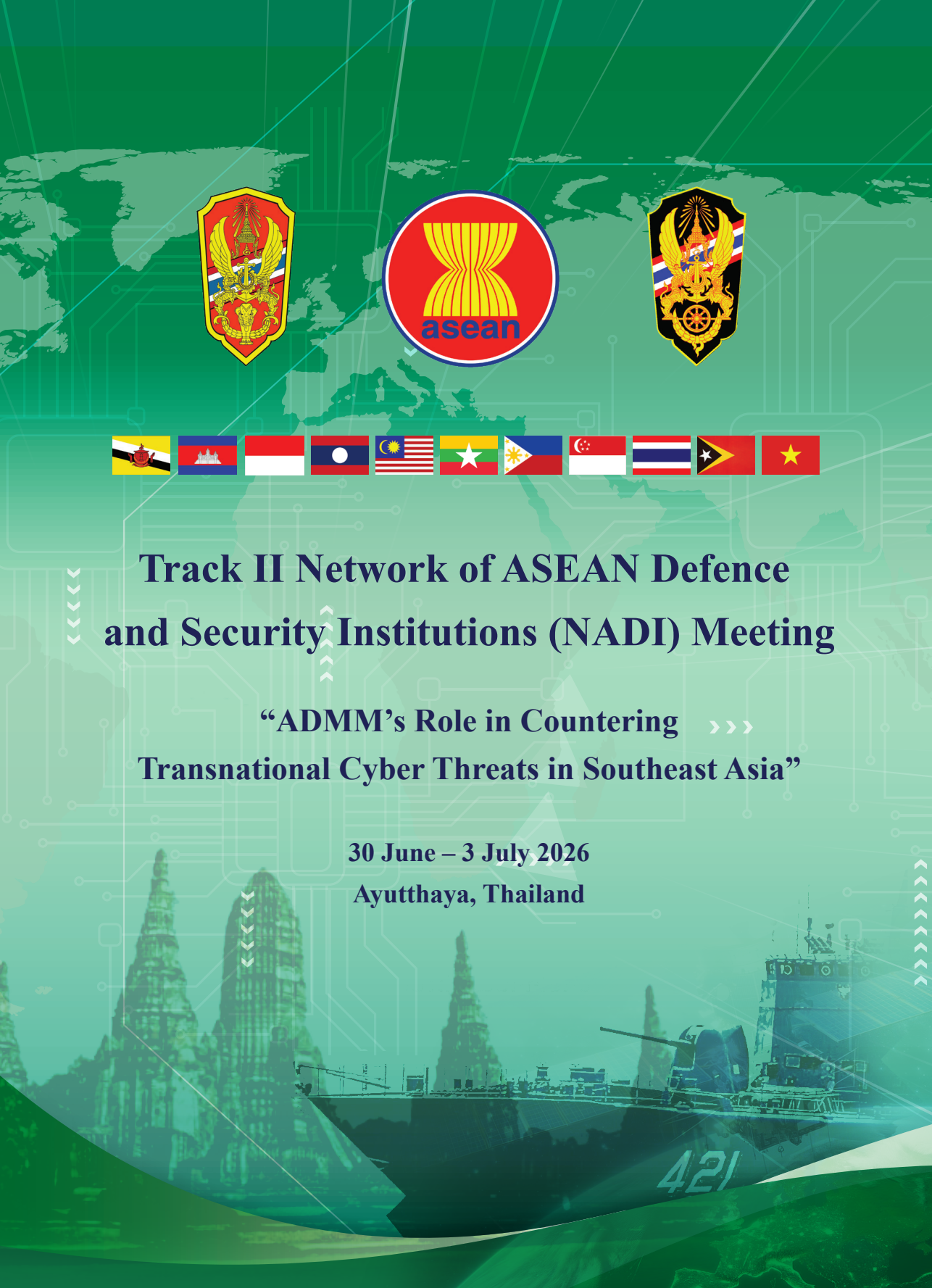


Track II Network of ASEAN Defence and Security Institutions (NADI) Meeting

"ADMM's Role in Countering Transnational Cyber Threats in Southeast Asia"

30 June – 3 July 2026

Ayutthaya, Thailand

National Library of Thailand Cataloging in Publication Data

Academic Paper: Track II Network of ASEAN Defence and Security Institutions (NADI) Meeting on "ADMM's Role in Countering Transnational Cyber Threats in Southeast Asia" 30 June – 3 July 2026 The Classic Kameo, Ayutthaya Thailand Strategic Studies Center (SSC), National Defence Studies Institute (NDSI), Royal Thai Armed Forces (RTARF)

Published by: Regional Studies Division, trategic Studies Center, National Defence Studies Institute, Royal Thai Armed Forces Headquarters

Years: 2026, 92 Pages.

Director	: AVM. Chaiya	Okdaeng
Deputy Director	: Gp.Capt. Sadit	Pringprayoon
	: Gp.Capt. Panya	Srising
Advising Editors	: Gp.Capt. Choosak	Kasatewit
	: Col. Kittipong	Ratanadilok Na Phuket
	: Col. Piyaphan	Phanwiroj
Compiler	: Sub Lt. Sittichai	Sukata
Associate Editors	: Sqn.Ldr. Siwalee	Sirirojborirak
	: Miss Napit	Kornpakawatjinda
	: Mr. Prakanthep	Srithanthapph
	: Mr. Sappamongkol	Somwong
Arts	: SM1 Sidaphat	Claythanin
	: Mr. Aue-Angkoon	Kumansing
English Editor	: Mr. Sakda	Panitpichat
	: Mr. Nattaphon	Charoenphan
	: Mr. Narongrit	Chanrit

Published by
Strategic Studies Center, National Defence Studies Institute
62 Vibhavadi Rangsit Rd., Dindaeng, Bangkok, 10400, Thailand.
E-mail: rsd.ssc2559@gmail.com, Tel./Fax: +66 2275 5716,
Website: www.sscthailand.org



Track II Network of ASEAN Defence and Security Institutions (NADI) Meeting

"ADMM's Role in Countering Transnational Cyber Threats in Southeast Asia"

30 June – 3 July 2026

Ayutthaya, Thailand

FOREWORD

The increasing complexity and borderless nature of modern cyber threats pose a severe risk to Southeast Asia's stability and economic development. Effectively countering these transnational challenges demands unprecedented regional cooperation and collective readiness among all ASEAN member states.

For this reason, the Strategic Studies Center, National Defence Studies Institute (SSC, NDSI) acting as the think tank of the Royal Thai Armed Forces Headquarters (RTARF) and a member of NADI has organized this NADI Meeting with the following objectives: (1) to examine the strategic landscape of transnational cyber threats in Southeast Asia (2) to present the findings of "Assessing the Security Impacts of Transnational Cyber Threats on ASEAN Member States and Regional Stability" (3) to discuss the findings of "Strengthening Regional Cooperation: Practical ADMM Efforts and Mechanisms in Responding to Transnational Cyber Threats" and (4) to promote academic collaboration among ASEAN defence and security institutions.

The outcomes of this meeting will significantly contribute to shaping policies and strategies at the highest levels of regional defence and security cooperation. These findings will be channeled through the ASEAN Defence Senior Officials' Meeting (ADSOM) for consideration by the ASEAN Defence Ministers at the ASEAN Defence Ministers' Meeting (ADMM).

CONTENTS

KEYNOTE ADDRESS : Keynote Speech on "The Strategic Landscape of Transnational Cyber Threats in Southeast Asia" 1

SESSION I : Presentation on "Assessing the Security Impacts of Transnational Cyber Threats on ASEAN Member States and Regional Stability" 5

- Brunei Darussalam (SHHBIDSS) 5
- Lao People's Democratic Republic (MSHD) 7
- Malaysia (MiDAS) 8
- Republic of the Union of Myanmar (OCAFT) 10
- Republic of the Philippines (NDCP) 12
- Democratic Republic of Timor-Leste (NDI-TL) 14

SESSION II: Presentation on "Strengthening Regional Cooperation: Practical ADMM Efforts and Mechanisms in Responding to Transnational Cyber Threats" 17

- Republic of Indonesia (RIDU) 19
- Malaysia (NDUM) 21
- Republic of the Philippines (OSSSM) 23
- Republic of Singapore (RSIS) 24
- Kingdom of Thailand (SSC) 26
- Socialist Republic of Vietnam (VIDSH) 29

Discussion 33

Recommendations 36

Annex 41

- Annex I List of Participants 43
- Annex II Agenda 51
- Annex III Programme 55
- Annex IV Photos 61
- Annex V Terms of Reference (TOR) 67

KEYNOTE ADDRESS

Keynote Speech on "The Strategic Landscape of Transnational Cyber Threats in Southeast Asia"

The Strategic Landscape of Transnational Cyber Threats in Southeast Asia

by General Nattapong Praokaew, Deputy Chief of the Joint Staff, Royal Thai Armed Forces Headquarters

Transnational cyber threats are reshaping Southeast Asia's security environment as criminal networks increasingly exploit digital technologies to conduct cross-border operations that threaten regional stability, national security, economic development, and public confidence. Cybersecurity has therefore evolved beyond a technical issue to become a strategic security priority requiring collective regional action.

Three major categories of cyber threats were identified: cyber espionage targeting governments and strategic industries; cyber disruption and disinformation affecting critical infrastructure and public trust; and cyber-enabled organised crime, including online scams, financial fraud, money laundering, and human trafficking. Online scam centres were highlighted as a growing transnational criminal ecosystem requiring coordinated action across cybersecurity, law enforcement, border management, financial regulation, and anti-human trafficking efforts.

The rapid expansion of digital technologies, intensifying geopolitical competition, and uneven levels of cyber governance and institutional capacity across AMS have significantly increased regional vulnerabilities. While digital transformation has generated substantial opportunities for economic growth and innovation, it has also expanded the cyber-attack surface

and created opportunities for criminals to exploit differences in national legal frameworks and institutional capabilities.

Thailand's experience highlighted four key lessons. First, new threats do not always require entirely new mechanisms; existing border security and bilateral cooperation mechanisms can be adapted to address emerging cyber threats. Second, cyber-enabled organised crime must be tackled not only in cyberspace but also by disrupting the physical infrastructure and cross-border logistics that support criminal networks. Third, complex cyber threats require integrated institutional responses. Thailand's Anti Online Scam Center (ACSC) was presented as an example of a multi-agency mechanism coordinating law enforcement, financial, telecommunications, digital, and international partners to combat online scams and cyber-enabled organised crime. Finally, sustained security cooperation with neighbouring countries remains essential despite political differences.

Looking ahead, six priorities were proposed to strengthen ASEAN's collective cyber resilience: enhancing cyber threat intelligence sharing; developing an ASEAN Cyber Fusion Network to connect existing cyber institutions; strengthening cooperation against cyber-enabled organised crime; expanding joint cyber exercises and incident response mechanisms; promoting cyber diplomacy and confidence-building measures; and leveraging artificial intelligence to improve regional threat detection, early warning, and decision-making. Sustained cooperation, mutual trust, and coordinated regional action were identified as the foundations for effectively countering transnational cyber threats.

****

SESSION I

Presentation on
“Assessing the Security Impacts of Transnational Cyber Threats on ASEAN Member States and Regional Stability”

Brunei Darussalam (SHHBIDSS)

Presentation by Ms. Siti Nurnabilah bte Hj Abdul Rahman, Research Officer, Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS), Ministry of Defence, Brunei Darussalam

Siti Nurnabilah bte Hj Abdul Rahman in her presentation shared that cyber threats have become a major transnational security challenge, affecting national resilience, defence preparedness, critical infrastructure and regional stability. As AMS continue to digitalise their economies and government systems, they face increasing risks from ransomware, cyber espionage, AI-enabled attacks, cyber-enabled fraud, and organised cybercrime. The growing convergence of cybercrime, hybrid threats, together with intensifying geopolitical competition, reinforces the need to view cybersecurity as a strategic defence and national security issue rather than solely a technical or law-enforcement concern.

Although ASEAN has established various cybersecurity cooperation mechanisms, differences in national priorities, cyber capabilities, and policy approaches continue to limit deeper operational coordination. Strengthening synergy between defence-sector cyber mechanisms and broader ASEAN cybersecurity initiatives—including the ADMM-Plus Experts' Working Group on Cyber Security, ADMM Cybersecurity and Information Centre of Excellence (ACICE), ASEAN Regional Computer Emergency Response Team (CERT), and other relevant ASEAN cyber mechanisms—would strengthen

information sharing, joint exercises, incident communication, and coordination on issues affecting critical infrastructure. Enhanced cross-sectoral cooperation will be essential to strengthening ASEAN's collective cyber resilience and improving regional preparedness to respond to transnational cyber threats.

****

Lao People's Democratic Republic (MSHD)

Presentation by Lieutenant Colonel Souksan Khaiphom, Head of the Office, Military Science and History Department (MSHD), Ministry of National Defence, Lao PDR

Lt.Col Souksan KHAIPHOM has highlighted the growing security impacts of transnational cyber threats on AMS and regional stability. As ASEAN becomes increasingly interconnected through digital technologies, cyber threats pose significant risks to national security, economic development, social stability and critical infrastructure. Cyberattacks can compromise government and defense systems, disrupt essential services, cause major economic losses and facilitate the spread of misinformation and disinformation that undermines public trust and social cohesion. Given the cross-border nature of cyberspace, cyber incidents can also create diplomatic tensions and affect regional peace, security and stability.

He also emphasized the importance of ASEAN collective action through the ADMM and ADMM-Plus frameworks, including strengthening cyber defense cooperation, enhancing joint cyber exercises, developing regional cyber incident response mechanisms and promoting public-private partnerships. In his summary, He explains the transnational cyber threats remain a common challenge for all AMS and through further enhancing mutual trust, capacity building and cooperation among AMS, regional security, stability and sustainable development can be effectively protected.

****

Malaysia (MiDAS)

Presentation by Rear Admiral Datuk Yusne Bin Hj Mokhtar RMN (HoD), Chief Executive Malaysia Institute of Defence and Security (MiDAS)

Rear Admiral Datuk Yusne Bin Hj Mokhtar RMN, Chief Executive of the Malaysian Institute of Defence and Security (MiDAS), emphasised that the rapid digital transformation across Southeast Asia has significantly enhanced regional connectivity while simultaneously exposing AMS to increasingly sophisticated transnational cyber threats. He highlighted that cybersecurity has evolved beyond a purely technical or information technology issue and is now a strategic security concern with direct implications for national resilience, defence preparedness, economic stability, and regional security. He noted that cyber espionage, ransomware attacks, state-sponsored cyber operations, disinformation campaigns, and attacks on critical national infrastructure have become more frequent and complex, enabling hostile actors to undermine state sovereignty and disrupt critical sectors without conventional military confrontation. From the MiDAS perspective, these threats present three major strategic implications for ASEAN: the disruption of critical infrastructure and essential public services, the degradation of defence and military operational readiness through cyber intrusions targeting command and control systems, and the erosion of regional trust and stability due to the challenges of accurately attributing cyberattacks, which could potentially escalate diplomatic and security tensions among Member States.

To address these challenges, MiDAS underscored the critical role of the ASEAN Defence Ministers' Meeting (ADMM) as the principal platform for strengthening regional cyber resilience through enhanced defence cooperation. MiDAS proposed prioritising stronger defence cyber information sharing and early warning mechanisms by promoting the systematic exchange of cyber threat intelligence, indicators of compromise, threat assessments, lessons learned, and emerging cyber trends among ASEAN defence establishments. In addition, MiDAS stressed the importance of narrowing cyber capability gaps through sustained capacity-building initiatives, including specialised training programmes, professional education, expert exchanges, collaborative research, workshops, and closer cooperation among defence institutions, military academies, and strategic think tanks. Regular multinational cyber exercises were also recommended to improve interoperability, test response procedures, strengthen crisis coordination, and enhance collective readiness against evolving cyber threats. MiDAS concluded that a more integrated and cooperative regional cybersecurity approach is essential, as no single ASEAN Member State possesses sufficient capacity to address these increasingly complex threats independently. Strengthening information-sharing mechanisms, expanding capacity-building initiatives, and institutionalising regular cyber exercises under the ADMM framework will reinforce ASEAN's collective resilience, mutual trust, confidence-building, and long-term regional security.

****

Republic of the Union of Myanmar (OCAFT)

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

MG Win Bo highlighted that the rapid digital transformation taking place across Southeast Asia has created both opportunities and vulnerabilities for AMS. While many countries have strengthened their cybersecurity commitments, significant differences in cyber readiness remain across the region. He noted that such disparities create security gaps that can be exploited by malicious actors, making regional resilience dependent upon the capabilities of all member states. He emphasised that ASEAN is facing an increasingly complex cyber threat environment characterised by ransomware attacks, phishing campaigns, cyber espionage, attacks on critical infrastructure, and supply-chain vulnerabilities. He further underlined the growing threat posed by cyber-enabled scam centres, which have evolved into a serious regional security concern involving online fraud, money laundering, organized crime, and human trafficking. According to his assessment, these activities not only generate substantial financial losses but also weaken governance, undermine the rule of law, and threaten regional stability. He stressed that transnational cyber threats can no longer be viewed solely as technical challenges but must be recognised as significant security issues requiring collective regional attention and coordinated responses.

He underlined that the ADMM and the ADMM-Plus framework

play an important role in enhancing regional cybersecurity cooperation. Through mechanisms such as the EWG on Cyber Security, ASEAN has promoted confidence-building measures, information sharing, capacity-building activities, and practical cooperation with dialogue partners. He noted that these initiatives contribute significantly to strengthening preparedness and improving coordination among defence establishments across the region. At the same time, he acknowledged that important challenges remain, including differing national legislation, uneven levels of cyber capability, limited intelligence sharing, and the absence of common regional cyber norms. He warned that failure to address these challenges could enable cybercriminal networks to expand their activities, threaten critical infrastructure, and undermine public confidence in digital systems. To strengthen regional resilience, he recommended the establishment of a regional cyber incident response mechanism under the ADMM framework and the expansion of joint cyber exercises, training programmes, and capacity-building initiatives. He concluded that stronger cooperation and practical action are essential for ensuring a secure, stable, and resilient digital future for ASEAN.

****

Republic of the Philippines (NDCP)

Presentation by Director Christine June P Cariño, MNSA, President, National Defense College of the Philippines (NDCP)

In her presentation, the National Defense College of the Philippines (NDCP) argued that transnational cyber threats have become a first-order strategic security challenge for ASEAN, one that defense establishments struggle to address. The NDCP identified three interconnected threat categories relevant to the region: a) state-sponsored cyber operations, including cyber espionage and AI-enabled disinformation; b) attacks on critical information infrastructure (CII) such as energy grids, financial systems, and subsea cables; and c) cross-border cybercriminal networks, whose server infrastructure and laundering channels converge with state-sponsored operations. Underlying all three is a structural liability: the asymmetry in cyber capability among AMS means the region's cybersecurity is only as strong as the weakest link. The NDCP also discussed the security impacts of these threats on the regional level as well as in bilateral relations between AMS. She argued that these cyber threats incur financial loss, degrade command, control, and communication systems, amplify existing geopolitical tensions, and erode ASEAN's non-interference norm.

To manage these security impacts, the NDCP provided several recommendations for the ADMM. First, the NDCP recommended creating an annual ADMM Cyber Threat Report to establish shared situational awareness in the region. Second, the NDCP recommended setting a minimum common cyber defense baseline covering network segmentation, incident response, and responsible AI use. Third, the ADMM may establish a regional cyber incident notification protocol to reduce the risk of strategic miscalculation

from misattributed attacks. Finally, institutionalized joint cyber defense exercises simulating escalation and de-escalation scenarios were recommended. In closing, the NDCP highlighted the convening authority of the ADMM to move from awareness-raising to operationalization in countering transnational cyber threats that undermine regional cohesion and stability.

****

Democratic Republic of Timor-Leste (NDI-TL)

Presentation by Dr. Guilherme Soares, Director of Research, Development and Innovation, National Defence Institute of Timor-Leste

Dr. Guilherme Soares examined the security implications of transnational cyber threats for ASEAN, arguing that cyber vulnerability in one Member State can rapidly become a regional security concern. Cybersecurity was framed not merely as a technical issue but as a strategic priority affecting sovereignty, economic resilience, military readiness, public trust, and regional stability. Three major categories of threats were identified: organised digital crime, attacks against critical infrastructure, and espionage, disinformation, and influence operations. Rapid digital transformation, the growing use of artificial intelligence, cybercrime-as-a-service, and increasingly interconnected digital supply chains were highlighted as key factors accelerating cyber risks. The presentation also emphasised that effective responses require whole-of-government and whole-of-society approaches involving defence institutions, law enforcement, government agencies, the private sector, and regional partners.

From Timor-Leste's perspective, cybersecurity is closely linked to state-building, digital sovereignty, maritime security, and ASEAN integration. As a young democracy and maritime nation, Timor-Leste underscored the need to strengthen minimum national cyber capacity while contributing actively to regional resilience. To enhance ASEAN's collective cyber preparedness, Dr. Soares proposed five priorities for the ADMM: maintaining cybersecurity as a permanent regional security agenda; strengthening regional

early warning and information-sharing mechanisms; conducting regular ADMM and ADMM-Plus cyber crisis exercises; developing minimum cybersecurity standards for the defence sector and critical infrastructure; and reinforcing public-private, legal, and cross-border cooperation. In conclusion, ASEAN's long-term cyber resilience will depend on sustained cooperation, mutual trust, capacity-building, and shared responsibility among Member States.

****

SESSION II

Presentation on "Strengthening Regional Cooperation: Practical ADMM Efforts and Mechanisms in Responding to Transnational Cyber Threats"

Republic of Indonesia (RIDU)

Presentation by Colonel (Army) Dr. Bambang Utomo, S.I.P., M.Sos., Head of Asymmetric Study Program, Faculty of Defense Technology RIDU

Col. Bambang Utomo, in his presentation "Navigating Digital Sovereignty: An Indonesian Perspective on Strengthening ADMM Mechanisms against Transnational Cyber Threats," highlighted the urgent need for a unified cybersecurity strategy within the ASEAN region. As rapid digitalization turned cyberspace into a critical arena for geopolitical contestation, he argued that isolated national policies were no longer sufficient to combat sophisticated state and non-state cyber threats. Indonesia's recent efforts, such as Presidential Regulation 47/2023 and the integration of national defense information systems, served as an important national foundation, yet he contended that these initiatives had to be effectively linked to a broader regional framework to ensure collective resilience.

To address these challenges, he proposed several strategic recommendations, including the definition of clear regional cyber rules of engagement to prevent accidental escalation and the evolution of the ASEAN Cyber Centre of Excellence (ACICE) into a permanent regional command and control hub. By institutionalizing joint multi-sectoral capacity building and integrating defense, law enforcement, and critical infrastructure sectors into a "whole-of-nation" approach, he suggested that the ASEAN Defense Ministers' Meeting (ADMM) could bridge the

gap between individual state initiatives and regional mechanisms. Ultimately, he emphasized that regional digital sovereignty and stability depended on collaborative, strategic, and unified action across Southeast Asia.

****

Malaysia (NDUM)

Presentation by Professor Dr Adam Leong Kok Wey, National Defence University of Malaysia

Over the past two decades, ADMM and ADMM Plus have achieved significant progress in regional security through practical cooperation in maritime security, counterterrorism, disaster management, peacekeeping, military medicine, mine action, and cyber security. As AMS has digitalized rapidly in multi sectors, transnational cyber threats have surged, including ransomware, bank theft, scams, and AI deepfake fraud, threatening national security, economic resilience, and social stability. ASEAN has launched various platforms under the auspices of ADMM such as the ASEAN Cyber Defence Network (ACDN), the ADMM Cybersecurity and Information Centre of Excellence (ACICE), and the ADMM-Plus Experts' Working Group on Cyber Security. Additionally, the ASEAN Cyber Capacity Development (ACCD) was initiated as a platform to build regional cyber resilience.

Despite these mechanisms, significant challenges threaten AMS's effective cyber response. Firstly, capacity disparity exists where sophisticated cyber capabilities are integrated with critical national infrastructure creating weak points for nefarious operations while sovereignty concerns and neighbourly suspicions hamper intelligence sharing and tangible cyber defence operations. Secondly, the absence of coherent regional cyber legal frameworks creates regulation and enforcement gaps allowing cybercriminals to exploit jurisdictional boundaries. Rather than proposing new platforms or building a regional binding legal regime which will face expected difficult consensus

challenges, recommendations from NDUM will focus on enhancing ACDN's tasks through regular executive courses, joint civilian-military training where advanced AMS assist weaker members, and focused virtual cyber exercises testing readiness and collaboration as confidence-building blocks. These attainable near-term enhancements will strengthen cyber defence and security cooperation to build sustained peace, stability, and development in Southeast Asia while ensuring ADMM mechanisms remain relevant for shaping the common strategic future.

****

Republic of the Philippines (OSSSM)

Presentation by BGEN JESSIE A. BANASTAO, PAF, Chief, Office of Strategic Studies and Strategy Management (OSSSM), Armed Forces of the Philippines

In his presentation, BGEN JESSIE A. BANASTAO, PAF, Chief OSSSM, AFP emphasized that transnational cyber threats have become a regional security concern because they disrupt not only military networks but also critical socio-economic systems such as banking, transport, communications, and government services. The presentation explains that while the Philippines has already taken important national steps through the National Cybersecurity Plan 2023–2028, CERT mechanisms, AFP cyberspace planning, incident response structures, exercises, and participation in ADMM and related ASEAN cyber platforms, these efforts still need stronger regional linkage to produce faster, more coordinated defense responses during actual crises.

Moreover, BGEN BANASTAO underscored that ASEAN and ADMM already have useful cyber cooperation frameworks, but major gaps remain in operational execution, common procedures, information sharing, capability balance, and cross-sector coordination during real incidents. Based on that assessment, BGEN BANASTAO recommends practical and defense-oriented measures for ADMM consideration: (1) Develop a cyber crisis coordination protocol, (2) Conduct a quarterly cyber table-top exercise, (3) Enhance the cyber defense collaborations, and (4) Strengthen partnerships among cyber agencies.

****

Republic of Singapore (RSIS)

Presentation by Mr Muhammad Faizal Bin Abdul Rahman, Research Fellow, Regional Security Architecture Programme, Institute of Defence and Strategic Studies, S.Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore

In his presentation, Mr Faizal opined that the security and resilience of ASEAN's cyberspace have become increasingly important as a regional security matter, given evolving transnational cyber threats and enhanced connectivity that the Digital Economy Framework Agreement (DEFA) would foster. It is crucial for AMS first to maintain a coherent national cybersecurity strategy and implementation roadmap that keeps pace with digitalisation and the way technological evolution redefines cyber stakeholders and threats.

Second, a stronger regional cybersecurity posture depends not only on establishing regional cooperative frameworks and initiatives, but also on how member states bring their national experiences to bear in participating in them, and on whether these initiatives are optimised, including those under the ADMM. Three recommendations are proposed:

I. First, ASEAN militaries could use the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace to assess how to incorporate these norms into policy, operations, and diplomacy within their national military contexts. This is an endeavour in which ASEAN militaries could collaborate more closely with the ADMM Cybersecurity

and Information Centre of Excellence (ACICE).

II. Second, the ASEAN Cybersecurity Coordinating Committee could explore cross-sectoral cooperation between the ASEAN Regional CERT and the military Computer Security Incident Response Teams (CSIRTs) across AMS. Lessons from the ASEAN Regional CERT's exercises could be adapted for use in the military context to support national-level efforts.

III. Third, ASEAN militaries could explore how they may better leverage the Malware Information Sharing Platform (MISP) and ACICE Chat, contact points, and events organised by the ACICE as an ADMM platform to support responses to transnational cyber threats and to keep abreast of how the evolving cyber threat landscape applies to the military context.

****

Kingdom of Thailand (SSC)

Presentation by Colonel Piyaphan Phanwiroj, Deputy Director of the Regional Studies Division, Strategic Studies Center (SSC), National Defence Studies Institute (NDSI), Royal Thai Armed Forces Headquarters

In his presentation, Colonel Piyaphan assesses that transnational cyber threats have evolved from purely technical and criminal challenges into strategic risks that directly affect national resilience, public trust, economic security, and regional stability. Southeast Asia currently faces three interconnected categories of cyber threats: cyber-enabled transnational criminal networks, state-sponsored cyber activities and espionage, and cyber-enabled information operations. The growing convergence of cybercrime, artificial intelligence, disinformation, and influence operations has expanded the impact of cyber threats beyond cyberspace into the political, economic, and social domains. These threats not only undermine national security and critical infrastructure but also erode social cohesion, weaken public confidence, and challenge ASEAN Centrality. In countering these challenges, there are three major gaps: information-sharing gaps, operational response gaps, and civil-military coordination gaps. In response to escalating transborder threats specifically transnational crime, human trafficking, and cybercrimes like call center scams Thailand established the Border Security Integration Center (BSIC) at the national level on June 2, 2026, to serve as a centralized command hub to enforce border security policies. The Chief of Defence Forces, serving as the Director of BSIC, holds absolute authority to command and coordinate across all government agencies. There are four core initiatives to operationalize this framework: 1)

Unifying military, civilian, and law enforcement agencies to eliminate duplication and enhance operational efficiency. 2) Establishing a Special Operations Center to suppress human trafficking and information technology crimes. 3) Appointing a legal advisory committee to support compliance with security and border policies. 4) Collaborative integration and cross-departmental sharing of information with relevant agencies.

To facilitate practical, timely, and coordinated joint responses to transnational cyber threats, the following three recommendations are proposed:

I. ACICE could bridge current information-sharing gaps by establishing automated, secure data pipelines. These pipelines could link the ACICE MISP directly to the ASEAN Regional CERT and the INTERPOL Desk, seamlessly integrating military intelligence with tactical law enforcement data.

II. ADMM could consider the technical expansion of the ASEAN Direct Communications Infrastructure (ADI) network to include direct, secure, and encrypted connections between the operational commanders of the ASEAN Cyber Defence Network (ACDN) and the directors of relevant national CERTs. At present, the ADI is restricted to ASEAN Defence Ministers. However, during acute cyber characterized by the near-instantaneous propagation of automated malware across regional networks, waiting for ministerial intervention causes critical delays, thereby exacerbating the operational response deficit.

III. ADMM cybersecurity exercises could shift from siloed military drills to whole-of-government tabletop and field exercises that simulate complex, overlapping jurisdictions.

****

Socialist Republic of Vietnam (VIDSH)

Presentation by Senior Colonel Vu Cao Dinh, Director, Department of International Studies, Institute for Vietnamese Institute for Defence Strategy and History (VIDSH)

In his presentation, Sr. Col. Vu Cao Dinh highlighted that transnational cyber threats have emerged as one of the most serious non-traditional security challenges in Southeast Asia amid rapid digital transformation and the advancement of digital technologies. In response, the ADMM and ADMM-Plus have progressively elevated cybersecurity to a priority area of defence cooperation, establishing dedicated mechanisms such as the ADMM-Plus EWG on Cyber Security, the ASEAN Cyber Defence Network (ACDN), and the ADMM Cyber and Information Centre of Excellence (ACICE). Through information-sharing, training programmes, expert exchanges and cyber exercises, cybersecurity cooperation within the ADMM framework has gradually evolved from confidence-building to substantive cooperation, thereby enhancing ASEAN's collective response capabilities and reinforcing ASEAN Centrality within the regional security architecture. Nevertheless, this cooperation continues to face a number of challenges, including disparities in technological development and cyber defence capabilities among AMS, as well as the impact of intensifying major-power competition in cyberspace. Viet Nam reaffirms its commitment to promoting a peaceful, secure and stable cyberspace in accordance with international law, while actively contributing to ASEAN and international cybersecurity cooperation mechanisms, notably

through hosting the opening ceremony for the signing of the United Nations Convention against Cybercrime (the Hanoi Convention).

Building on this assessment, he recommended that the ADMM further advance cybersecurity cooperation in a more practical and effective manner. In particular, it could strengthen the coordinating role of the ADMM-Plus EWG on Cyber Security, enhance the effectiveness of the ACDN in information-sharing, early warning and emergency coordination among ASEAN militaries, and further develop the role of ACICE in research, high-quality human resource development and cybersecurity policy support. He also proposed expanding the scale and quality of cybersecurity exercises through more inter-agency, cross-border and practice-oriented activities, with a focus on protecting critical information infrastructure, countering information warfare and managing transnational cyber crises. In addition, greater emphasis could be placed on technical assistance, technology transfer, training and the sharing of best practices in order to narrow capability gaps among AMS and strengthen ASEAN's collective resilience and capacity to respond to increasingly complex cyber threats.

****



Discussion



Discussion

1. Cybercrime cannot be addressed effectively without acknowledging political sensitivities and vested interests. In some cases, individuals within institutions may benefit from cyber-enabled criminal activities, making regional cooperation more challenging.

2. Building trust is essential, not only among AMS but also in engaging stakeholders who may have influence over or connections to transnational criminal networks.

3. Cyber-enabled organised crime poses a long-term threat to ASEAN's security, reputation, and future generations. Without decisive action, ASEAN risks in future being perceived as a hub for cybercrime, human trafficking, and drug trafficking.

4. ASEAN could strengthen cooperation not only among AMS but also with Dialogue Partners and other relevant stakeholders to address the evolving and increasingly complex nature of transnational cyber threats.

****



Recommendations



Recommendations

1. The ADMM could strengthen existing regional cyber mechanisms, including ACICE, ACDN, and the ADMM-Plus Experts' Working Group on Cyber Security, to enhance research, policy support, timely information-sharing, early warning, operational coordination, and capacity building. This will also facilitate the exchange of cyber threat intelligence, indicators of compromise, best practices, and lessons learned, while the technical expansion of secure communications among relevant operational cyber authorities could also be explored to facilitate timely responses to cyber incidents.

2. The ADMM could strengthen regional cyber preparedness through practical cooperation, including regular joint cyber exercises, scenario-based tabletop exercises, and incident response exercises, thereby enhancing interoperability and the preparedness of ASEAN defence establishments to respond effectively, in a timely and coordinated manner, to transnational cyber incidents affecting regional defence and security.

3. The ADMM could strengthen regional cyber capacity and resilience through joint civilian-military training, professional education, expert exchanges, technical assistance, technology transfer, collaborative research, and greater cooperation among defence establishments, law enforcement agencies, critical infrastructure operators, financial institutions, telecommunications authorities, the private sector, and other relevant stakeholders.

4. The ADMM could promote practical defence cooperation to enhance the protection of defence establishments, military networks, and defence-related critical information infrastructure against transnational cyber threats through closer information-sharing, coordinated preparedness, and the exchange of operational best practices, thereby strengthening the resilience of ASEAN defence cooperation.

5. The ADMM could promote a common regional approach to cyber defence by developing a minimum cyber defence baseline covering critical areas such as network protection, incident response, and the responsible use of emerging technologies, while encouraging the implementation of internationally recognised norms of responsible State behaviour in cyberspace.

6. The ADMM could enhance strategic regional cooperation by producing an Annual ADMM Cyber Threat Report to strengthen shared situational awareness and evidence-based policymaking, while continuing practical cooperation, confidence-building measures, and exchanges of expertise with Dialogue Partners and other relevant stakeholders.

****



Annex



Annex I

List of Participants

List of Participants

	Brunei Darussalam
1	**Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS)** **Ministry of Defence , Brunei Darussalam** 1. Nor Azriah Binti Haji Abdul Aziz (HoD) Research Officer 2. Nabilah Abd Rahman Research Officer
	Indonesia
2	**Republic of Indonesia Defense University (RIDU)** **Jakarta, Indonesia** 1. Colonel (Army) Dr. Bambang Utomo, S.I.P., M.Sos. Head of Asymmetric Study Program, Faculty of Defense Technology RIDU
	Lao PDR
3	**Military Science and History Department (MSHD)** **Ministry of National Defence, Lao PDR** 1. Brigadier General Khouanming Bidasack (HoD) Director General of Military Science and History Department 2. Lieutenant Colonel Souksan Khaiphom Head of the Office, MSHD 3. Lieutenant Colonel Anousone Thepphavong Director of ASEAN Political-Security and Multilateral Cooperation Division, FRD.

Malaysia	
4	**Malaysian Institute of Defence and Security (MiDAS)** **Ministry of Defence, Malaysia** 1. Rear Admiral Datuk Yusne Bin Hj Mokhtar RMN (HoD) Chief Executive Malaysia Institute of Defence and Security (MiDAS) 2. Col Azri bin Hj Ahmad RMAF Director of Regional Affairs Malaysia Institute of Defence and Security (MiDAS) 3. Lt Col Mohamad Fairus bin Md Salleh Assistant Director of Regional Affairs Malaysia Institute of Defence and Security (MiDAS)
5	**National Defence University of Malaysia (NDUM)** 1. Professor Dr. Adam Leong Kok Wey (HoD) Professor/Director 2. Lt Cdr Dr. Mazura binti Md Saman (R) Senior Lecturer/Head of Cluster
Myanmar	
6	**Office of the Chief of Armed Forces Training (OCAFT)** **Republic of the Union of Myanmar** 1. Major General Win Bo (HoD) Deputy Chief of Armed Forces Training (Strategic Studies) 2. Lieutenant Colonel Kyaw Zeyar Staff Officer, OCAFT 3. Major Ye Lwin Oo Staff Officer, OCAFT

Philippines	
7	**National Defense College of the Philippines (NDCP)** 1. Director Christine June P Cariño, MNSA President, NDCP 2. Ms Christine Lisette M Castillo Defense Research Officer II
8	**Office of Strategic Studies and Strategy Management (OSSSM), Armed Forces of the Philippines** 1. BGen Jessie A Banastao PAF Chief, OSSSM, AFP 2. Capt Jude Joseph A Sumpay, PN (GSC) Chief, Strategic and Special Studies Division (SSSD), OSSSM AFP 3. Ms. Merlina R. Magdangal Administrative Officer IV, SSSD, OSSSM, AFP
Singapore	
9	**S. Rajaratnam School of International Studies (RSIS) Nanyang Technological University, Singapore** 1. Mr Lawrence Anderson (HoD) Senior Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore 2. Mr Muhammad Faizal bin Abdul Rahman Research Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore 3. Mr Tsjeng Zhizhao (Henrick) Associate Research Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore

Thailand	
10	**Strategic Studies Center (SSC), National Defence Studies Institute (NDSI), Royal Thai Armed Forces Headquarters (RTARF HQ), Thailand** 1. Air Vice Marshal Chaiya Okdaeng Director of SSC, NDSI 2. Group Captain Choosak Kasatewit Director of Regional Studies Division, SSC, NDSI 3. Colonel Kittipong Ratanadilok Na Phuket Deputy Director of Regional Studies Division, SSC, NDSI 4. Colonel Piyaphan Phanwiroj Deputy Director of Regional Studies Division, SSC, NDSI
Timor-Leste	
11	**National Defense Institute of Timor-Leste (NDI-TL)** 1. Guilherme Da Costa De Jesus Soares Director of Research, Development and Innovation 2. Ermegina Alves Head of Education and Training Department 3. Rosalia Claudia Alves Da Costa Head of the Academic Services Department

Vietnam	
12	**Vietnamese Institute for Defence Strategy and History (VIDSH), Ministry of National Defence of Viet Nam** 1. Senior Colonel Le Thanh Bai Deputy Director General, Viet Nam Institue for Defence Strategy and History 2. Senior Colonel Vu Cao Dinh Director of International Studies Department, Viet Nam Institue for Defence Strategy and History 3. Senior Colonel Bach Thanh Phuong Researcher, International Studies Department, Viet Nam Institue for Defence Strategy and History

****



Annex II

Agenda



Agenda

1. Opening Remarks by General Sidha Mahasandana Commanding General, National Defence Studies Institute, Royal Thai Armed Forces Headquarters

2. Adoption of Agenda

3. Keynote Address on
   "The Strategic Landscape of Transnational Cyber Threats in Southeast Asia"

4. Session I: Presentation by NADI delegations, 10 minutes for each member on
   "Assessing the Security Impacts of Transnational Cyber Threats on ASEAN Member States and Regional Stability"

5. Session II: Presentation by NADI delegations, 10 minutes for each member on
   "Strengthening Regional Cooperation: Practical ADMM Efforts and Mechanisms in Responding to Transnational Cyber Threats"

6. Discussions and Recommendations

7. Other Matters

8. Consideration of the Chairman's Report

9. Closing Remarks by Air Vice Marshal Chaiya Okdaeng, Director of Strategic Studies Center

****

Annex III

Programme

Programme

Day 1: Tuesday, 30 June 2026			
TIME	**ACTIVITIES**	**PLACE**	**REMARKS**
All Day	Arrival of Delegates at Suvarnabhumi Airport and travel to the Hotel	Bangkok -Ayutthaya	Transportation will be provided by SSC
1900 - 2100	**Welcome Dinner** hosted by the Director of SSC	Classic Kameo, Ayutthaya	Smart Casual
Day 2: Wednesday, 1 July 2026			
TIME	**ACTIVITIES**	**PLACE**	**REMARKS**
0830 - 0900	Registration	Venue: Yodia, 2nd Floor	Lounge Suit
0900 - 0910	**Opening Ceremony** Opening Remarks by General Sidha Mahasandana, Commanding General of National Defence Studies Institute		
0910 - 0925	Group Photo		
0925 - 0930	Adoption of Agenda		
0930 - 1030	**Keynote Address on "The Strategic Landscape of Transnational Cyber Threats in Southeast Asia"** By Gen. Nattapong Praokaew, Deputy Chief of Joint Staff, Royal Thai Armed Forces Headquarters		
1030 - 1050	Coffee Break		

1050 - 1210	**Session I:** Presentation on **"Assessing the Security Impacts of Transnational Cyber Threats on ASEAN Member States and Regional Stability"** By - Brunei (SHHBIDSS) - Lao PDR (MSHD) - Malaysia (MiDAS) - Myanmar (OCAFT) - Philippines (NDCP) - Timor-Leste (NDI-TL)		10 minutes per each
1210 - 1330	Lunch	Venue: The Orchard, 1st Floor	
1330 - 1430	**Session II:** Presentation on **"Strengthening Regional Cooperation: Practical ADMM Efforts and Mechanisms in Responding to Transnational Cyber Threats"** By - Indonesia (RIDU) - Malaysia (NDUM) - Philippines (OSSSM) - Singapore (RSIS) - Thailand (SSC) - Vietnam (VIDSH)		10 minutes per each
1430 - 1500	Coffee Break		
1500 - 1530	Discussions and Recommendations		
1530 - 1600	Other Matters		

1800 - 2100	**Official Dinner** hosted by the Commanding General of National Defence Studies Institute or representative	Venue: U-Thong 1, 3rd Floor	Smart Casual
Day 3: Thursday, 2 July 2026			
TIME	**ACTIVITIES**	**PLACE**	**REMARKS**
0830 - 0900	Registration	Venue: Yodia, 2nd Floor	Lounge Suit
0900 - 1015	Consideration of Chairman's Report		
1015 - 1030	Coffee Break		
1030 - 1130	Consideration of Chairman's Report (Continued)		
1130 - 1200	**Closing Ceremony**		
1200 - 1330	Lunch	Venue: The Orchard, 1st Floor	
1330 – 1600	Cultural Visit		Transportation will be provided by SSC
1700 – 1900	Ayutthaya Cruise with Dinner	Krungsri River Hotel	
Day 4: Friday, 3 July 2026			
TIME	**ACTIVITIES**	**PLACE**	**REMARKS**
All day	Departure of Delegates to Suvarnabhumi Airport		Transportation will be provided by SSC

****

Annex IV

Photos

Photos


Track II Network of ASEAN Defence and Security Institutions (NADI) Meeting
"ADMM's Role in Countering
Transnational Cyber Threats in Southeast Asia"


Track II Network of ASEAN Defence and Security Institutions (NADI) Meeting
"ADMM's Role in Countering
Transnational Cyber Threats in Southeast Asia"
30 June – 3 July 2026
Ayutthaya, Thailand


Track II Network of ASEAN Defence and Security Institutions (NADI) Meeting
"ADMM's Role in Countering




ntering
n Southeast Asia"


























Track II Network of ASEAN Defence and Securit
"ADMM's Role in Cou
Transnational Cyber Threats ir
30 June – 3
Ayutthaya,
CHAIRMAN


"ADMM's Role in Countering
Transnational Cyber Threats in Southeast Asia







"ADMM's Role in Countering

Annex V

Terms of Reference (TOR)

NADI TOR as of 21 May 2024

For circulation to NADI Member Countries Only

Terms of Reference (TOR)
Track II Network of ASEAN Defence and Security Institutions (NADI)

The Terms of Reference serves as reference and guidelines for all activities conducted under the Track II Network of ASEAN Defence and Security Institutions (NADI).

A. Introduction

1. The Track II Network of ASEAN Defence and Security Institutions (NADI) was initiated in August 2007 by the S. Rajaratnam School of International Studies (RSIS), Singapore, as the Track II think tank group to support the ASEAN Defence Ministers' Meeting (ADMM). The inaugural meeting was attended by representatives from Track II institutions of ASEAN members.

2. The establishment of NADI was timely and necessary to discuss, in a Track II setting, issues of defence and security cooperation that the ASEAN Summit and ASEAN Defence Ministers or ASEAN Defence Senior Officials' Meeting (ADSOM) had raised, as well as fresh ideas and issues that are ahead of the curve, and can contribute to further enhancing ADMM cooperation and its cooperation with the Plus countries.

3. While all NADI members would be aware of the positions taken at the ASEAN Leaders Summit, ASEAN Foreign Ministers' Meeting and the ADMM, NADI participants are

encouraged to discuss issues and ideas in their personal capacities so that they can go beyond their national positions and to suggest relevant inputs and policy recommendations, without attribution to any participants but as a collective view of the meeting, to the ADMM track.

4. The informal Track II platform offers an environment more conducive to an open discussion of defence and security cooperation in ASEAN as well as raising ideas and proposals that may be deemed sensitive to be formally tabled at an official Track I meeting.

B. Aims

1. NADI aims to perform the following functions and roles:

   a. A forum to network, promote dialogue, build confidence and familiarity among ASEAN think tanks and research institutions to facilitate closer cooperation.

   b. A useful academic forum for policy analysts specialising in defence and security issues, academics researching security cooperation and defence officials to discuss issues of defence and security cooperation including those that the ASEAN Summit and ASEAN Defence Ministers have raised.

   c. A forum where NADI participants can express opinions beyond their respective governments' positions, to provide timely and new ideas as well as relevant recommendations to the ADMM Track to enhance ADMM cooperation and its cooperation with the Plus countries as well as to

promote closer cooperation among militaries of the ASEAN.

d. A forward-looking platform to discuss issues relating to current and future defence and security challenges as well as opportunities for cooperation.

C. Principles of NADI Meetings & activities

1. The core NADI institution of each ASEAN country will act as focal contact point. The list of NADI institutions will be updated periodically.

2. Membership in NADI is limited to Track II institutions among ASEAN members only. Only delegates from the core and partner NADI institutions can attend the NADI Annual General Meetings, NADI Meetings and Retreats. However, the core and partner institutions may bring in representatives from other think tanks and officials to participate in their personal capacities as observers or resource persons.

3. NADI participants may present their national positions in their presentations. However, in discussing fresh ideas and issues, the participants shall do so in their personal capacity. This encourages participants to think creatively and innovatively on defence and security issues beyond their respective government's positions and to contribute fresh and relevant ideas and recommendations to the ASEAN defence track and the ADMM process. This shall ensure ideas and recommendations submitted to the ADMM are not attributed to any particular NADI member.

4. All NADI activities are to be conducted in a closed-door manner without major media publicity

5. The Chairman shall at the end of each NADI Meeting or Retreat, submit the Chairman's Report to the ASEAN Defence Senior Officials' Meeting (ADSOM) for their information and attention, and for ADMM's consideration. The NADI Chairman will inform all heads of the NADI institutions and the NADI Secretariat of this action. The NADI Secretariat will only upload the NADI Chairman's Report onto the NADI website after ADSOM has been informed.

6. NADI members have agreed that NADI should remain the Track II forum to advise the ADMM, and membership should not be expanded to include any non-ASEAN country. This NADI position was highlighted during the 8th NADI Annual Meeting held in Kuala Lumpur in 2015.

7. NADI members may consider the development of activities, on an ad-hoc basis, with relevant think-tanks from within and outside ASEAN that specialise on defence and strategic issues of importance. Any engagement shall be determined by consensus. NADI must ensure that ASEAN remains in the driver's seat in such engagements, which must not affect NADI's established processes.

8. Bearing in mind the need to keep membership at a practical number to facilitate discussion, new institutions wishing to join NADI must secure the sponsorship of its host government and the consensus of all existing members. Any member institution that wishes to exit NADI must formally announce its intention to leave and provide a plan for a new institution

from the exiting institution's country to take its place. This does not apply to any country that has more than one institution represented at NADI.

D. Arrangement of NADI Meetings & Activities

1. *NADI Annual General Meeting:*

a. The main purpose of the Annual General Meeting is to review activities conducted throughout the year, revisit important points made and brainstorm on new ideas for the upcoming year. The delegations could also review the regional political and security environment and identify emerging challenges to peace and stability in the region.

b. The NADI Annual General Meeting shall meet once a year and shall cover two working days, which may include a visit programme. The Annual General Meeting is usually held either in March or April. This should be held as a physical activity, unless prevented by serious difficulties such as constraints imposed by a pandemic. For the conduct of virtual Meetings, please refer to Annex II.

c. The programme for the NADI Annual General Meeting should include a session with the Leader of the ADSOM for an exchange of views and for the NADI Chairman to brief ADSOM and for NADI members to have a better understanding of ADSOM's areas of interest. The NADI Chair can exercise flexibility over the timing of this session, as long as it is held within the first day.

d. New Meetings for the year can be proposed under the agenda item 'Other Matters'. The NADI delegation proposing a new Meeting should give a brief presentation on the theme, purpose and objectives of the Meeting, for consideration of the Annual General Meeting. It is highly recommended that NADI members should plan their Meetings in advance, so that NADI members will have ample time for preparations. NADI members are strongly encouraged to propose Meetings at the Annual General Meeting and use subsequent Meetings to update the other members of the agendas and other details of their proposed Meetings.

e. The hosting of the NADI Annual General Meeting shall be rotated alphabetically to coincide with the ASEAN country holding the Chairmanship of the ADMM.

f. The host's invitation letters to NADI core and partner institutions, and the NADI Secretariat should be sent out at least two months before the Annual General Meeting together with (a) the agenda, (b) the programme, (c) administrative notes to provide information on hotel accommodations, hotel rates, weather, local transport arrangements and (d) reply form on participation and delegation list, request for accommodation bookings, and the flight details (arrival and departure) of delegation.

g. NADI members shall pay for their own return air tickets, hotel accommodation and other personal expenses (telephone/fax services, laundry, mini bar, internet). However, host countries may offer to pay for the hotel accommodation of heads of delegations if they wish.

h. The host country shall provide participants with conference facilities and other local hospitalities.

i. By the end of the Annual General Meeting, the Chairman shall submit the agreed Chairman's Report to ADSOM for their attention and for ADMM's consideration. The Chairman's Report could include the NADI schedule of annual activities.

2. *NADI Meeting:*

a. The main purpose of the NADI Meetings is to discuss specific defence and security issues that were agreed on; and come up with a collective list of recommendations on how the issue should be dealt with.

b. The hosting of NADI Meetings is on a voluntary basis and does not have to be in an alphabetical order. The Meeting should be on a topic that can further enhance ADMM cooperation as well as cooperation among the militaries of the ASEAN countries.

c. NADI Meetings shall, as far as possible, be organised 2–3 times a year after the conduct of the Annual General Meeting for that year. Each Meeting shall cover 2 working days. The host may offer site visit during the Meeting. The Meeting should be held physically, unless prevented by serious difficulties such as constraints imposed by a pandemic. For the conduct of virtual Meetings, please refer to Annex II .

d. The scheduled Meetings may be arranged to be conducted every 3–4 months. This is to provide ample time for substantive preparations as well as budgetary concerns.

e. The host's invitation letters to NADI core and partner institutions, and the NADI Secretariat should be sent out at least two months before the Meeting together with (a) the agenda, (b) the programme, (c) administrative notes to provide information on hotel accommodations, hotel rates, weather, local transport arrangements and (d) reply form on participation and delegation list, request for accommodation bookings, and the flight details (arrival and departure) of delegation.

f. NADI members shall pay for the return air tickets and hotel accommodations of the heads as well as members of the delegations.

g. The host country shall provide participants with conference facilities and other local hospitalities.

h. The final outcome of the Meeting's report shall capture substantive discussions and recommendations agreed upon at the Meeting. The Chairman of the NADI Meeting shall submit the Chairman's Report to the ADSOM Chairman for circulation to ADSOM members for consideration.

i. Any matters pertaining to NADI activities and other issues to be followed up from the NADI Annual General Meeting could be taken up under agenda item 'Other Matters'.

3. *NADI Retreat:*

   a. The NADI Retreat should be organised and hosted by the NADI Chair when necessary.

   b. The purpose of Retreats, among others is to provide longer term recommendations for cooperation to the ADMM and its related meetings.

   c. For convenience, the NADI Retreat could be held back-to-back with the NADI Annual General Meeting or a NADI Meeting hosted by the NADI Chair. If a Retreat is held back-to-back with a NADI Annual General Meeting or a NADI Meeting, the total duration of the combined event can be up to two and a half working days.

E. Secretariat

1. RSIS, as agreed in the 1st NADI Meeting, shall be the main Secretariat of NADI.

2. The main role of the Secretariat is to provide an update on the current status of NADI activities and its website.

3. At the request of some NADI core institutions, the NADI Secretariat could provide advice on the conduct of NADI Annual General Meetings and NADI Meetings, and on the agenda of these activities.

F. NADI Website

1. With the agreement of all the NADI members, RSIS launched the NADI Website (www.rsis.edu.sg/nadi) in 2009, and continues to maintain it. The NADI Website highlights the work of NADI and maintains a record of the Chairman's Reports of the NADI Annual General Meetings and NADI Meetings.

2. Each Chairman's Report, along with its related annexes such as the agenda and programme, is to be uploaded onto the NADI Website by the NADI Secretariat after the host of the NADI event has submitted it to ADSOM and the ADMM track for their consideration.

3. The costs of maintaining the Website are borne by RSIS.

G. Review of TOR

1. The Terms of Reference shall be reviewed as needed.

Note
The NADI Terms of Reference (TOR) was proposed by the Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS) in March 2013 for consideration of the 6th NADI Annual Meeting in Brunei Darussalam. The TOR was agreed to on 7 March 2013. A second update was conducted

following suggestions from NADI delegations during the NADI Workshop held in Bali in October 2015. A third request for an update to the NADI TOR was made by NADI delegations during the Workshop held by Cambodia in October 2021, to better reflect the practice of NADI activities during COVID-19 pandemic situation. Consequently, a further update was made to the NADI TOR to reflect the change in nomenclature from "Annual Meeting" to "Annual General Meeting", and from "Workshop" to "Meeting", at the NADI 17th Annual Meeting in 2024.

(The NADI Secretariat has updated the TOR after further negotiation and consultation with NADI Members).

Dated 21 May 2024

XXXXX

ANNEX I

A. Suggested NADI Annual General Meeting/NADI Meeting Proceedings

1. It is suggested that the NADI Annual General Meeting or NADI Meeting be held for two working days, where one and a half days will be dedicated for discussions in the meeting. The host may also organise a half day site visit. The sequence of events of each NADI Annual General Meeting or NADI Meeting can be organised as follows:

   a. The programme may begin with a welcome dinner on the first evening after the arrival of delegates.

   b. On the first day, there could be welcome remarks by the host NADI Chairman to be followed by a keynote speech by a distinguished speaker, and then a group photograph-taking. The distinguished speaker is not expected to participate in the subsequent discussions by NADI delegates.

   c. The Annual General Meeting/Meeting resumes with the adoption of the agenda and programme.

   d. This may be followed by presentations on the agenda items, followed by a session for NADI delegates to exchange views on the relevant inputs and policy recommendations to be submitted to the ADMM track.

e. This could then be followed by an agenda item on "Other Matters" where updates on NADI Meetings, and other matters which the NADI Secretariat and other NADI delegations may raise. New Meetings can be proposed under this session. The NADI delegation proposing a new Meeting should give a brief presentation on the theme, purpose and objectives of the Meeting, for consideration of the meeting.

f. The first day could conclude with the host preparing a draft Chairman's Report for delegates to review in preparation for the consideration of the Chairman's Report the following day. NADI delegates shall agree on the collective inputs and recommendations but reserve their right to retain their individual inputs and recommendations in their respective sections of the Chairman's Report. However, other NADI delegates may still raise language or other clarification and this, together with the presenter's replies, could be also reflected in the Chairman's Report.

g. There may be an official dinner that evening.

h. In the morning of the second day, the NADI Annual General Meeting/NADI Meeting shall deliberate on the draft Chairman's Report and adopt it.

i. In the afternoon of the second day, the host may wish to arrange a site visit to a cultural or historical place, or to an institution of a defence and security nature which conducts activities relating to the NADI Annual General Meeting or NADI Meeting.

j. Before the delegates' departure, the host could provide each delegation a CD or thumbdrive containing some photographs of the meeting and the Chairman's Report.

ANNEX II

A. Arrangement of NADI Activities through Video-Teleconference (VTC)

1. In the event that NADI activities cannot convene physically due to an emergency situation, NADI can host activities virtually. This may require flexibility in terms of the arrangement of NADI activities, such as NADI Annual General Meetings, NADI Meetings and Retreats.

2. *NADI Annual General Meeting:*

   a. The virtual NADI Annual General Meeting may cover a maximum of three working days. The meeting can be held either in March or April.

   b. The host's invitation letters to NADI core and partner institutions, and the NADI Secretariat should be sent out at least two months before the meeting together with (a) the agenda, (b) the programme, (c) information on Meeting and IT Coordinators and (d) reply form on participation and delegation list.

3. *NADI Meeting:*

   a. Virtual NADI Meetings shall, as far as possible, be organised 4–5 times a year after the conduct of the Annual General Meeting for that year. Each Meeting should cover a maximum of three working days. It is strongly encouraged that NADI members should propose Meetings at the Annual General Meeting and use subsequent Meetings to

update the other members of the agendas and other details of their proposed Meetings.

b. The scheduled activities may be arranged to be conducted every 1-3 months. This is to provide ample time for substantive preparations, especially research and budget preparations.

c. In the event that a NADI Member would like to host a physical Meeting, it should be scheduled at least two months after the last virtual Meeting.

d. The host's invitation letters to NADI core and partner institutions, and the NADI Secretariat should be sent out at least two months before the Meeting together with (a) the agenda, (b) the programme, (c) information on Meeting and IT Coordinators and (d) reply form on participation and delegation list.

4. *Virtual Pre-test and Dry-Run:*

a. The pre-test and dry-run for the video-conferencing may be held one to two days prior to the NADI activities.















Strategic Studies Center,
National Defence Studies Institute

62 Vibhavadi Rangsit Rd., Dindaeng, Bangkok, 10400, Thailand.
Tel./Fax: 0-2572 2313, Website: www.ssctheiland.org