

AI in Defence: Implications for Southeast Asia Militaries

*Erick Nielson C. Javier**

ABSTRACT

As the employment of military AI makes headlines in conflicts in Europe and the Middle East, Southeast Asian militaries too are showing increasing interest in the technology. This paper investigates the possible rationales and use cases for AI in select Southeast Asian militaries. AI in mission command, surveillance, and select weapons systems, may help meet territorial defence needs, as well as ensure technological relevance, and influence norms for military AI use at the regional level. However, technical, operational and materiel challenges will need to be addressed to fully realize AI's potential for Southeast Asian defence forces, while minimizing potential vulnerabilities.

Keywords: military artificial intelligence, AI in defence, AI in warfare, military uses of AI, Southeast Asia military AI, AI for national defence

Introduction

Up until the mid-2010s, artificial intelligence (AI) was once considered to be the preserve of fiction. However, since the 2020s and with the explosion in popularity of learning language model (LLM) applications such as ChatGPT, Grok, Gemini, Anthropic and DeepSeek, private companies and governments alike are in a rush to incorporate AI in nearly every possible field of human endeavour. AI is everywhere, and warfare is no exception to this.

The application of AI to warfare has been the subject of intense academic and political debate, verging on cliché science-fiction tropes, as seen in many depictions on how AI will supposedly be used to kill all humans, or defend against threats that humans themselves could not prevail against. While the most fantastical visions of militarized AI, in the form of anthropomorphic and human-like “killer robot” characters or god-like intelligences leading enormous machine armies, may yet remain just fiction, there are many more practical uses for AI in warfare that are already being researched and implemented. Lethal autonomous weapon systems (LAWS) are perhaps the most-theorized application, eliciting the most concern from arms control and disarmament advocates. AI and automation more generally are also being investigated for important diagnostics, repair, maintenance, logistics and

*Erick Nielson C Javier is a Defence Research Officer in the Research and Special Studies Division of the National Defense College of the Philippines. His research interests include revolutions in military affairs, deterrence for small states and the future of warfare.

support functions.¹ The use of AIs to provide decision-making and targeting support have also become more controversial, following Israel's alleged use to generate target lists for its war in Gaza.²

While there are many developments and discussions on the use of AI in warfare, these have largely been within the context of great powers such as the United States of America, the Russian Federation, and the People's Republic of China. Despite some studies indicating interests in AI for defence among other Indo-Pacific countries, particularly those in Southeast Asia, there is a dearth of analyses on these states' underlying reasons and objectives. This paper investigates the possible rationales and use cases that would help explain why and how Southeast Asian militaries may try to leverage AI for defence.

For the purposes of this paper, "military AI" is defined as systems used "in operational military activities... directly relating to the planning, preparation and conduct of military operations." This includes AI applications in command and control; intelligence, surveillance and reconnaissance; weapons systems; and cyber and information systems."³ Adopted from a February 2026 paper published by the Stockholm International Peace Research Institute (SIPRI), such a definition excludes other possible applications of AI in the defence establishment, including on human resource management, policy development and health services. This paper also focuses primarily on military AI use at the operational and tactical levels. This is currently where the vast majority of military AI research and deployment occurs; while there are potential uses for the AI at the strategic level,⁴ this paper will not address them.

It should be acknowledged that what systems are considered AI vary considerably: ChatGPT and other popular LLMs are often labelled as generative AI, and are different from systems used specifically for weapons such as assisted aim sights, missile guidance, and fire control. There is some contention as to whether generative AI and other programs classified or marketed as "AI" can truly be

¹ See "AI-Driven Autonomy Revolutionizing Aircraft Inspections", *Lockheed Martin*, 28 March 2024, available at: <https://www.lockheedmartin.com/en-us/news/features/2024/AI-Driven-Autonomy-Revolutionizing-Aircraft-Inspections.html> (all internet references were last accessed July 2026); Akhil Kadidal, "PLAAF deploys AI-assisted refuelling system for YY-20", *Jane's Defence Weekly*, 1 April 2026, available at <https://www.janes.com/defence-intelligence-insights/defence-news/defence/plaaf-deploys-ai-assisted-aerial-refuelling-system-for-yy-20-tanker>.

² Yasmeen Sehran, "How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare", *TIME*, 19 December 2024, available at: <https://time.com/7202584/gaza-ukraine-ai-warfare/>.

³ Netta Goussac and Vincent Boulanin, *Responsible Procurement of Military Artificial Intelligence*, Stockholm International Peace Research Institute, February 2026, p. 2, available at: <https://www.sipri.org/publications/2026/other-publications/responsible-procurement-military-artificial-intelligence>.

⁴ Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, The Hague, 2025, p. 11, available at: <https://hcss.nl/wp-content/uploads/2025/09/GC-REALM-Strategic-Guidance-Report-Final-WEB.pdf>.

classified as "intelligence", due to their limited ability to understand and infer abstract concepts.⁵ For the purposes of this paper's analysis, they will be considered as "AI". As far as is known, all extant applications of AI are not artificial general intelligence (AGI), or strong AIs that can actually replicate human intelligence.⁶

What is and why AI in defence?

Applying direct force

AI in defence is generally considered an enabling technology, rather than a standalone system.⁷ This means that there are many potential real-world applications for AI in defence. In terms of weapon systems specifically intended with AI in mind, LAWS has animated years of high-level discussions under the ambit of the Convention on Certain Conventional Weapons (CCW). In the December 2025 version of the rolling texts of the United Nations Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE-LAWS), LAWS are described as "functionally integrated combinations of one or more weapons and technological components, that can identify, select and engage a target, without intervention by a human operator in the execution of these tasks."⁸ Prior to this, the United States' Department of Defense defined autonomous weapons systems as a "weapon system that, once activated, can select and engage targets without further human intervention by an operator."⁹ The common denominator in these definitions or descriptions is the ability to select and engage targets without intervention by a human. Such systems promise removing ones' own soldiers from risk, and provide reaction times faster than that possible with manual inputs, which may be critical in certain combat scenarios that require above-human reflexes, such as air and missile defence.¹⁰ However, the prospect of giving weapons the ability to decide to take lives, perhaps even without humans supervising or giving orders, is a major operational

⁵ John Nosta, "Can LLMs Think Like Us?", *Psychology Today*, 24 August 2024, available at: <https://www.psychologytoday.com/us/blog/the-digital-self/202408/can-llms-think-like-us>.

⁶ B. Jack Copeland, "Artificial Intelligence", *Britannica*, 02 February 2026, available at: <https://www.britannica.com/technology/artificial-intelligence>.

⁷ N. Goussac and V. Boulanin, above note 3.

⁸ United Nations Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Box I, Item 1, 18 December 2025, available at: [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2026\)/CCW_GGE_LAWS_Rolling_Text_-_status_18_December_2025.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2026)/CCW_GGE_LAWS_Rolling_Text_-_status_18_December_2025.pdf).

⁹ United States Department of Defense Directive 3000.09 – Autonomy in Weapon Systems, 25 January 2023, p. 22, available at <https://media.defense.gov/2023/Jan/25/2003149928/-1/-1/0/DOD-DIRECTIVE-3000.09-AUTONOMY-IN-WEAPON-SYSTEMS.PDF>.

¹⁰ John K. Hawkey, *Patriot Wars: Automation and the Patriot Air and Missile Defense System*, Voices from the Field Research Report, Center for a New American Security, January 2017, p. 4, available at: <https://www.jstor.org/stable/resrep06103?seq=8>.

and ethical issue, and why LAWS garners much concern from futurists, philosophers and legal luminaries.¹¹

Weapon systems do not need to be designed bespoke to be able to make use of AI, as they are now being added as an upgrade or improvement to existing weapons categories without necessarily replacing human operators. The manned F-35 fighter is an example of an existing platform being upgraded with AI; under Project Overwatch, onboard AI will assist pilots in identifying contacts detected by the aircraft's sensors.¹² There are also so-called "smart sights", or assisted optical aiming systems, like the SMASH Handheld developed by the Smart Shooter company, which uses "artificial intelligence, computer vision and machine learning"¹³ in a module that can be attached to any rifle or small arm to improve aim regardless of conditions, greatly improving the effectiveness of soldiers using the system. Another example of a "platform-agnostic" AI, that can be installed on different platforms, is the Hivemind "AI pilot" developed by the Shield AI company, which has flown a variety of aircraft types, from quadcopter drones, larger unmanned air vehicles, to even the F-16, a manned fighter aircraft.¹⁴

Nor is AI's contribution to defence and warfighting limited to being part of weapons. AI and automation could be conceivably applied to any of the following major warfighting functions: mission command, movement and manoeuvre, intelligence gathering and processing, fires, sustainment, and protection.¹⁵ Each function encompasses multiple tasks, not all of which require direct application of force. Such activities that do not directly involve target selection, target engagement and direct application of military force, are also known as "upstream" military tasks.¹⁶ There are different desirable levels of autonomy corresponding to the specific taskings required, with particular emphasis on whether it is computationally

¹¹ William Boothby, "Dehumanization: Is There a Legal Problem Under Article 36?", in Wolff Heinschel von Heinegg, Robert Frau and Tassilo Singer (eds), *Dehumanization of Warfare – Legal Implications of New Weapons Technologies*, Springer International Publishing AG, Cham, 2018, pp. 21-51; Netta Goussac, "Safety net or tangled web: Legal reviews of AI in weapons and war-fighting", *Humanitarian Law and Policy*, 18 April 2018, available at: <https://blogs.icrc.org/law-and-policy/2019/04/18/safety-net-tangled-web-legal-reviews-ai-weapons-war-fighting/>.

¹² Sydney J. Freedberg, "Lockheed test-flies F-35 with artificial intelligence to quickly ID unknown contacts", *Breaking Defense*, 26 February 2026, available at: <https://breakingdefense.com/2026/02/lockheed-test-flies-f-35-with-artificial-intelligence-to-quickly-id-unknown-contacts/>.

¹³ "About", *Smart Shooter*, 2026, available at: <https://www.smart-shooter.com/about-smart-shooter/>.

¹⁴ Colin Demarest, "Shield AI to let Hivemind software fly three more aircraft", *DefenseNews*, 9 April 2024, available at: <https://www.defensenews.com/artificial-intelligence/2024/04/08/shield-ai-to-let-hivemind-software-fly-three-more-aircraft/>.

¹⁵ Thomas Ryan and Vikram Mittal, "Potential for Army Integration of Autonomous Systems by Warfighting Function", *Military Review*, Vol. 99, No. 5, September-October 2019, p. 123.

¹⁶ Sarah Grand-Clément, *Artificial Intelligence Beyond Weapons - Application and Impact of AI in the Military Domain*, UN Institute for Disarmament Research, Geneva, 2023, p. 10, available at: https://undir.org/wp-content/uploads/2023/10/UNIDIR_AI_Beyond_Weapons_Application_Impact_AI_in_the_Military_Domain.pdf.

expansive and taxing on mental endurance.¹⁷ The intelligence, sustainment and protection warfighting functions were deemed to be the largest beneficiaries of increased application of autonomous systems¹⁸, as these functions normally need large numbers of personnel and high responsiveness which could be more seamlessly provided via autonomous systems.

The impact of using AI for intelligence can be seen in the Israeli use of AI as decision support systems (DSS) for its operation during the war in Gaza.¹⁹ Examples include *Habsora* (Gospel), which was allegedly employed from 2023-onward,²⁰ and Lavender, which began to appear in reports from March-April 2024.²¹ These systems aggregate and analyse data from multiple information streams to identify and recommend potential targets to human analysts, who then pass the information directly to combat commanders in the field. *Habsora*, Lavender, and other companion AI have allowed the rapid generation of tens of thousands of targets for Israeli strikes during the Gaza war, up to fifty (50) times faster²² than could be possible with teams of human intelligence analysts.

The data used to generate these targets, while not publicly confirmed, are generally assumed to include image intelligence (IMINT) data from satellites and drones, and electronic and radio data from other sources such as smartphone messages, phone calls and video feeds.²³ The sheer volume and variety of data gathered is so expansive that it could actually hobble a military's ability to gain actionable insights from such data, making AI necessary to parse through the information.²⁴ While Israeli AIs enable the rapid identification of valid military targets such as missile launchers and arms, the large-scale civilian casualties from the attacks, which were supposedly recommended by Israeli AI DSS, have triggered questions on the exact parameters that Israeli AI use to classify targets. As AI depend

¹⁷ T. Ryan and V. Mittal, above note 15, p. 124.

¹⁸ T. Ryan and V. Mittal, above note 15, p. 133.

¹⁹ Marta Bo and Jessica Dorsey, "Symposium on Military AI and the Law of Armed Conflict: The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians", *OpinioJuris*, 4 April 2024, available at: <https://opiniojuris.org/2024/04/04/symposium-on-military-ai-and-the-law-of-armed-conflict-the-need-for-speed-the-cost-of-unregulated-ai-decision-support-systems-to-civilians/>.

²⁰ Duval Abraham, "'A mass assassination factory': Inside Israel's calculated bombing of Gaza", *+972 Magazine*, 30 November 2025, available at: <https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/>.

²¹ Vinay Patel, "Israeli AI Technology Used to Identify 37,000 Hamas Targets", *International Business Times*, 4 April 2024, available at: <https://www.ibtimes.co.uk/israeli-ai-technology-used-identify-37000-hamas-targets-1724204>.

²² D. Abraham, above note 20.

²³ Anwar Mhaje, "Regulating Military AI: Gaza and Beyond", *Survival*, Vol. 68, No. 2, May 2026, p. 26.

²⁴ Noah Sylvia, *The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose*, Royal United Services Institute, London, 04 July 2024, available at: <https://www.rusi.org/explore-our-research/publications/commentary/israel-defense-forces-use-ai-gaza-case-misplaced-purpose>.

heavily on the quality of training data used to identify patterns, fears have surfaced²⁵ that the targeting metrics may be based on biased variables that have no direct bearing on whether the target in question is a legitimate member of the adversary organization, let alone combatants.

Speed in decision-making

The desire for fast reaction across the various warfighting functions follows from preexisting trends for more automated weapon systems that progressively reduce the numbers of humans needed for functions such as loading and maintenance. A similar rationale inspires the implementation of AI in upstream military tasks outside of weapons systems, especially in intelligence gathering and processing algorithms that improve the speed of threat detection, prioritization and decision-making for command and control. This is part of a long-standing desire to enhance a military's observe-orient-decide and act (OODA) loop. First coined by US Air Force Colonel John Boyd, it is a type of action-learning cycle²⁶ that asserts that the faster one can observe, orient, decide then act compared to their adversaries – “getting inside the enemy's OODA loop” – the better the chances of winning. Superior decision-making speed will help a military react faster than their adversaries, allowing them to gain or retake initiative and maintain pressure until the enemy capitulates and is defeated.

Great powers lead the way

This “need for speed” is clearly seen in the United States' Artificial Intelligence Strategy, published by the Department of Defense (or Department of War) on January 2026, which stated that “[w]e must weaponize learning speed, and measure and manage cycle time and adoption rates as decisive variables in the AI era.”²⁷ This builds on earlier US policies on incorporating AI into defence as part of the Third Offset Strategy²⁸, which highlighted how emerging technologies can be used to offset the growing conventional and asymmetric capabilities of both state competitors and non-state adversaries. To this end, the United States works extensively to implement AI tools across the armed forces, from dedicated platforms such as the Collaborative

²⁵ Geoff Brumfiel, “Israel is using an AI system to find targets in Gaza. Experts say it's just the start”, *National Public Radio*, 14 December 2023, available at: <https://web.archive.org/web/20240220015604/https://www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-targets-in-gaza-experts-say-its-just-the-st>.

²⁶ Brett Crowley, “The OODA Loop”, *The Decision Lab*, 2025, available at: <https://thedecisionlab.com/reference-guide/computer-science/the-ooda-loop>.

²⁷ United States Department of War Artificial Intelligence Strategy, 9 January 2026, p. 4, available at: <https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF>.

²⁸ United States Department of Defense, “The Third U.S. Offset Strategy and its Implications for Partners and Allies”, 28 January 2015, available at: <https://www.defense.gov/News/Speeches/Speech/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/>.

Combat Aircraft (CCA) programs of the US Air Force²⁹, to backfitted solutions to improve the readiness and capability of existing military forces such as Project Overwatch and SMASH Handheld mentioned earlier. The 2026 AI Strategy called for further integration of AI systems in the US military's upstream tasks, exemplified in the development and deployment of the Maven Smart System. Developed under Project Maven, it is an expansive data analysis and decision-making software that is intended to be able to fuse data from a variety of sources and interoperate with other US systems.³⁰ The Maven Smart System has already seen wide use in strike planning, notably during the US-Israeli air campaign against Iran, which began on 28 February 2026.³¹

For the People's Republic of China and its People's Liberation Army, their drive to AI in defence is seen in its concepts of fighting "informatized local wars", wherein information is considered a key domain of warfare and one of, if not the, central means to wage conflict³² in the modern era. Indeed, PLA strategic writings emphasize information sources, quality of collection and circulation speed among other variables to "seek decision-making advantages with information advantages".³³ China recognizes the importance of developing AI among other cutting-edge technologies for military advantage, as stated in its 2019 Defence White Paper.³⁴ Incorporating these cutting-edge technologies is key to PLA modernization, representing the third of a three-phase program of "mechanization, informatization and intelligentization".³⁵ To meet these targets, Chinese developers have demonstrated an array of AI-enabled technologies, from Norinco's Intelligent Precision Strike System that uses AI to deploy and control multiple drones to find

²⁹ Jennifer DiMascio, *US Air Force Collaborative Combat Aircraft*, Congressional Research Service, 28 November 2025, p. 1, para. 1, available at: <https://www.congress.gov/crs-product/IF12740>.

³⁰ Courtney Albon, "Palantir wins contract to expand access to Project Maven AI tools", *DefenseNews*, 31 May 2024, available at: <https://www.defensenews.com/artificial-intelligence/2024/05/30/palantir-wins-contract-to-expand-access-to-project-maven-ai-tools/>.

³¹ Sydney J. Freedman, "'Insatiable appetite' for AI: Maven usage surged for strikes on Iran, Pentagon AI chief says", *Breaking Defense*, 12 May 2026, available at: <https://breakingdefense.com/2026/05/insatiable-appetite-for-ai-maven-usage-surged-for-strikes-on-iran-pentagon-ai-chief-says/>.

³² Edmund J. Burke *et al.*, *People's Liberation Army Operational Concepts*, RAND Corporation, 2020, p. 5, available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf.

³³ Xiao Tianliang *et al.*, "Chapter 13 - Operational Guidance", *Science of Military Strategy*, National Defense University Press, Beijing 2020, p. 227. Translation available at: <https://www.airuniversity.af.edu/CASI/Display/Article/2913216/in-their-own-words-2020-science-of-military-strategy/>.

³⁴ State Council of the People's Republic of China White Paper on China's National Defense in the New Era, 24 July 2019, pp. 6-7, available at: <https://english.www.gov.cn/atts/stream/files/5d3943eec6d0a15c923d2036>.

³⁵ Josh Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield", *Cyber Defense Review*, US Army Cyber Institute, West Point, 16 December 2024, p. 30, available at: <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4012231/the-path-to-chinas-intelligentized-warfare-converging-on-the-metaverse-battlefi/>.

targets and devise and execute attacks, AI-enabled synthetic brigades that combine AI with multiple manned and unmanned platforms, and proprietary operational decision support, intelligence repository and battlefield intelligence systems, meant to showcase China’s growing capabilities in the military AI domain.³⁶

As both the United States and China are considered the leaders in military AI and its applications, and are currently locked in an intense geopolitical competition, it is very likely that this drive for speeds and wide applicability will inform other militaries’ efforts to adopt AI.

ASEAN and AI in defence

States’ efforts to incorporate military AI

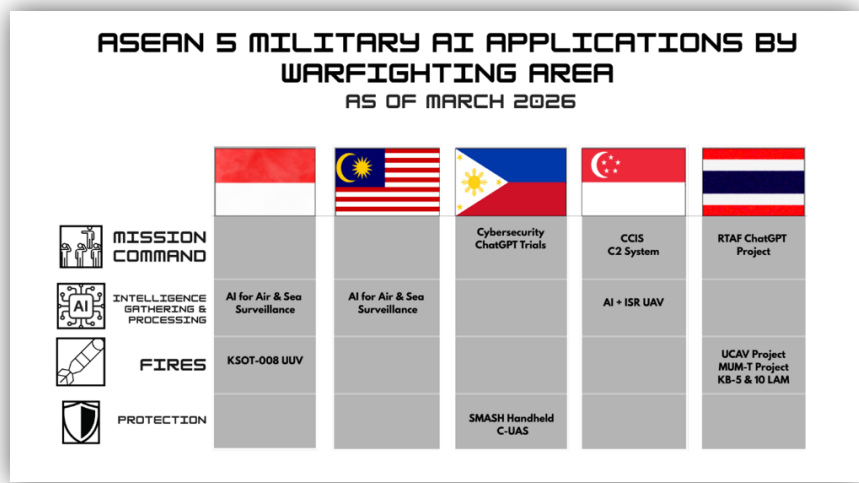


Figure 1. ASEAN 5 Military AI Applications by Warfighting Area as of March 2026
Source: Author’s illustration

The implications for AI in defence have not been lost in the Southeast Asian region. Individual Southeast Asian states have already begun investigating the potential uses of AI in defence for several years prior. Singapore has been leading the way among its peers, in keeping with its established practices of maintaining strong defence

³⁶ Tye Graham and Peter W. Singer, “New Products Show China’s Quest to Automate Battle”, *Defense One*, 2 March 2025, available at: <https://www.defenseone.com/threats/2025/03/new-products-show-chinas-quest-automate-battle/403387/>.

capabilities.³⁷ The Singapore Armed Forces (SAF) was among the first ASEAN member militaries to begin testing applications of AI in mission command, using a command and control information system (CCIS) fitted with AI in the Forging Sabre series of military exercises with the United States since 2021.³⁸ In 2022, it formed the Digital and Intelligence Service (DIS), effectively a fourth branch of the SAF, whose tasks include optimizing the application of AI across the entire spectrum of the SAF's operations.³⁹ In early 2026, SAF began testing unmanned aerial vehicles (UAV) integrated with Shield AI's Hivemind SDK AI system, ostensibly for intelligence and surveillance missions.⁴⁰

The Indonesian Ministry of Defence announced in 2024 that it would cautiously explore adopting AI systems, particularly for "securing airspace", although they acknowledged that the technology was far from reliable⁴¹; the Indonesian Air Force in particular pushing for the technology's adoption. The Indonesian Navy have begun testing KSOT-008 torpedo-armed AI-powered autonomous underwater vehicles in October 2025,⁴² as part of Indonesia's drive for self-reliance and their ongoing naval modernization.

The Malaysian Ministry of Defence, in its mid-term review of its 2019 Defence White Paper, highlights the need to acquire the latest technologies, such as AI tools.⁴³ The Malaysian Armed Forces have apparently already begun doing so, stating in parliamentary inquiries that they have been integrating AI tools for surveillance in land, air and sea domains, as well as using AI-assisted training

³⁷ Daniel Lu, *Poison Shrimp: Deterrence, Defense Cooperation, and Total Defense from Europe and Asia*, Naval Postgraduate School, December 2020, p. 29, available at: <https://calhoun.nps.edu/server/api/core/bitstreams/c13d876a-7df8-4cbb-a919-c25f7461fa11/content>.

³⁸ Aqil Hamzah, "AI, data analytics improve decision-making process, but human touch still key at SAF exercise", *Straits Times*, 22 September 2023, available at: <https://www.straitstimes.com/singapore/ai-data-analytics-improve-decision-making-process-but-human-touch-still-key-at-saf-exercise>.

³⁹ Ministry of Defence of the Republic of Singapore, "Remarks By Minister For Defence Dr Ng Eng Hen at the Aspen Strategy Group and Amazon Web Services Roundtable On 'Allied Artificial Intelligence: Strengthening The Technological Edge'", 14 February 2025, available at: https://www.mindef.gov.sg/news-and-events/latest-releases/15feb25_speech_2/.

⁴⁰ Oishee Majumdar, "Singapore tests UAV equipped with Shield AI software", *Janes Defence Weekly*, 06 March 2026.

⁴¹ Walda Marison and Resinta Sulistiyandari, "Indonesia to cautiously adopt AI in defense by 2025", *Antara Indonesian News Agency*, 19 December 2024, available at: <https://en.antaranews.com/news/338622/indonesia-to-cautiously-adopt-ai-in-defense-by-2025>.

⁴² Akhsan Erido Elezhar, "Indonesia Debuts AI-Powered Autonomous Submarine Armed With Six Torpedoes", *The Defense Post*, 10 October 2025, available at: <https://thedefensepost.com/2025/10/10/indonesia-ai-submarine-torpedoes/>.

⁴³ Adam Leong Kok Wey, "Malaysia's Defense White Paper Midterm Review: Emerging AI-Enabled Security Threats", *The Diplomat*, 23 September 2025, available at: <https://thediplomat.com/2025/09/malysias-defense-white-paper-midterm-review-emerging-ai-enabled-security-threats/>.

simulators and logistics systems.⁴⁴ There also seem to be intentions to implement “AI-enabled military drones, enhanced cyber defence and smart weapon automation.”⁴⁵

The Philippines, in its National Security Policy 2023-2028, stated that they would “innovate and modernize maritime, air, and space systems and security operations through the use of space science and technology applications, and integration of AI.”⁴⁶ The Philippine Department of National Defense acknowledged the threat posed by AI systems used by their adversaries,⁴⁷ which was evidenced in the release of an internal memorandum banning the use of AI image generator apps which were seen as potential vectors for data breaches and data gathering for deepfake operations.⁴⁸ The Armed Forces of the Philippines (AFP) are studying the potential uses of AI in defence, including trial applications of systems like ChatGPT,⁴⁹ and have procured some AI-powered systems such as the SMASH Handheld rifle sight for counter-unmanned aerial system (C-UAS) work, which debuted publicly⁵⁰ during the 2025 *Balikatan* Exercises between the AFP and the United States Armed Forces.

The Royal Thai Air Force (RTAF) in its 2024 Defence White Paper outlined plans to develop AI – specifically an RTAF equivalent of ChatGPT, beginning in 2028.⁵¹ Such an initiative is intended to help the RTAF in its ambitions to be a future-ready air force in the region, and is in line with other Thai military research that investigated the potential uses of generative AI for defence tasks.⁵² The 2024 White Paper also indicated RTAF initiatives to develop unmanned combat air vehicles (UCAV), tactical UAVs, and manned-unmanned teaming (MUM-T) as part of the force’s future expansion and modernization.⁵³

⁴⁴ Nurnabihah Dini, “Malaysia advances smart military transition with new cyber, AI capabilities”, *The Malaysian Reserve*, 19 November 2025, available at: <https://themalaysianreserve.com/2025/11/19/malaysia-advances-smart-military-transition-with-new-cyber-ai-capabilities/>.

⁴⁵ *Id.*

⁴⁶ National Security Policy 2023-2028, National Security Council of the Philippines, p. 20.

⁴⁷ JV Ordonez, “Why The DND Wants a Revamped Military Modernization Plan”, *Esquire Magazine*, 31 July 2025, available at: <https://www.esquiremag.ph/politics/news/dnd-seeks-revamped-modernization-plan-to-counter-cyberthreats-a8072-20250731>.

⁴⁸ Erick Nielson C Javier, “Artificial intelligence threat makes data protection priority for Philippine military”, *East Asia Forum*, 3 July 2024, available at: <https://easiaforum.org/2024/07/03/artificial-intelligence-threat-makes-data-protection-priority-for-philippine-military/>.

⁴⁹ Jekki Pascual, “AFP studying use of AI for defense”, *ABS-CBN News*, 17 January 2025, available at: <https://www.abs-cbn.com/news/technology/2025/1/17/afp-studying-use-of-ai-for-defense-1553>.

⁵⁰ Pia Lee-Brago, “Modern weapon systems showcased at Balikatan drills”, *Philstar Global*, 05 May 2025, available at: <https://www.philstar.com/headlines/2025/05/05/2440569/modern-weapon-systems-showcased-balikatan-drills>.

⁵¹ Royal Thai Air Force (RTAF) Defence White Paper 2024, pp. 31 and 74.

⁵² Kanok Bunnag, “Generative Artificial Intelligence and its Military Application”, *Defence Technology Academic Journal*, Vol. 6, No. 13, pp. 28–41, May 2024.

⁵³ RTAF, above note 51, pp. 46–48.

The above is not an exhaustive review of these Southeast Asian states' official statements or forays into military AI applications. Nor is it meant to be a review of all ASEAN military AI capabilities, as efforts from Brunei, Cambodia, Laos, Myanmar, Timor Leste and Vietnam have yet to be reliably documented in the open media. It should be sufficient to illustrate the real interest and efforts of states in the region to harness the technology for their defence and security.

ASEAN tackles AI

In addition to individual member states, AI in defence has increasingly gained the attention of ASEAN as a collective. Interest in the topic could be evidenced as early as 2021, with Track II⁵⁴ discussions on the impacts of AI and unmanned systems to defence and security for the Southeast Asian region.⁵⁵ This was followed by a Track II workshop held in 2025 focused on AI in defence. In February 2025, the ASEAN Defence Ministers Meeting (ADMM) released the Joint Statement by the ASEAN Defence Ministers' Meeting on Cooperation in the Field of the Defence Sector,⁵⁶ marking the first regional statement specifically on the issue of AI in defence.

Prior to ADMM and Track II discussions on ASEAN, the organization released the ASEAN Guide to AI Governance and Ethics in 2024. The guide skirted the issue of military AI, as it was intended to be a "practical guide for organizations in the region that wish to design, develop and deploy traditional AI technologies in commercial and non-military or dual-use applications."⁵⁷ An ASEAN Working Group on AI Governance was thereafter also established.

⁵⁴ Founded in 2007, the Network of ASEAN Defence and Security Institutions (NADI) is a Track II network of ASEAN defence academic institutions that also serve as think-tanks. While not encompassing the totality of ASEAN's defence intelligentsia and think-tank population, its status as a recognized Track II platform that directly forwards information and recommendations to the ASEAN Defence Ministers' Meeting (ADMM) gives it some weight in representing views of these states' defence establishments with regard to thinking about AI in defence, even if some of the ASEAN states have not yet publicly disclosed specific defence AI programmes or experiments.

⁵⁵ Chairman's Report of the Track II NADI Workshop on Emerging Technologies and Its Impacts to Defence and Security, 29-30 September 2021, available at: https://www.rsis.edu.sg/nadi/pdfs/emgtech_1/Chairman_Report.pdf.

⁵⁶ Joint Statement of the ASEAN Defence Ministers on Cooperation in the Field of Artificial Intelligence in the Defence Sector, 26 February 2025, available at: <https://asean.org/wp-content/uploads/2025/02/JS-ON-COOPERATION-IN-THE-FIELD-OF-AI-IN-THE-DEFENCE-SECTOR.pdf>.

⁵⁷ ASEAN Guide on AI Governance and Ethics, February 2024, p. 3, available at: https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf.

Analysis of ASEAN's interest in AI

Following trends and meeting threats

Southeast Asian views on AI in defence seem to largely follow global discussions on the technology. They generally acknowledge AI's potential to increase speed and efficiency in defence and security, as well as the ethical risks. There is some perception among ASEAN member states that AI will be useful for not just warfighting, but for non-combat military tasks such as humanitarian assistance and disaster response (HADR), as well as general surveillance. At least one Southeast Asian state sees AI as useful in supplementing military anti-corruption practices,⁵⁸ which while important, do not neatly fall in any of a military's warfighting functions. For another ASEAN member state, the importance placed on AI was not matched with substantive discussion on what its warfighting applications would be.⁵⁹

Examining some of the stated rationales from ASEAN government officials, a case could also be made that the interest of Southeast Asian states to incorporate AI in defence is as much about ensuring they are not left out in the discussion and exploitation of this technology. Statements in both Track I⁶⁰ and Track II⁶¹ defence discussions within ASEAN generally echo the perception of AI being an ubiquitous technology that is being harnessed everywhere, therefore individual member states and indeed ASEAN as a whole must have access to the technology too. There is general sentiment among ASEAN members that "halting AI is not an option, and instead, ASEAN must learn to adapt while addressing disparities in AI capacities across the region."⁶²

In addition to access to the technology, some ASEAN states have exerted active efforts to influence the shaping of international regulations on military AI. Lao PDR, the Philippines and Singapore participate in the GGE-LAWS discussions,

⁵⁸ Bernama, "Mindef to leverage AI, digital tech to tackle corruption in armed forces", *New Straits Times*, 31 January 2026, available at: <https://www.nst.com.my/news/nation/2026/01/1368695/mindef-leverage-ai-digital-tech-tackle-corruption-armed-forces>.

⁵⁹ Kuik Cheng-Chwee, *Malaysia Reassesses Security: The Mid-Term Review of the Malaysian Defence White Paper*, Perspective Issue No. 11-2026, ISEAS-Yusof Ishak Institute, Singapore, p. 4, available at: https://www.iseas.edu.sg/wp-content/uploads/2026/01/ISEAS-Perspective_2026_11.pdf.

⁶⁰ Joint Statement of the ADMM on Cooperation in the Field of Artificial Intelligence in the Defence Sector, p. 2, available at: <https://asean.org/wp-content/uploads/2025/02/JS-ON-COOPERATION-IN-THE-FIELD-OF-AI-IN-THE-DEFENCE-SECTOR.pdf>.

⁶¹ Chairman's Report of the Track II NADI Meeting on The Emerging Security Architecture in Asia-Pacific, Assessment of Implications, and Recommendations for ASEAN, 18-21 September 2024, p. 1, available at: https://www.rsis.edu.sg/nadi/pdfs/ESAAPAIR_1/ChairmanReport.pdf.

⁶² Chairman's Report of the Track II NADI Meeting on Artificial Intelligence (AI) in Defence: Potential and Challenges for ADMM Cooperation, 26-29 August 2025, p. 10, available at https://www.rsis.edu.sg/nadi/pdfs/Alid_1/ChairmanReport.pdf.

while Thailand is an observer.⁶³ The Philippines co-endorsed a draft protocol VI for the CCW in the 2022 sessions of GGE-LAWS,⁶⁴ and also organized the Manila Meeting on Indo-Pacific Perspectives on Autonomous Weapon Systems on 13-14 December 2023.⁶⁵ Singapore co-hosted the Responsible AI in the Military Domain (REAIM) Regional Consultations for Asia on 26-27 February 2024.⁶⁶

By contrast to their official views on AI in defence, concrete defence acquisitions of AI-enabled systems can be more broadly seen as a reflection of specific states' threat perceptions and interests. As summed up in Figure 1 above, several ASEAN states seek the technology to enhance their capabilities for enhanced mission command, intelligence and surveillance, protection and fires capabilities. These seem to be geared toward meeting territorial defence challenges: the Philippines is embroiled in intense maritime and territorial disputes with China over features and maritime jurisdictions in the South China Sea (SCS) and is sensitive to both overt military and non-military coercive measures, including attempts to steal its data. Malaysia also has maritime and territorial claims in the SCS. While not directly affected by the disputes, Indonesia and Singapore are affected by tensions in the SCS, harbour growing concerns on the regional balance, and have critical and/or expansive waterways and airspace to monitor and protect. Thailand's drive to defence capability development may be influenced by a general need to maintain defence capacity, which was subsequently proven given the resumption of a long-running border conflict with Cambodia throughout 2025.

However, the piecemeal implementation of AI among Southeast Asian militaries, and in mostly niche capabilities compared to the expansive programs of the United States and China, demonstrates differences in doctrinal focus and approach, in addition to more familiar issues of funding, and the abovementioned perceived need for caution and further study expressed in Track II fora and the ADMM Joint Statement on AI in the Defence Sector.

⁶³ List of Participants, Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, 10 September 2025, available at [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2025\)/CCW-GGE.1-2025-INF.1.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2025)/CCW-GGE.1-2025-INF.1.pdf).

⁶⁴ Draft Protocol VI Submitted by Argentina, Ecuador, Costa Rica, El Salvador, Guatemala, Kazakhstan, Nigeria, Panama, the Philippines, Sierra Leone and Uruguay, 9 August 2022, available at [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_\(2022\)/CCW-GGE.1-2022-WP.8.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_(2022)/CCW-GGE.1-2022-WP.8.pdf).

⁶⁵ Inputs from the Philippines, United Nations Secretary General Report on Resolution 78/241 (Lethal autonomous weapon systems), 17 May 2024, p. 1, available at: [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-241-Philippines-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-241-Philippines-EN.pdf).

⁶⁶ Singapore's National Submission on the Topic of Lethal Autonomous Weapon Systems, 9 May 2024, p. 3, available at: [https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_\(2024\)/78-241-Singapore-EN.pdf](https://docs-library.unoda.org/General_Assembly_First_Committee_-_Seventy-Ninth_session_(2024)/78-241-Singapore-EN.pdf).

Challenges for ASEAN states' adoption of AI

A careful reading of the ADMM Joint Statement may indicate that ADMM's understanding of AI remains largely cybersecurity focused, evident by their intention to develop knowledge and capacities for cooperation on AI under the ambit of ASEAN's cybersecurity platforms.⁶⁷ This, as well as the abovementioned interest in non-warfighting applications of AI in defence, may be explained by ADMM's general reticence to discuss military hardware and platforms (which would include autonomous systems such as LAWS). This is perhaps in keeping with ASEAN norms on non-interference in members' affairs⁶⁸, considering that the subject of procurements could quickly become sensitive issues due to the still extant territorial disputes between members.

It should also be noted that while ADMM has a growing portfolio of defence cooperation initiatives; ASEAN itself is not a security alliance in the same way as the North Atlantic Treaty Organization (NATO). Its members are unlikely to form such a similar defence pact due to divergent defence and security interests, as acknowledged publicly by at least one ASEAN member state's defence secretary.⁶⁹ This is before taking into account actual conflict between member states, as exemplified most recently by the Cambodia-Thailand border clashes. By comparison, ADMM have had extensive discussions on cybersecurity and cyber defence, established an Expert Working Group (EWG) on Cyber Security in 2017, the ADMM Cybersecurity and Information Centre of Excellence (ACICE) and the ASEAN Cyber Defence Network in 2021.⁷⁰

Using cybersecurity as a base for AI cooperation may be valuable in protecting generative AI and LLMs, especially if the AI and their databases are locally hosted. Local hosting and isolating the training databases would help reduce cyber risks,⁷¹ compared to just using models and databases with regular access to the open internet, which may open them to the risk of incorporating disinformation that can negatively impact the assessments AIs provide.⁷²

⁶⁷ ADMM, above note 60, p. 3.

⁶⁸ Treaty of Amity and Cooperation in Southeast Asia, 24 February 1976, Art. II.

⁶⁹ Martin Sadongdong, "Is ASEAN ready to have a NATO-like counterpart? 'Not possible at this time', says Teodoro", *Manila Bulletin*, 5 November 2024, available at: <https://mb.com.ph/2024/11/5/asean-nato-counterpart-teodoro>.

⁷⁰ ASEAN Cybersecurity and Information Centre of Excellence Update on The Cyber Domain, March 2025, p. 5 available at: https://www.acice-asean.org/files/cybersecurity%20centre%20reports/mar25_cyber.pdf.

⁷¹ Daniel Anderson, "How to Run AI Locally: Benefits, Challenges, and Solutions", *Autonomous*, 29 July 2025, available at: <https://www.autonomous.ai/ourblog/run-ai-locally>.

⁷² Mackenzie Sadeghi, "Top 10 Generative AI Models Mimic Russian Disinformation Claims A Third of the Time, Citing Moscow-Created Fake Local News Sites as Authoritative Sources", *NewsGuard*, 18 June 2024, available at: <https://www.newsguardtech.com/special-reports/generative-ai-models-mimic-russian-disinformation-cite-fake-news/>.

Protecting networks is essential to effective use of AI LLMs especially if these systems will be used to inform operational planning and ultimately targeting decisions, akin to Israel's *Habsora* and the United States' Maven. The reliability of current AI applications for operational planning is debatable even without the risk of data tampering or flooding of malicious data, due to the likelihood that an AI's training database may have plenty of information on what constitutes targets, but not enough information on what does not constitute targets, as was reportedly found out in initial Israeli trials of what would become *Habsora* in 2021.⁷³

Cybersecurity and data protection may be even more paramount if off-the-shelf commercial AI models are used for such purposes. Costs could be reduced by the adoption of these commercial models for intelligence consolidation, analysis and assistance to mission command, in comparison to having to devise bespoke models suitable for Southeast Asian states' needs, and this is a tempting prospect due to the general need for Southeast Asian states to balance their defence spending with other development priorities. However, relying on off-the-shelf models come with their own risks. In general, commercial AI LLM models pose an inherent level of data security risk, due to their dependence on databases maintained on the open web, and usually in data centres that may not be within the user states' borders.

There is also the basic issue of digital sovereignty; the leading LLM models are either developed by firms in the United States or China,⁷⁴ which opens up concerns regarding data security and control. Some companies, such as Anthropic, have expressed concerns, if not total opposition, to certain military uses of their Claude AI, which may have been used in assisting the planning of Operation Absolute Resolve that led to the United States' capture of Venezuelan president Nicolas Maduro in January 2026.⁷⁵ Regardless of where one stands on Anthropic's position, a private firm deciding on what uses are permissible for its AI will likely influence some states' decisions to use their services. That same AI was also recently the subject of a major cyber-attack, where hackers of alleged Chinese origins were able to subvert Claude to conduct cyber-attacks on a number of corporations and government bodies,⁷⁶ reinforcing the security risks of using commercial AI.

Finally, there is the need to minimize the data potentially accessible to outsider and adversary AI; the Philippine 2023 internal memo banning use of certain

⁷³ Jewish Institute for the National Security of America, *Gaza Conflict 2021 Assessment: Observations and Lessons*, Washington D.C., October 2021, p. 31, available at: <https://jinsa.org/wp-content/uploads/2021/10/Gaza-Assessment.v8-1.pdf>.

⁷⁴ "AI Leaderboards", *LLMStats*, 11 March 2026, available at: <https://llm-stats.com>.

⁷⁵ Paulo Carvão, "Should AI Go To War? Anthropic And The Pentagon Fight It Out", *Forbes*, 20 February 2026, available at: <https://www.forbes.com/sites/paulocarvao/2026/02/20/should-ai-go-to-war-anthropic-and-the-pentagon-fight-it-out/>.

⁷⁶ David Klepper and Matt O'Brien, "Anthropic warns of AI-driven hacking campaign linked to China", *Associated Press*, 15 November 2025, available at: <https://apnews.com/article/ai-cyber-china-hacking-artificial-intelligence-anthropic-4e7e5b1a7df946169c72c1df58f90295>.

AI apps is one example of a countermeasure intended to deny or at least hobble potential sources of sensitive personal information for adversaries.

Limitations of AI: not a panacea for lack in military capability

To what extent AI can grant advantages to smaller states which are not necessarily leaders in the technology, or lack the necessary infrastructure to fully realize aspirations of a self-reliant or independent system? While AI is a disruptive technology that could grant asymmetric advantages for states that invest in them, there is the distinct possibility that AI by itself will not be sufficient to gain reverse asymmetry⁷⁷ for small states, wherein the smaller state aims to leverage military innovation to overcome larger opponents. This is due to the reality that great powers not only have more resources than smaller states, but are also often technology leaders with first-mover advantages and at least a temporary monopoly over new military technologies.⁷⁸

For AI to be able to help a state win, that state will still need sufficient quantities of everything from munitions to sensors, (region-specific) training data, secure supply chains and motivated and trained soldiers. This can be seen in the ongoing Russian invasion of Ukraine; while the adoption of unmanned systems is moving rapidly in Ukraine's armed forces, including successful field tests of a variety of unmanned systems⁷⁹, the outcome of the war remains uncertain, in part due to the Russians' own adaptability and still-significant conventional and numerical preponderance. Even as emerging technologies are implemented, war is ultimately still a contest of wills⁸⁰ and attrition in materiel and lives. This is made worse by the fact that, unlike most other technologies identified as providing asymmetric advantage such as drones, AI is not necessarily cheap to invest in⁸¹, requiring substantial investments in data centre infrastructure. Quite apart from the up-front capital costs, AI data centre infrastructure will likely pose additional strains on scarce

⁷⁷ Michael Raska, "Chapter 3 - Creating a reverse asymmetry: military innovation concepts, issues and debates in the IDF", in *Military Innovation in Small States: Creating a reverse asymmetry*, Routledge, London & New York, 2016, p. 91.

⁷⁸ Francis Domingo, "Distribution of Power and Cyber Capability Development", in *Making Sense of Cyber Capabilities for Small States: Case Studies from the Asia-Pacific*, Routledge, London, 2022, p. 96.

⁷⁹ Andrew White, "Why Ukraine's all-drone, multi-domain attack could be a 'seminal' moment in warfare", *Breaking Defense*, 24 January 2025, available at: <https://breakingdefense.com/2025/01/why-ukraines-all-drone-multi-domain-attack-could-be-a-seminal-moment-in-warfare/>.

⁸⁰ Michael Raska and Richard A. Bitzinger, "Introduction: The AI Wave in Defence Innovation", in *The AI Wave in Defence Innovation - Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*, Routledge, London & New York, 2023, p. 9.

⁸¹ National Defense College of the Philippines, "Defense industrial ecosystem dev't highlighted in first Security Lounge for 2026", 27 February 2026, available at: <https://ndcp.edu.ph/defense-industrial-ecosystem-devt-highlighted-in-first-security-lounge-for-2026/>.

water and energy resources,⁸² which are already major concerns for several Southeast Asian states.

Expectations that AI can give asymmetric advantage must be weighed against the physical and material readiness of Southeast Asian military forces. It should be noted that even as they are modernizing their forces, they still do not yet have the preponderance of force to achieve their desired force objectives, such as establishing an anti-access/area-denial (A2/AD) network.⁸³

Ways Forward

AI in defence is still very much an evolving and growing area of development and study. Even as militaries seek the speed and efficiency that AI promises, there is reason for a more cautious approach. The alleged impact of decision-support AI in Gaza points to the potential collateral damage and casualties that could happen if speed of generating targets is prioritized above all other considerations.⁸⁴

As the decision to attack still ultimately lies with the analysts and commanders who recommend and make the decisions to attack, this implies that future use of such decision-support AIs must be coupled with increased training requirements for future operators,⁸⁵ aiming to increase awareness of the essential principles on the law of armed conflict (LOAC) and international humanitarian law (IHL). While unlikely to be foolproof, it must be ensured that the officers that sign off on AI-recommended attack orders know clearly the risks of blindly trusting AI systems and their recommendations.

Military forces may opt to design specific military directives most suitable for providing specific guidance and delimitation for AI systems; be it rules of engagement (ROE), fragmentary orders (FRAGO), operational orders (OPORD) or other appropriate instructions. The skill and competence to design such instructions may need to be part of future training requirements, wherein the desire for

⁸² Paul Barry, *2025-2026 Data Centre Construction Cost Index*, Turner & Townsend, 5 November 2025, available at: <https://reports.turnerandtowntsend.com/data-centre-construction-cost-index-2025/>.

⁸³ Evan Laksamana, "6. Implications and Considerations", *Contingent Capabilities: Southeast Asia's Emerging Anti-Access Environment*, International Institute of Strategic Studies, London, February 2026, p. 33, available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2026/contingent-capabilities-southeast-asias-emerging-anti-access-environment/contingent-capabilities-southeast_asias-emerging-anti-access-environment.pdf.

⁸⁴ N. Sylvia, above note 24.

⁸⁵ Erick Nielson C. Javier, *Reality from Science Fiction: Strategic Implications of Autonomous Weapon Systems for Philippine Defense and Deterrence*, NDCP Executive Policy Brief No. 2024-01, National Defense College of the Philippines, Quezon City, 27 March 2024, p. 6, available at: <https://ndcp.edu.ph/wp-content/uploads/2024/04/EPB-2024-01.pdf>.

precautions on use of AI must be balanced with operational suitability and technical competence.⁸⁶

At the ASEAN level, proposals to improve ADMM's cooperation on military AI currently revolve around areas of practical cooperation, particularly non-combat operations such as maritime security exercises, as well as exercises for responding to cyber threats to AI systems.⁸⁷ These are in line with ASEAN's preferred approach for cooperation, meant to build confidence among members. Given that the largest benefits and highest risks of military AI tend to involve high decision-making speeds, it is likely that stress-testing such AI, which is essential to really establish actual baselines on AI models, will need different operational scenarios, specific to the ASEAN region, to better visualize the challenges and thresholds that future commanders must keep in mind when using AI for decision support. While exercising use of military AI in high-intensity scenarios at the ASEAN level may be politically unlikely at present, moving towards such exercises has to be considered sooner or later; otherwise, individual ASEAN member states may opt to investigate building such capabilities in partnership with other willing members, or with third party states. While building with third-party state providers is expedient and provides access to capabilities probably not available yet within ASEAN, it creates potential strategic vulnerabilities that ASEAN states would rather avoid.

In terms of AI-assisted weapons and materiel, there seem to be no clear consensus yet amongst ASEAN member states on standards and practices. ASEAN and ADMM could build on the Joint Statement of the ASEAN Defence Ministers on Cooperation in the Field of Artificial Intelligence in the Defence Sector and explore discussing guidelines, standards and practices for material applications of AI; perhaps as a means of strengthening ASEAN Defence Industry Collaboration (ADIC)⁸⁸, another ongoing ADMM initiative for concrete defence cooperation.

Ultimately, while AI is likely to derive some marginal efficiencies in force command and control as seen in initial experiments, or provide some niche operational capability, much will need to be done before AI can result in enhanced effectiveness for Southeast Asian militaries, given those states' other capability gaps. Southeast Asian states would face other factors that may mitigate whatever advantage AI could bring, such as rules of engagement considerations or more

⁸⁶ Jonathan Kwik *et al.*, *Controlling Military Artificial Intelligence: Harnessing Rules of Engagement and Military Directives*, Asser Policy Brief 2025-01, TM Asser Institute, The Hague, February 2025, pp. 21-22, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5132731.

⁸⁷ Mohammed Faizal Bin Abdul Rahman, *AI in Defence: The Way Forward for ASEAN's ADMM Cooperation*, IDSS Paper No. 084, S. Rajaratnam School of International Studies, Singapore, pp. 3-4, available at: <https://www.rsis.edu.sg/wp-content/uploads/2025/08/IP25084.pdf>.

⁸⁸ Concept Paper on Enhancing ASEAN Defence Industry Collaboration adopted by the 19th ASEAN Defence Ministers Meeting, 31 October 2025, available at: https://admm.asean.org/dmdocuments/2025_19th%20ADMM_KL,%20Malaysia,%2031%20October%202025_Concept%20Paper%20on%20Enhancing%20ADIC.pdf.

fundamental disparities in arms and capabilities. Like other countries, the key for Southeast Asian states to enhance their security will be to combine the adoption of AI with the requisite material capabilities, and strategic, organizational and operational adaptability, that mark effective military forces.⁸⁹

The use of AI in the military will likely only increase, especially as the technology matures and is successfully demonstrated in other regions of the world. As the militaries of Southeast Asia prepare to meet a future of warfare where AI plays major roles, they must be ready to balance the imperative to experiment with prudence and caution.

⁸⁹ M. Raska and R. Bitzinger, above note 81, p. 9.