Center for Strategic Studies, Research, and Development (CSSRD) of Tentara Nasional Indonesia.

14. MG. Army A.Z.R. Dondokambey, S.E. M.Han, pointed out that there are challenges for ASEAN to increase its capacity to overcome cyber threats through closer cybersecurity cooperation, improving regional information technology infrastructure capabilities, and increasing human resource capabilities through cooperation in cybersecurity in ASEAN. Cyber infiltration and misuse of communication protocols can escalate in the form of activities or actions aimed at entering, controlling, modifying, stealing, damaging, destroying, and disabling information systems or assets through

cyberattacks on the state network infrastructure, either government, military and civilian, and have an impact on the economic condition of a country as well as basic services to the civilian population.

15. Therefore, ASEAN in this regard, ADMM-Plus needs to strengthen the ADMM Cybersecurity and Information Centre of Excellence (ACICE) by establishing the ASEAN Cyberthreat Countermeasures Centre. ASEAN also needs to increase the function of the ASEAN Cyber Capacity Program (ACCP) through a cyberattack research centre in the defence sector that focuses on policy formulation in AMS related to cyber security. To increase the capacity of human resources, AMS needs to cooperate in the cybersecurity sector through various. Tabletop Joint Exercise among the military and cyber defence units.

Republic of the Philippines

Presentation *by Ms. Christine Lisette M. Castillo, Defense Research Officer II, National Defense College of the Philippines* (NDCP)

16. In her presentation, Ms. Christine Lisette Castillo discussed cyber threats in Southeast Asia and the challenges in addressing them. Ms. Castillo noted that combating cyber threats such as cyber conflict, cyber espionage, and cyber terrorism poses challenges to regional security in three points. First, there is a shortage of cybersecurity professionals in the region which is problematic because the demand for digital transformation continues to increase while the supply of skills struggles to keep pace. Second, there is insufficient investment in cybersecurity which can perpetuate more cyber threats and lead to huge financial loss. Third, there is a low commitment to cybersecurity which can be attributed to low prioritization to address cyber threats. With these, cyber threats compromise regional security and affect the region's pursuit of economic integration. Also, cyber threats hinder cyber cooperation among AMS because of suspicion and differences in priorities and cyber capabilities. With ASEAN's strategic relevance, it is, therefore, necessary to address cyber threats not only within states but also among them.

17. Ms. Castillo put forward several recommendations for combating cyber threats. Individually, AMS should continue to improve its respective cybersecurity maturity, strategy, and execution. Relatedly, a proactive and preventive approach is necessary to avoid the damage caused by unpreparedness and miscalculation. AMS must always strive to be multiple steps ahead of cyber threat actors. Corollary to this is the development of their cyber defence to safeguard military and other vital networks and ultimately secure common security interests. Honing local talents through training and education is also beneficial to help address the shortage of cyber skills in the region. Collectively, ASEAN should strengthen cooperation channels through the finalization of the ASEAN Cybersecurity Cooperation Strategy (2021-2025). The development of a plan of action for the implementation of cyber norms must continue, including efforts in other dimensions of Cooperation such as capacity-building, cyber hygiene, and multilateral engagements. Finally, AMS must have collective support for programs such as the ASEAN Cybersecurity Skilling Programme which aims to strengthen the cybersecurity workforce.

Lao People’s Democratic Republic

Presentation by BG. Viengxay Somvichit, Director General, Military Science and History Department (MSHD), Ministry of National Defence

18. Brigadier General Viengxay Somvichith stated that some countries still lack good cyber security, and they become targets of terrorist groups. Cyberspace has been operated of achieving its goals of attacking its target organizations, such as recruiting and training terrorist groups, trying to obtain military secrets, obtaining security information, and so on. The stability of the national network is an important factor to ensure political, economic security and social stability. We must ensure the safe operation of the national network.

19. He also emphasized that there have been many cyber-attacks aimed at achieving political, military, and economic goals. These attacks use different types of weapons that are not explosive weapons used in war, but cyber weapons such as viruses, worms, script attacks, rogue Internet codes, and denial-of-service (DDoS).

Malaysia

Presentation by Assoc. Prof. Mohd Hazali Bin Mohamed Halip, Director, Cyber Security and Digital Industrial Revolution Centre, National Defence University of Malaysia (NDUM)

20. In his presentation, Assoc. Prof. Mohd Hazali mentioned, many nations including ASEAN countries have seen cyber threats as major issues as any other security threat. In this current digital era, protecting cybers from attacks is now more important in which connectivity and information flow are vulnerable to attacks. Defending national cyberspace is becoming more challenging due to the growing number and varieties of cyber threats. As cyber threat actors such as Advanced Persistent Threat (APT) groups continue to develop new tactics and techniques for cyber-attack to undermine organizations' business missions and the nation's national security, there is a growing need for security professionals and defenders to understand how a cyber-attack can impact those objectives.

21. Malaysia, as with any other nation, must be ready to protect and defend the sovereignty of its nations from such threats, which has motivated this presentation in cyber threat intelligence by looking at and analyzing the activities of APT groups and how their operations, campaign, and activities will continue to impact ASEAN nations of their critical and information infrastructures at present and in near future. Furthermore, while we can identify some of these APT Groups, one of the biggest challenges we have seen is it is still difficult in assigning attribution to most of the cyber-attacks. Thus, with a thorough understanding of threat actors and the characteristics of their activities, we would be able to associate activities with new or known APT groups and through threat intelligence sharing, we can detect, mitigate and prevent future cyber-attacks.

Republic of the Union of Myanmar

Presentation by Major General Myint Kyaw Tun, Deputy Chief of Armed Forces Training (Strategic Studies), Office of the Chief of Armed Forces Training (OCAFT), Republic of the Union of Myanmar

22. Major General Myint Kyaw Tun mentioned that cybercrime, including spreading malware, ransomware, DDoS attacks, data breaches, and phishing, continues to increase in Southeast Asia, according to the UNODC report. In a report titled "ASEAN Cyberthreat Assessment 2021", INTERPOL warns that ASEAN has become a prime target for cyberattacks and says that Business E-mail Compromise (BEC), Phishing, Ransomware, E-commerce Data Interception, Crimeware-as-a-Services, and Cyber Fraud are the notable cyber threats in 2020 and a persistent trend facing AMS.

23. He suggested that law enforcement agencies need to share information and step-up joint efforts to develop a common operational framework to be effective in fighting cybercrime in the ASEAN region. In addition, cyberattacks continue to pose a serious threat to the AMS economy and various government agencies, including financial and defence institutions, and there is a need for more coordination, training, and exchanges to respond. He urged AMSs to discuss strengthening cyber norms and rules to better manage the governance of the cyber and digital domains.

SESSION II: Presentation on "What are the possible regional efforts to handle the cyber threats and how to strengthen the regional cooperation in dealing with cyber threats in the region?"

Malaysia

Presentation by Lt Col Ts. Erman Shah bin Mohd Khafe, Senior Officer 1 Cyber, Defense Cyber and Electromagnetic Department (BSEP), Malaysia Armed Forces.

24. Lt. Col. Ts. Erman Shah Mohd Khafe presented possible regional efforts and actions that should be taken to strengthen regional cooperation in dealing with cyber threats in the region. With the advent of Information and Communications Technology (ICT), cyber security has become a concern for all sectors of society, including the government, the business sector, and the general public. Significant increase in cyber threats globally, need ASEAN to be prepared to overcome these challenges.

25. Strategically, ASEAN can put forward regional efforts to combat cyber threats. Thus, he recommended that the following effort can be used as a weapon to combat cyber threats.
    a. Responding to Cyber Security Threats Collectively.
    b. Minimizing Gaps, Enhancing Commonalities & Capacity Building.
    c. Legal, Regulatory, and Policy.

Republic of the Philippines

Presentation by BGen Edgardo C Palma PA (MNSA), Chief, Office for Strategic Studies and Strategy Management (OSSSM)

26. In his presentation, Brigadier General Edgardo C Palma implied that as a regional effort, AMS mainly respond to future crises in a timely manner, which it envisions to have readiness for a safer cyberspace as a region. It ensures that the ASEAN cyberspace could continue to gain trusted enabler that will allow the delivery of essential services to the public, and a key enabler of the digital economy to aid in the post pandemic recovery efforts. BGEN PALMA enumerated the possible regional efforts for the AMS to consider in handling the cyber threats: First, to adjust national frameworks, basically, this will entail the development of national cybersecurity strategies with a legal and regulatory framework which will take multi-stakeholder approach in closely giving attention to the establishment of incident response. Second, the cybersecurity requires international cooperation through information sharing. Amidst the COVID-19 pandemic, the information sharing is very crucial in dealing with cyber-related issues. In cyberspace, there will be a common enemy and hence, collaboration

through policy, technical, and law enforcement level are significant in protecting the public and to work together in finding solutions. Third, unifying awareness campaigns at all ages, levels and regardless of any industry, there is a need to educate more the public about the knowledge about cybersecurity. Governments and private sector must join together in working towards unified awareness campaigns. The public should never be the last line of defense in cybersecurity but they need to play a role in educating each other. Therefore, cybersecurity is a shared responsibility.

27. BGEN PALMA also emphasized the these are the following actions that ASEAN member states might consider: First, to strictly observe the 11 norms recommended in the 2015 Report of the UN Group of Governmental Experts which deems the creation of a free, open, peaceful, and secured cyberspace. Second, to have a complete compliance under the ASEAN CERT (Computer Emergency Response Team). Since 2006, Singapore held the Incident Drills test incident response procedures which strengthen cybersecurity preparedness and cooperation among ASEAN and other partners. Lastly, to foster sustainable development in cybersecurity capabilities should support the Singapore's framework on ACCP, which aimed to generate fund resources, to enhance expertise, and training to help nations build up the necessary cyber infrastructure. It includes the conduct of workshops, seminars, and conferences as well as consultancy efforts in forming national cybersecurity strategies and related legislations

Republic of Singapore

Presentation by Mr. Benjamin Ang, Senior Fellow; Deputy Head of Centre of Excellence for National Security; Coordinator of Cyber and Homeland Defence Programme, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore

28. In his presentation, Mr. Benjamin Ang explained the nature of regional cyber threats and examined three possible types of regional cooperation. First, he outlined joint exercises between ASEAN and other states, as well as among AMS. Second, he highlighted confidence-building measures, particularly important high-level dialogues that have launched important regional centres for cooperation, such as the ASEAN Ministers Cyber Conference (AMCC), the cross-sectoral and cross-pillar ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC), as well as the ADMM, which in turn is establishing the ACICE to complement the ASEAN Cyber Defence Network. Third, he cited capacity building and highlighted how the ASEAN-Singapore Cyber Centre of Excellence (ASCCE) provides many capacity-building programmes in partnership with the UN and others

29. Mr. Ang underscored the fact that regional efforts and cooperation could be further enhanced in those three fields, and provided the following recommendations:
    a. Joint exercises could include more private sector participants, especially since the private sector owns, operates, and controls the most critical infrastructure.
    b. Confidence Building Measures could include initiating more dialogue with diverse stakeholders, such as institutes, relevant private sector organizations, and civil society. Many of the regional threats involved non-state actors, either as attackers, victims, or defenders.
    c. Capacity building can extend to Track 2 to support the above, such as further workshops and studies conducted by NADI. States could also support their institutes by participating in international dialogues such as the United Nations

Open Ended Working Group on State use of ICT (UN OEWG) and the Council for Security Cooperation Asia Pacific (CSCAP).

Kingdom of Thailand

Presentation by Flying Officer Nittaya Nganwai, WRTAF, Researcher Strategic Studies Centre (SSC), National Defence Studies Institutes, *Royal Thai Armed Forces Headquarters*

30. Flying Officer Nittaya Nganwai, WRTAF highlighted that the COVID-19 pandemic and the rapid technological development and the internet have caused an increase in reliance on digital technologies around the world. Southeast Asia is the region with the fastest growing number of internet users in the world. The Increasing in digital connectivity in the region not only brings opportunity but also brings threats from using the Internet and computers as a means of attack. Cyber threats tend to be an increasingly serious issue in the region. As a main regional institution, ASEAN defines cybercrime as one of the transnational crimes in the ASEAN Political and Security Community Blueprint 2025. ASEAN has existing mechanisms related to cooperation in cybercrime management as follows: (1) Intra-ASEAN cooperation: Cybersecurity is a key agenda under the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) and ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) (2) Multilateral Cooperations such as The ASEAN Regional Forum Inter-Sessional Meeting on Counter Terrorism and Transnational Crime (ARF ISM on CTTC), the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus) on cybersecurity issues which ADMM-Plus Experts' Working Groups (EWGs) was established to exchange expertise and transfer practical knowledge in a variety of cybersecurity-related fields (3) Declaration: ASEAN has developed a security instrument in the form of a Declaration. AMS have adopted ASEAN Declaration to Prevent and Combat Cybercrime during the 31st ASEAN Leaders' Summit in Manila, Philippines.

31. To respond to cyber threats occurring in the region, recommendations are as follows: (1) ASEAN should strengthen cooperation among the networks of the Computer Emergency Response Team (CERT) in each country to effectively respond to cyber threats. (2) ASEAN should exchange necessary information, knowledge, and technology among AMS and other non-regional dialogue partners. (3) ASEAN should develop human resource capacities such as IT personnel and experts on cybersecurity and implement collaborative activities such as courses and training, joint research, and publications related to combatting cybercrimes and strengthen closer cooperation through the existing mechanisms.

Socialist Republic of Vietnam

Presentation by Colonel Vu Cao Dinh, Deputy Director, Department of International Studies, Institute for Defence Strategy, Vietnamese Ministry of National Defence.

32. Colonel Dinh highlighted that, in recent years, cyber threats have become major challenges and had serious consequences for countries in the region and around the world. The threats include deliberate cyberattacks on critical information infrastructure; cross-site request forgery; establishment of financial services websites and online platforms for buying, selling, transferring, and storing foreign currencies, gold, cryptocurrency, etc., trade-in and dissemination of private information and data in cyberspace; popularisation of false information; infiltration into other people's computers to steal, modify, or employ encryption to hold a victim's information at ransom. There are also cyberattacks on critical national infrastructure such as airports, banking systems, military bases, government offices, etc., or the use of the internet for

terrorist purposes. These threats are presenting cybersecurity challenges to the security and development of each nation as well as Southeast Asia and the world as a whole

33. Cooperation in improving AMS's cyber resilience is extremely important because cybersecurity involves not only a nation but many nations. Additionally, uneven development gaps between AMS may hinder their capacity to deal with cyber threats. Diversification of culture, religion and legal system in AMS may make the problem more complex. Moreover, there remain certain limitations in the sharing and exchange of information between governments in the region. Strengthening regional cooperation in dealing with cybersecurity threats requires AMS to raise people's, state agencies, and enterprises' awareness of cybersecurity threats; step up cooperation and exchange of information on cybersecurity with countries outside the region and international organizations; further promote cooperation in education and training, research and development in terms of information technology; enhance coordination and collaboration in response to cybersecurity, cybercrime, and cyber warfare.

Republic of Indonesia

Presentation by Dr. Agus Hasan Sulistiono Reksoprodjo, *Asst. Professor of Asymmetric Warfare Studies Republic of Indonesian Defense University (RIDU)*

34. Dr. Reksoprodjo highlighted that Cyber Threats are immense for the ASEAN nations. Cyber Security threats have heightened in numerous levels of complexity covering worldwide territorial and national security causing various cyber dangers. An orchestrated and sophisticated cyber-attack can target multiple nations at the same time or impact the regional cyber environment. To a certain degree, cyber incidents especially those caused by cyber threats and attacks cannot be considered simply cyber crimes but as an act of cyber war since cyber warfare is the best strategy choice for an asymmetric conflict. The cyber defence has become the responsibility of a country through its authorities. Unfortunately, human resources with expertise dedicated to cyber defence are still limited, and therefore on the behalf of RIDU, he proposed a concept of an emergency communication protocol tool and policy when needed given the example of an aircraft transponder mechanism.

35. It is becoming very important and necessary for AMS to agree in terms and have a common understanding of cyber dangers as well as understanding "how" to deal with them. In cyber defence, human analysis is assisted, not substituted by technology. The use of proxy causes difficulties for attack attribution, human to human communication is important to avoid misperception during a conflict situation. Immediate incident response communication protocol is required to counter cyber emergencies. Exchange of incident response, conducting a joint investigation, and remediation will add experience to every nation involved. A joint regional cyber defence exercise will build trust and strengthen cyber capabilities in the region

<u>Summary of Discussions</u>:

The meeting discussed some crucial points, as follows:

NADI delegates exchanged views on "What are the challenges of cyber threats and their impacts on the security of Southeast Asia?" Here are some points that need to be further discussed.

1. Establishing cybersecurity regulations. A specific task force should be created among AMS to formulate cyber regulations.

2. Increasing human resources capacities on cybersecurity and cyber defence among AMS.
3. Evaluating the existing mechanisms that have not been implemented by AMS in dealing with non-military cybersecurity and military cyber defence threats.

NADI delegates exchanged views on "What are possible regional efforts to handle the cyber threats and how to strengthen the regional cooperation in dealing with cyber threats in the region?"

1. AMS should agree on terms and a common understanding of cyber dangers is necessary.
2. Emergency for immediate incident response communication protocol is needed for further regional effort in dealing with cyber security threats.
3. AMS should exchange Incident Response activities to review all infected hosts and if needed get used to conducting joint investigation and remediation to add to the experience.
4. The need to organize the Joint Regional Cyber Defence exercise among AMS.

Recommendations

1. Establishing joint communication protocols among AMS to strengthen confidence building and mutual trust in cybersecurity.
2. Establishing a Regional Control Centre or Cyber Incident Response Team (CIRT) to monitor and mitigate any possible cyber-crime and cyber-attacks in the region through open approaches to intelligence sharing among AMS.
3. Strengthening regional cooperation by conducting joint cyber defence exercises among AMS which may also include more private sector participants, especially since the private sector owns, operates, and controls most critical infrastructures.
4. Establishing coordination between the proposed ADMM Cybersecurity and Information Centre of Excellence (ACICE), the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) and the ADMM-Plus Experts' Working Group on Cybersecurity.
5. Enhancing the function of the ASEAN Cyber Capacity Program (ACCP) and the ASCCE through a cyber-attack research centre.
6. Improving the capacity building of human resources in the cybersecurity sector in ASEAN through joint education, training and exercises, joint researches and publications as well as workshops, exchanges, and studies at the Track II level.

Other Matters

7. Forthcoming NADI activities

Date	Activities	Country	Via
23 - 24 November 2022	NADI Workshop: Strengthening Border Management Cooperation	CSSRD-TNI, Indonesia	VTC

Consideration of NADI Workshop Chairman's Report

1. The meeting considered the draft Chairman's Report of the NADI Workshop on Cyber Threats and Their Impacts on National and Regional Security in Southeast Asia. After examining the Chairman's Report carefully, the meeting endorsed the report.

2. The NADI Workshop Chairman will submit the Report to the ADSOM Chairman for consideration at the ADMM Track and a copy to the NADI Chairman.

Concluding Remarks by Major General TNI Jonni Mahroza, Ph.D., Vice Rector I for Academic and Student Affairs of the Republic of Indonesia Defense University (RIDU).

In his concluding remarks, Major General TNI Jonni Mahroza, Ph.D expressed sincere appreciation to delegates and all NADI members for their dedication in participating this NADI Workshop. All contributions will be useful in supporting the ADMM in strengthening our regional cooperation in dealing with cyber threats in our region in the future.