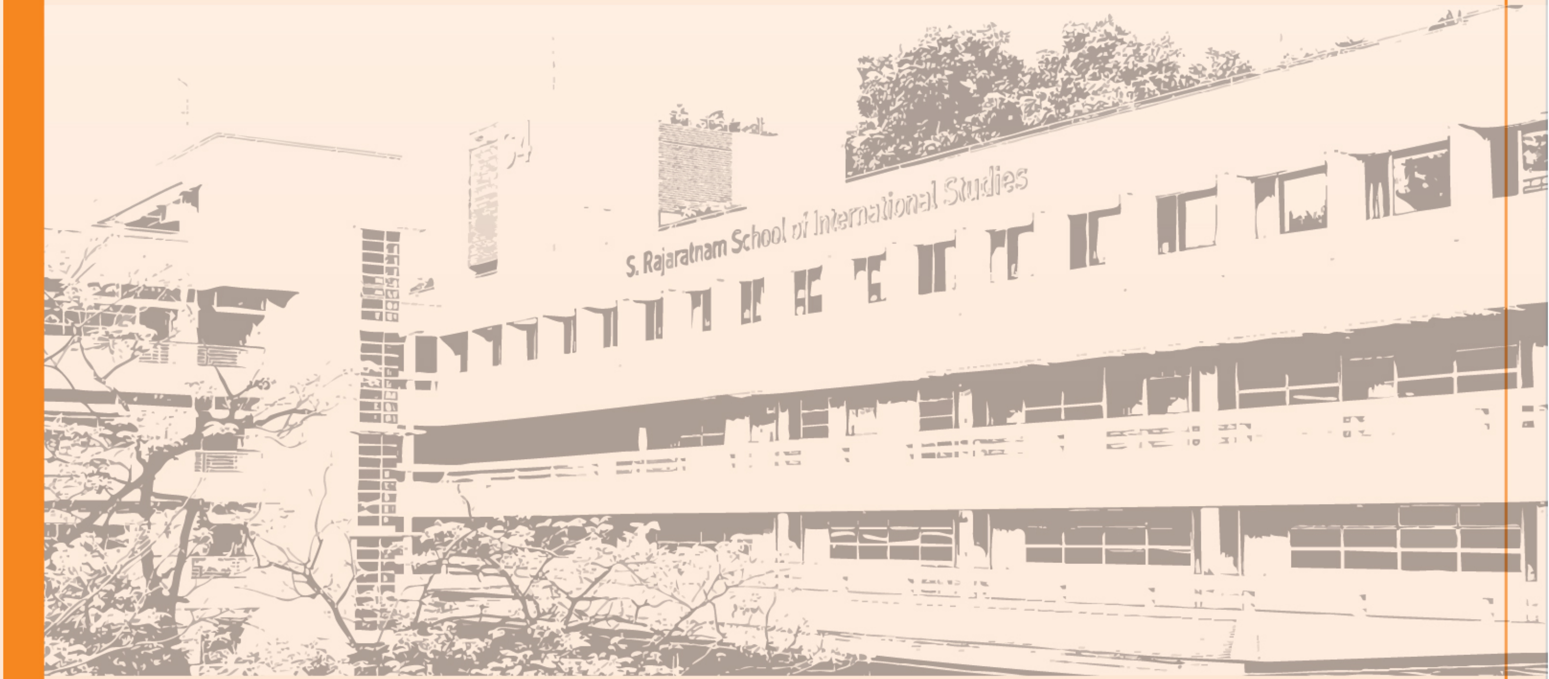
IDSS PAPER

29 August 2025

AI in Defence: The Way Forward for ASEAN's ADMM Cooperation

Muhammad Faizal Bin Abdul Rahman



RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ponder the Improbable since 1996

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No.084– 29 August 2025

The authors' views are their own and do not represent the official position of the Institute of Defence and Strategic Studies of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the authors and RSIS. Please email to Editor IDSS Paper at RSISPublications@ntu.edu.sg.

AI in Defence: The Way Forward for ASEAN's ADMM Cooperation

Muhammad Faizal Bin Abdul Rahman

SYNOPSIS

The ASEAN Defence Ministers' Meeting (ADMM) Retreat in February 2025 adopted the joint statement on Cooperation in the Field of Artificial Intelligence (AI) in the Defence Sector. As the 19th ADMM in November 2025 draws nearer, it is timely for ASEAN militaries to think of the way forward for regional cooperation in this area.

COMMENTARY

AI has been described as the holy grail of digital technology and an integral component in defence modernisation. It enables computers and machines to think and learn, which in turn can support defence strategic planners, commanders and soldiers in their tasks during both peacetime and conflict.

As the 19th ASEAN Defence Ministers' Meeting (ADMM) in November 2025 draws nearer and ASEAN militaries plan for future multilateral cooperation, they could examine the multidimensional impact – both the opportunities and risks – of using AI in defence, consider how to cooperatively monitor the key risk issues, and explore where AI can support practical cooperation in the ASEAN defence context.

Multidimensional Impact of AI in Defence

The impact of AI on organisational behaviour is profound. AI is transforming how militaries think and prepare for a multitude of challenges by providing them with smarter tools to augment human judgement and effort. These apply to operations both in the physical world and cyberspace.

For example, the US Cyber Command has submitted a budget request for 2026 to fund the development of an AI roadmap, which it unveiled in 2024, aimed at maintaining superiority in cyber operations. Likewise, China is using DeepSeek AI for non-combat functions and combat simulation scenarios.

At the operational dimension, AI features significantly in the future of warfare as the technology influences military intelligence, strategy, operations and the conduct and rules of warfare.

AI is transforming how militaries think and prepare, influencing intelligence, strategy, operations and the conduct and rules of warfare. *Image source: The Dutch Ministry of Foreign Affairs via Flickr.*

In August this year, the Singapore Armed Forces (SAF) announced that new soldiers will learn to operate drones on the battlefield to enhance their spatial awareness and fighting capabilities. This development draws on lessons from the Russia-Ukraine conflict, where both sides are competing in the development and deployment of AI-powered drones for warfighting.

At the strategic dimension, the incorporation of AI in defence capabilities is shaping global power dynamics. Advanced countries are investing more in AI to enhance their soft power, by, for instance, exporting military AI solutions and influencing standards in the development and norms of military AI use, thereby creating spheres of influence where geopolitics and technology intersect.

Additionally, investments in AI can make cognitive warfare more persuasive, thereby transforming hard power. Improvements to the precision and lethality of conventional military capabilities can have a profound impact on deterrence by affecting the soldiers' will to fight and how adversaries calculate risks and gains on the battlefield.

An instructive case study on AI risks is the India-Pakistan conflict in May this year. On the cognitive front, disinformation was widespread on both sides, thickening the fog of war. AI-generated deepfake videos were shaping narratives and opinions.

First, there was the risk of distorted threat perceptions triggering miscalculations that could lead to military escalation or, worse, a nuclear crisis. Second, AI-generated disinformation in the post-conflict landscape served to perpetuate tensions between both sides, making it more challenging to repair bilateral tensions and restore regional security.

On the kinetic front, both sides fought their first drone war, with swarm tactics and loitering munitions being used to overwhelm air defences, create psychological impact and conduct cross-border targeting without deploying manned aircraft.

Although such AI-powered unmanned systems may offer a restrained form of warfare, certain risks could emerge as these systems lower the operational and political threshold for military action.

First, these systems lower the cost of conflict. They could normalise frequent and low-intensity strikes that may unintentionally escalate into bigger confrontations. Second, concerns over each side's motives have embroiled them in an AI-driven arms race in preparation for future conflict. In a post-conflict landscape, these risks could leave regional security in a more fragile state.

Monitoring AI Risks

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 and enabled militaries to conduct peacetime operations such as humanitarian assistance and disaster relief (HADR).

Nonetheless, there are key risk issues that ASEAN should monitor to prevent them from escalating and jeopardising regional security.

These issues include (i) the loss of human control in using AI in the digital and physical domains, resulting in misperception that could affect international relations, (ii) the need for guardrails to keep up with technological advances and ensure that the use of military AI does not violate international law or the principles of the ASEAN Charter, and (iii) the need to protect the data and digital infrastructure that AI depends on from cybersecurity threats.

ASEAN should follow up on the Joint Statement by ASEAN Defence Ministers on Cooperation in the Field of AI in the Defence Sector, which calls for the development of "collective AI knowledge and capacity, including under the ASEAN Cyber Defence Network (ACDN), ADMM Cybersecurity and Information Centre of Excellence (ACICE) and the ADMM-Plus Experts' Working Group (EWG) on Cybersecurity."

First, ASEAN should explore ways to leverage existing ADMM platforms more effectively to monitor AI risks. Relatedly, the ADMM points of contact, who represent their countries on these platforms, have a crucial role in sharing the discussions and analysis reports produced by these platforms with the relevant departments in their respective defence ministries.

Second, cross-pillar policy-making exchanges on the risks and responsible use of AI could be initiated by ASEAN between ADMM officials, who represent the ASEAN Political-Security Community, and the ASEAN Working Group on AI Governance (WG-AI), which comes under the ASEAN Economic Community.

AI in Areas of Practical Cooperation

Besides monitoring the risks of AI use in warfare, ASEAN militaries could benefit from incorporating AI in non-combat applications that can help promote regional security.

This line of effort was underscored by the aforementioned ASEAN ministers' joint statement that encouraged "ADMM-Plus EWGs to incorporate AI into their works and discussions, where appropriate, to coordinate efforts in leveraging the advantages of AI while proactively addressing its risks and implications."

For example, ADMM-Plus EWG table-top (TTX) and field training (FTX) exercises could incorporate elements of AI. A maritime security exercise could explore the benefits and risks of using AI for enhanced domain awareness and analysing data on vessel behaviour to predict their intent, as well as utilising sea drones as a force multiplier to cover vast areas and counter maritime threats.

Lessons learnt from the exercise could inform efforts to develop confidence-building measures, such as pre-notification of drone deployment near maritime borders, a regional consensus on the minimum level of human oversight, and stress-testing the usefulness of drones in coordinated sea patrols.

Generally, table-top exercises in all areas could benefit from the use of AI to develop scenarios and exercise injects. Additionally, there can be cross-pillar technical exchanges between ADMM officials, who represent their military-cyber units, and the ASEAN Regional Computer Emergency Response Team (CERT), which represents civilian cybersecurity agencies, on cyber threats to AI systems and AI-enabled cyber threats to critical infrastructure essential to military functions.

Conclusion

This paper suggests that analysis of the impact – opportunities and risks – of AI in defence and regional security could encompass the three overarching dimensions of (i) organisational behaviour, (ii) operations, and (iii) strategy. With a deeper understanding of key risk issues pertinent to the ASEAN defence context, ASEAN would be better positioned to leverage existing ADMM platforms or create new initiatives, such as cross-pillar exchanges, to monitor and deepen the understanding of AI risks.

Furthermore, there could be strategic benefits from incorporating elements of AI in non-combat applications such as those under the ADMM-Plus EWGs' areas of practical cooperation. Lessons distilled from these activities could inform efforts to develop confidence-building measures, which are increasingly crucial to ASEAN regional security as more countries adopt AI as part of their defence modernisation.

By thinking of the way forward for regional cooperation on AI in defence, ASEAN could maintain its institutional relevance and demonstrate some agency in a critical area that is increasingly shaped by an AI arms race between powerful states competing for geostrategic superiority.

Muhammad Faizal Bin Abdul Rahman *is a Research Fellow (Regional Security Architecture Programme) with the Institute of Defence and Strategic Studies (IDSS) at the S. Rajaratnam School of International Studies (RSIS), Singapore.*

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.