CHAIRMAN'S REPORT OF
Track II Network of ASEAN Defence AND SECURITY INSTITUTIONS (NADI) Meeting

Artificial Intelligence (AI) in Defence: Potential and Challenges for ADMM Cooperation

26 – 29 August 2025
The Heritage Pattaya Beach Resort, Chonburi Province, Thailand

1. Track II Network of ASEAN Defence and Security Institutions (NADI) Meeting on **"Artificial Intelligence (AI) in Defence: Potential and Challenges for ADMM Cooperation"** was organized by Strategic Studies Center (SSC), National Defence Studies Institute (NDSI), at The Heritage Pattaya Beach Resort, Chonburi Province, Thailand, from 26 – 29 August 2025.

2. Representatives from Brunei Darussalam, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Republic of the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand, and the Socialist Republic of Vietnam attended the meeting. The list of participants is attached in Annex I. Major General Nirut Duangpanya, Director of the Strategic Studies Center, National Defence Studies Institute, Royal Thai Armed Forces, chaired the meeting.

Opening Remarks by General Nakrob Boonbuathong, Senior Adviser, National Defence Studies Institute (NDSI), Royal Thai Armed Forces Headquarters

3. The meeting was conducted under the theme "Artificial Intelligence (AI) in Defence: Potential and Challenges for ADMM Cooperation," a topic of great timeliness and importance to ASEAN and the wider world. Artificial Intelligence (AI) is rapidly transforming defence and security with its capabilities in processing vast amounts of data, enabling autonomous decision-making, and advancing weapon technologies. The speech emphasized the need for ASEAN to assess both the opportunities and risks of AI in defence, and to strengthen regional cooperation to monitor and prevent associated threats. The meeting was expected to generate valuable insights and foster a deeper understanding of AI's implications, guiding future ADMM cooperation

Adoption of Agenda:

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

SESSION I: Keynote Speaker

Keynote speech on "Artificial Intelligence (AI): Potential and Challenges" by Assoc. Prof. Dr. Supan Tungjitkusolmun, President of CMKL University

5. The world today faces urgent challenges: geopolitical uncertainty, rapid digital transformation, growing cybersecurity threats, and the pressing need for resilient societies. Artificial Intelligence (AI) stands at the center of these issues—not only as a disruptive technology, but also as a potential enabler of solutions. To understand its role, it is essential to be clear about what AI is, where it originated, and how it is evolving. From its early

foundations in symbolic reasoning to today's breakthroughs in machine learning and generative models, AI has rapidly advanced into a transformative force.

6. Dynamic trends are shaping AI's future: generative systems that redefine creativity, edge computing that brings intelligence closer to the battlefield and the factory floor, and human-AI collaboration that enhances decision-making in both civilian and defence contexts. As Thailand's first AI-focused university, CMKL has been at the forefront of developing talent, conducting research, and fostering partnerships in this critical field. Yet the potential of AI comes with profound challenges, including governance, trust, ethics, and security. This talk, Artificial Intelligence (AI): Potential and Challenges, examines today's challenges, the evolution and trends of AI, and the responsibility of leaders to harness AI as both a source of strategic advantage and a driver of societal progress and stability.

SESSION II: Presentation on the "AI in Defence: Implications for Regional Security and Way Forward for ADMM Cooperation"

Republic of Indonesia (CSSRD, TNI)

Presentation by Brigadier General Tarsisius Yoga Pranoto, S.Sos. Center for Strategic Studies, Research and Development of Tentara Nasional Indonesia (CSSRD TNI)

7. Brigadier General Tarsisius Yoga Pranoto highlighted that the integration of artificial intelligence (AI) in the defence sector is a strategic necessity for ASEAN in addressing both conventional and non-conventional security threats in the digital era. While AI offers transformative potential in enhancing military effectiveness and regional cooperation, challenges such as capability gaps, ethical dilemmas, and cyber risks demand a collective and coordinated response.
8. Through the Complex Interdependence approach and the principles of Responsible Innovation, ADMM, and ADMM-Plus can steer the utilization of AI toward strengthening regional stability, technological independence, and collective defence solidarity. Therefore, he recommended ADMM to

    a. Establish an ASEAN AI in Defence Working Group as a permanent technical body under ADMM tasked with formulating regulations, ethical standards, and system interoperability for ASEAN military AI, while also facilitating dialogue between the military, technologists, and policymakers.
    b. Draft an ASEAN Code of Responsible Military AI as a normative document containing ethical principles, usage limitations, and accountability protocols in the development and application of AI for defence and security purposes in the region.
    c. Promote collaborative AI projects in priority sectors such as Military Medicine, HA/DR, Defence Education, and Border Management through pilot projects, joint exercises (TTX), and shared data platforms to strengthen interoperability and strategic trust among ASEAN member states.

Lao People's Democratic Republic

Presentation by: LT.COL Souksan Khaiphom, Director of the Office of Military Science-History Department (MSHD), Ministry of National Defence (MOD), Lao PDR

9. Artificial Intelligence plays a vital role in today's defence and security landscape. AI, as a result, has been increasingly integrated into applications in the defence sector to potentially maximize defence capabilities and performance. While AI enhances security, battlefield awareness, efficiency, and decision-making, it also reduces risks to human soldiers. However, there are ethical, technical, and security concerns regarding its accountability, transparency, biases, and over-reliance on AI. Vulnerability to cyberattacks and disparities in the AI domain among members also remain a key challenge for ASEAN.
10. Given its vital benefits and drawbacks, AI has become an important tool and has increasingly gained more attraction in the defence sector, especially under the ASEAN Defence Ministers' Meeting (ADMM) and ADMM-Plus. The Joint Statement by the ASEAN Defence Ministers on Cooperation in the Field of Artificial Intelligence in the Defence Sector adopted by the ASEAN Defence Ministers' Meeting Retreat in Penang, Malaysia in February 2025 has demonstrated ADMM's commitment in enhancing capabilities in AI domain among AMS through the existing platforms particular those under the ADMM framework to promote regional resilience since such engagements will allow ASEAN Member States not only to share best practices and expertise, conduct trainings and joint exercises to improve capacity and response protocols, but also to create a shared framework of ethical guidelines for the development and deployment of AI in defence to promote responsible AI use and awareness of the implications of AI.

Malaysia (MiDAS)

Presentation by Lieutenant General Dato' Seri Haji Muhammad Huzaimi bin Sabri, Chief Executive, Malaysian Institute of Defence and Security (MiDAS).

11. The presentation highlights the growing challenges posed by advanced technologies, particularly Artificial Intelligence (AI), in the global defence and security landscape. AI is rapidly reshaping modern warfare, enabling new capabilities such as autonomous drones and predictive threat assessments, while also creating unprecedented risks, including the rise of deepfake technologies and sophisticated cybercrime. Militarized applications of AI in autonomous weapon systems and decision-support systems raise significant ethical concerns, particularly regarding reliability, fairness, and transparency.
12. To address these challenges, MiDAS recommends that ASEAN adopt a unified, strategic, and collaborative regional approach. In the short term, this includes establishing common guidelines for responsible AI use based on the ASEAN Guide on AI Governance and Ethics, as well as capacity-building initiatives to enhance digital literacy. In the long-term actions, MiDAS advocates for binding regional AI policies to facilitate cross-border coordination and leverage AI to drive sustainable development in areas such as disaster management. Prioritizing ethical standards, transparency, and accountability in defence applications of AI is crucial to ensure it contributes positively to regional stability and harmony.

Republic of the Union of Myanmar

Presentation by Brigadier General Win Bo, Deputy Chief of Armed Forces Training (Strategic Studies), Office of the Chief of Armed Forces Training (OCAFT)

13. In his presentation, BG Win Bo explored the growing role of Artificial Intelligence (AI) in the defence sector, especially in the context of ASEAN and regional security. He mentioned that AI is becoming an essential part of everyday life and is transforming every sector, including defence. It was noted that AI is already being utilized in various military applications, including surveillance, autonomous systems, cyber defence, and decision-making. He provided examples of how countries and regional bodies are investing in AI to strengthen their national and collective security. The presentation highlighted that ASEAN, while recognizing the value of AI, focuses not only on its opportunities but also on its potential risks and challenges. He explained that AI could enhance regional defence through better early warning systems, improved intelligence sharing, and faster crisis response. It could also support counter-terrorism efforts, maritime monitoring, cybersecurity, peacekeeping operations, military medicine, humanitarian assistance, and clearance operations. However, he also noted challenges, such as unequal technological development among AMS, a lack of shared frameworks, ethical concerns, and the risk of an AI arms race. He mentioned that while ASEAN's tradition of non-interference and consensus-based decision-making helps preserve unity and trust, it can also slow the adoption of robust AI-based security strategies. ASEAN's limited funding and infrastructure in some AMS were also identified as obstacles. He stressed the importance of addressing these issues now, before AI developments outpace regional preparedness.
14. He examined ASEAN's current capacity and cooperation efforts regarding AI in the defence domain. It was pointed out that ASEAN does not yet have a joint military AI program or a dedicated defence research institution focused on AI. However, existing mechanisms, such as the ADMM and ADMM-Plus, were highlighted as useful platforms for dialogue and coordination. He observed that some AMS are more advanced in AI development, while others lag behind due to a lack of infrastructure and resources. He described ASEAN's initial steps, such as its Digital Masterplan 2025 and working groups related to cybersecurity and humanitarian assistance, as promising signs. It was suggested that partnerships with external actors, such as the US, China, Japan, and the EU, could help strengthen ASEAN's AI capabilities through training, policy exchange, and technology sharing. He clearly stated that ASEAN must overcome gaps in policy, coordination, and trust to benefit from AI technologies without increasing regional tensions. Towards the end, he focused on what the ADMM should do to move forward. He recommended establishing a shared framework for responsible and ethical use of AI in defence and security; promoting joint education, training, and partnerships to build AI capacity across ASEAN defence establishments; leveraging existing ASEAN mechanisms to coordinate AI policies, exercises, and knowledge sharing; engaging external partners, including ADMM-Plus countries and international organizations, to align with global standards; and advancing peaceful AI applications in disaster relief, peacekeeping, and humanitarian missions to reinforce ASEAN's role as a zone of peace. These steps, he believed, would help ASEAN maintain its peace and stability in a rapidly evolving security environment.

Republic of the Philippines (NDCP)

Presentation by Ms. CHRISTINE LISETTE M CASTILLO, Defense Research Officer II, NDCP

15. In her presentation, Ms. Christine Lisette Castillo discussed the promises and perils of artificial intelligence (AI) in defence. Regarding the promises and advantages, Ms. Castillo noted that AI can play a crucial role in battlefield success through its integration in geospatial data, command and control, military training and simulations, and military medicine. AI

integrated into autonomous systems also provides advantages in warfare, exemplified by unmanned aerial vehicles (UAVs) or drones used for reconnaissance and combat operations, as well as radar systems used for tracking and monitoring. Furthermore, Ms. Castillo stated that AI technologies can help inform strategic decision-making and situational awareness for executive authorities, as well as combat disinformation and malign information operations. For the perils and risks of AI in defence, Ms. Castillo discussed the ethical concerns about the ability of autonomous AI systems to think and act independently, which raises discussions about accountability and the need for human oversight. Meanwhile, AI-powered cyber-attacks and attacks on AI systems are also considered risks. Ms. Castillo highlighted that AI-powered cyber-attacks leverage AI or machine learning algorithms and techniques to automate, accelerate, or enhance various phases of a cyber-attack. Another risk is AI-altered media content, where generative AI enables the creation of deepfake videos with the intention of deception and the dissemination of disinformation. In addition, AI-altered media content acts as a primary tool in the conduct of malign information operations.

16. In this regard, Ms. Castillo presented several ways forward for regional cooperation on AI in defence. First, the ADMM may consider developing ASEAN guidelines on the responsible use of AI in defence. It is important to ensure that AI in defence, particularly its use in the military, is regulated and conforms to the laws governing armed conflict, such as international humanitarian law. Second, the ADMM should foster close collaboration with the private sector in maximizing the potential of AI in defence and in addressing the risks brought by AI. Given that the private sector outpaces the government in technological innovations, the defence ministries of AMS will benefit from closely collaborating with private tech companies in the region through knowledge exchange, learning of best practices, and research and development. Third, the ADMM may consider prioritizing defence education and training on AI in defence. Defence education should include developing critical thinking skills among relevant defence personnel and soldiers, as this is crucial for understanding how AI systems work in defence and for mitigating the risks associated with AI. Fourth, the ADMM should further explore and highlight the advantages of AI in defence, such as those for maritime domain awareness and cyber defence. One opportunity for regional cooperation is to put focus on AI use for maritime domain awareness. The use of AI systems allows better situational awareness, early detection, and prediction of incidents that may happen at sea.

Kingdom of Thailand

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

17. Artificial Intelligence (AI) is rapidly transforming defence and security in ASEAN, offering opportunities to enhance humanitarian assistance and disaster relief (HA/DR), strengthen border management, and modernize defence education. For Thailand, AI can improve predictive disaster response, optimize logistics, and foster regional trust through non-traditional security cooperation. In border security, AI-enabled surveillance, data fusion, and autonomous patrols can help combat smuggling, trafficking, and insurgent movements, while adaptive learning platforms and AI-driven simulations will advance military education and leadership development. These applications not only improve efficiency but also promote transparency, interoperability, and confidence-building within ASEAN frameworks such as ADMM and ADMM-Plus.

18. However, challenges remain significant. Risks include the potential for an AI arms race, algorithmic bias, cyber vulnerabilities, and the absence of unified ethical governance across ASEAN. Unequal adoption could widen security gaps, while over-reliance on technology may erode human judgment. To mitigate these risks, ASEAN must prioritize shared ethical standards, transparency, and interoperability. Establishing monitoring mechanisms, scenario-based exercises, and capacity-building initiatives will strengthen regional resilience. For Thailand, embedding AI literacy across defence institutions and aligning national AI governance with ASEAN frameworks will be critical to balancing innovation with security. If responsibly managed, AI can serve as a tool for building trust and promoting collective security in the region.

SESSION III: Presentation on "AI in Defence: Implications for Regional Security and Way Forward for ADMM Cooperation"

Brunei Darussalam

Presentation by Siti Nurnabilah Haji Abd Rahman, Research Officer at the Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies, Ministry of Defence, Brunei Darussalam

19. ASEAN's 2025 ASEAN Defence Ministers' Meeting (ADMM) Joint Statement on Cooperation in the Field of Artificial Intelligence in the Defence Sector represents a significant regional commitment to responsible AI governance. It underscores the importance of transparency, human-in-the-loop (HITL) oversight, adherence to International Humanitarian Law (IHL), and capacity-building through the sharing of best practices. However, there are notable gaps, including a lack of comprehensive governance and ethical safeguards, as well as disparities in technological capacity among member states. These gaps heighten the risks of misperceptions, strategic miscalculations, and uncoordinated AI development.
20. To address these challenges, ASEAN should consider establishing a Defence AI Code of Practice at the multisectoral level. The Code would serve as a normative framework, formalizing shared principles to ensure the ethical, transparent, and accountable use of AI in defence. It would enhance interoperability, build trust among member states, and provide common standards for governance, oversight, and incident management. In parallel, ASEAN could also develop a Multilayered Defence AI Research and Development Consortium. Unlike the Code, which focuses on governance and principles, the Consortium would serve as a practical innovation platform to pool expertise, funding, and infrastructure for joint R&D. It would enable collaborative projects in areas such as maritime domain awareness and humanitarian assistance and disaster relief (HADR), strengthen technological sovereignty, reduce reliance on external providers, and promote sustained cooperation and innovation across the region.

Republic of Indonesia (RIDU)

Presentation by FADM Ruby Alamsyah, M.Han., M.Tr.Opsla., MCE. (Secretary of the Institute for Research and Community Service, RIDU).

21. **Artificial intelligence (AI) in the Defence Sector** offers transformative opportunities for the ASEAN region, but it also carries significant risks that demand proactive, cooperative management. From the perspective of opportunities, artificial intelligence can enhance situational awareness, strengthen maritime domain monitoring, improve predictive maintenance and logistics, enable rapid-response autonomous defence platforms, and fortify

cyber defence capabilities through advanced pattern recognition and real-time threat detection. From the perspective of challenges, concerns include an artificial intelligence-driven arms race that could destabilize strategic balances, the risk of algorithmic errors leading to unintended escalation, the possibility of misuse by non-state actors, the lack of universal ethical and operational guidelines, and uneven technological capabilities across member states. In terms of regional cooperation, the ASEAN framework can serve as a platform to establish joint monitoring mechanisms, create shared ethical standards, facilitate secure intelligence and data exchange, conduct artificial intelligence-enabled joint exercises, and promote collaborative research and development to reduce dependence on external suppliers. However, these initiatives will require overcoming differences in national capacities, managing the tension between security confidentiality and data-sharing needs, resolving differing perceptions of risk, and defending shared systems against cyber intrusions. Addressing NTS challenges requires ASEAN to adopt a holistic and cooperative approach that focuses on tangible and measurable goals. ASEAN can effectively navigate these complex challenges by enhancing institutional frameworks, promoting information sharing, investing in capacity building, and strengthening regional and international cooperation. A unified and resilient ASEAN will not only safeguard regional stability but also contribute to sustainable development and human security. The journey ahead requires concerted and coordinated efforts, innovative strategies, and unwavering commitment from all ASEAN member states and stakeholders. Examining potential applications within the ADMM and ADMM-Plus framework, AI can contribute directly to maritime security, counter-terrorism, cyber defence, peacekeeping operations, and confidence-building measures. Nonetheless, success will depend on overcoming interoperability issues, preventing misuse of shared intelligence, ensuring legal compliance, and safeguarding systems from manipulation.

22. **Recommendations.**
    a. Establish a Regional Code of Conduct on Artificial Intelligence in Defence. Formulate and adopt a binding document outlining ethical principles, operational limits, and legal compliance requirements for the deployment of artificial intelligence in defence operations.
    b. Create a Regional Artificial Intelligence Threat Intelligence Sharing Centre. Develop a secure, centralized hub for sharing timely and actionable intelligence on threats related to artificial intelligence applications in defence.
    c. Conduct Regular Joint Exercises with Artificial Intelligence-enabled Scenarios. Organize multi-nation exercises using realistic simulations to test interoperability, evaluate preparedness, and refine joint operational protocols.
    d. Develop a Long-term Regional Roadmap for Artificial Intelligence in Defence. Produce a strategic plan covering research, development, capability building, and regulatory alignment over a multi-year horizon, ensuring balanced access to technology for all member states.
    e. Ensure Compliance with International Law and Humanitarian Principles. Integrate the provisions of international humanitarian law and existing multilateral security agreements into all regional artificial intelligence defence policies, maintaining the spirit of mutual respect and trust that defines ASEAN cooperation.

f. Promote Capacity Building and Technology Transfer. Implement programs to close the technological capability gap among member states through training, knowledge exchange, and joint development projects.
g. Implement Resilience Measures Against Adversarial Manipulation. Establish robust technical safeguards, verification systems, and testing protocols to protect artificial intelligence systems from manipulation, data poisoning, or other adversarial attacks.

Malaysia (NDUM)

Presentation by Professor Dr. Adam Leong Kok Wey, Director, Centre for Defence and International Security Studies (CDISS), National Defence University of Malaysia (NDUM)

23. ASEAN today faces a multitude of Artificial Intelligence (AI)-enabled threats—ranging from cyber terrorism to the use of AI for maritime piracy. AI technology itself poses a shared risk for ASEAN Member States (AMS), as it may one day surpass human control and initiate its own power-grabbing operations, resulting in an AI-dominated world. Although ASEAN has launched some collective responses to cybersecurity risks, the region still lacks a targeted approach for addressing emerging AI-enabled security risks. While AI-driven crime should be countered through policing and law enforcement measures, AI-driven terrorism, maritime piracy, and AI-related political and strategic risks require AI-enhanced military defensive and offensive operations, as well as ethical and regulatory frameworks. Such measures could be coordinated through ADMM/ADMM-Plus platforms to ensure that ASEAN Centrality remains the guiding principle in mitigating AI-related security risks in Southeast Asia.
24. There is an urgent need for a concerted effort to manage and mitigate AI-driven security risks and to address regional AI security challenges. The National Defence University of Malaysia (NDUM) recommends integrating an AI-security agenda into the ADMM-led ASEAN Cyber Defence Network (ACDN), rather than establishing a new platform specifically for AI issues. This approach would minimize duplication of effort and create a centralized command hub for AI-security activities, including capacity building, joint exercises, resource sharing, defensive measures, and offensive operations. Such a framework would promote coordinated regional collaboration with a clear strategic direction. More importantly, the ACDN must deliberate and establish regional AI ethics, regulations on AI, and AI research and development guidelines to ensure continued human mastery over AI - preventing AI from becoming an “entity” that could challenge humanity and compete for control over global systems and political domination of the world.

Republic of the Philippines (OSSSM)

Presentation by CAPTAIN JAMES S RAMON JR PN (MNSA), Chief, Policy Studies Division, Office of Strategic Studies and Strategy Management (OSSSM), Armed Forces of the Philippines.

25. The presentation by CAPT RAMON highlighted that while ASEAN Member States are increasingly integrating AI into defence, disparities in readiness and governance remain evident. AI presents valuable opportunities for the region, including enhanced maritime domain awareness in contested areas, improved predictive analytics for threat assessments, and the development of advanced training simulations to strengthen interoperability and preparedness of ASEAN forces. At the same time, serious challenges persist, particularly the risk of AI misuse for misinformation, deepfakes, and data manipulation, as well as the potential for miscalculation and accountability gaps arising from autonomous decision-making.

26. CAPT RAMON underscored the importance of leveraging established mechanisms such as the ADMM Cybersecurity and Information Centre of Excellence (ACICE), the ASEAN Cyber Defence Network (ACDN), and the AI-Ready ASEAN initiative to strengthen threat detection, response, and literacy. He further emphasized that the principles outlined in the ASEAN Guide on AI Governance and Ethics, such as human oversight, accountability, and transparency, should be expanded and applied to the defence sector, in alignment with international best practices, including NATO standards, the EU AI Act, and the Tallinn Manual. Furthermore, CAPT RAMON recommended that the ADMM focus on scaling up joint research, capacity-building, and regional exercises, while embedding robust safeguards to ensure the responsible use of AI in defence, thereby reinforcing ASEAN's resilience and centrality in the evolving regional security landscape.

Republic of Singapore

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

27. In his presentation, Mr. Faizal said that the impact of artificial intelligence (AI) on organizational behavior is profound. AI is transforming how militaries think and prepare for a multitude of challenges by providing them with smarter tools to augment human judgment and effort. Operationally, AI features significantly in the future of warfare, as technology influences military intelligence, strategy, operations, and the conduct and rules of warfare. Strategically, AI in defence capabilities is shaping global power dynamics, thereby creating spheres of influence where geopolitics and technology intersect.
28. The adoption of AI in defence is an unstoppable trend. It is similar to how the emergence of aviation technology in the early 1900s foreshadowed a change in the character of warfare. To manage the risks, four recommendations are proposed:
    a. First, ASEAN should explore how to leverage these existing ADMM platforms better to monitor AI risks. Discussions and analysis reports produced by these platforms should be shared with the relevant departments in ASEAN defence ministries.
    b. Second, cross-pillar exchanges on risks and the responsible use of AI could be initiated between ADMM representatives, who are part of the Political-Security Community, and the ASEAN Working Group on AI Governance (WG-AI), which is part of the Economic Community.
    c. Third, ASEAN militaries could explore incorporating AI in non-combat applications, particularly in the various areas of practical cooperation under the ADMM-Plus EWGs. ADMM-related exercises that incorporate elements of AI could inform efforts to develop confidence-building measures.
    d. Fourth, cross-pillar exchanges between ADMM representatives and the ASEAN Regional Computer Emergency Response Team (CERT) could foster a deeper understanding of cyber threats to AI systems and AI-enabled cyber threats to critical infrastructure essential to military functions

Socialist Republic of Vietnam

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

29. Senior Colonel Vu Cao Dinh emphasized that AI is being increasingly used in military and defence applications, which presents both opportunities and challenges for regional security.

There are five main groups of tasks AI can undertake in the military, such as integration into weapon systems to create smart or autonomous weapons, participation in operational planning by analyzing and predicting situations based on operational data, direct involvement in the command-and-control process, support for training activities, and application in logistics and technical support. These applications help to minimize risks to military personnel while enhancing the effectiveness of military operations. Nevertheless, AI applications in the military and defence field could pose ethical and legal challenges, present cybersecurity risks, potentially lead to a new arms race, and create difficulties for counterterrorism efforts.

30. To harness the opportunities of AI applications in the military and defence domain while mitigating the risks entailed, Sr. Col. Dinh recommended that ADMM should introduce initiatives to enhance awareness and capacity to research, develop, and apply AI in the military and defence domain, particularly in less sensitive fields such as prevention and response to non-traditional security challenges. Besides, ADMM should develop a code of AI governance in the military and defence domain, along with accompanying guidelines, to provide a legal foundation for the responsible and trustworthy development of AI in this area. In addition, ADMM should encourage cooperation with partners in researching, developing, and applying advanced AI technologies to prevent and respond to non-traditional security threats.

Discussion

31. Participants agreed that the presentations reflected similar perspectives, with a broad consensus that AI is a double-edged sword—offering opportunities to enhance defence while posing serious risks that cannot be ignored. They emphasized that halting AI is not an option, and instead, ASEAN must learn to adapt while addressing disparities in AI capacities across the region. Suggestions were made to create working clusters and retain technical groups to guide regional efforts.
32. Delegates highlighted that ASEAN already has established mechanisms, such as the ASEAN Cyber Defence Network (ACDN), the ASEAN Cybersecurity and Information Centre of Excellence (ACICE), and the AI-Ready ASEAN initiative. These platforms could be further leveraged to strengthen threat detection, response, and digital literacy. However, participants noted that most existing initiatives focus on civilian applications, while defense-specific aspects remain underdeveloped. There was a strong call to maximize current mechanisms for governing both the use and misuse of AI in defence, ensuring compliance with International Humanitarian Law (IHL).
33. The discussion also raised concerns about the exponential growth of AI and the risks of overreliance, which could erode human cognitive abilities and undermine decision-making, particularly among soldiers and younger generations. Participants emphasized the lack of a global governing institution for AI, unlike in the cybersecurity domain, and urged ASEAN to examine AI's risks more thoroughly. Some experts even suggested that AI could be recognized as a new defence domain, alongside land, sea, air, space, and cyber.
34. Delegates reflected on lessons from ongoing conflicts, such as Ukraine and Israel, where AI has been deployed in facial recognition, autonomous drones, and battlefield decision-making. These cases highlighted both the advantages and vulnerabilities of AI in defence, particularly the risks of dependency on external technology providers and critical infrastructure, such as commercial satellite services.

35. Overall, participants emphasized the need to balance innovation with safeguards, strengthen governance and ethical standards, and fully utilize ASEAN's existing frameworks to ensure that AI becomes a source of resilience and security, rather than instability and vulnerability, for the region.

Recommendations

36. ADMM should develop a Code of Responsible Military AI and a Defence AI Code of Practice to help ensure ethical, transparent, and accountable use of AI in defence, aligned with International Humanitarian Law (IHL) and the ASEAN Guide on AI Governance and Ethics.
37. ADMM could look into establishing a Regional AI Threat Intelligence Sharing Centre, while also integrating AI-security agendas into existing mechanisms such as the ASEAN Cyber Defence Network (ACDN), ADMM Cybersecurity and Information Centre of Excellence (ACICE), and the AI-Ready ASEAN initiative.
38. ADMM could encourage wider collaboration with the private sector, external partners, and cross-pillar exchanges (e.g., between ADMM, WG-AI, and ASEAN CERT) to advance AI technologies for non-traditional security threats while remaining mindful of risks such as cyber vulnerabilities.
39. ADMM should promote AI applications in collaborative projects and activities under ADMM-Plus Experts' Working Groups as well as in defence industry, defence education, and confidence building measures.
40. ADMM should develop a Long-term Regional Roadmap for Artificial Intelligence in Defence and produce a strategic plan covering research, development, capability building, enhancement of digital literacy, and regulatory alignment over a multi-year horizon, ensuring balanced access to technology for ASEAN Member States (AMS).

Other Matters

41. Forthcoming NADI activities

Date	Activities	Country	Via
10 - 13 November 2025	Meeting on "The Evolving Character of Warfare: Readiness and Adaptation"	Brunei	Physical
20 – 24 April 2026	Annual General Meeting / Retreat	Manila - Philippines	Physical
June/July 2026	NADI Meeting	Thailand (Place & Topic-TBC)	Physical
Oct/Nov 2026	NADI Meeting	Vietnam (Place & Topic-TBC)	Physical

Consideration of NADI Meeting Chairman's Report

42. The meeting considered the draft Chairman's Report of the NADI Meeting on "Artificial Intelligence (AI) in Defence: Potential and Challenges for ADMM Cooperation." After examining the Chairman's Report carefully, the meeting endorsed the report.
43. The NADI Meeting Chairman will submit the Report to ADMM through ADSOM for consideration and a copy to the NADI Chairman.

Concluding Remarks by Major General Nirut Duangpanya, Director of the Strategic Studies Center (SSC), National Defence Studies Institute (NDSI), Royal Thai Armed Forces

44. In his closing remarks, Major General Nirut expressed sincere gratitude to all delegates for their active participation, valuable insights, and strong commitment throughout the two-day meeting on "Artificial Intelligence (AI) in Defence: Potential and Challenges for ADMM Cooperation." He highlighted that the discussions underscored the importance of cooperation and collaboration in addressing both the opportunities and risks associated with AI in defence. Major General Nirut commended the spirit of solidarity and mutual support demonstrated by academics and experts across ASEAN, noting that such engagement will meaningfully shape regional security strategies. Appreciation was extended to General Nakrob Boonbuathong for presiding over the opening ceremony, and to the Strategic Studies Center for organizing the event. He encouraged participants to carry forward the momentum and insights gained to strengthen cooperation and build a secure and prosperous future for the region, before formally closing the meeting.