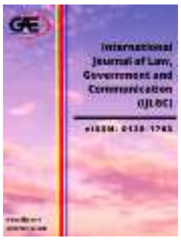

INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.gaexcellence.com/ijlgc

EMERGING MILITARY TECHNOLOGIES IN THE U.S.–CHINA RIVALRY: IMPLICATIONS FOR SOUTHEAST ASIA'S DEFENSE LANDSCAPE

Herlin Anak Aman[1], Aini Fatihah Roslam[2*], Tharishini Krishnan[3]

[1]Department of Strategy and Defence Studies, Faculty of Defence Studies and Management, National Defence University of Malaysia (UPNM), Malaysia.
herlin@upnm.edu.my https://orcid.org/0009-0003-1835-0607

[2]Department of International Relations, Security and Law, Faculty of Defence Studies and Management, National Defence University of Malaysia (UPNM), Malaysia.
ainifatihah@upnm.edu.my https://orcid.org/0000-0001-9066-4895

[3]Department of Strategy and Defence Studies, Faculty of Defence Studies and Management, National Defence University of Malaysia (UPNM), Malaysia
tharishini@upnm.edu.my https://orcid.org/0000-0002-1463-6232

*Corresponding Author

Article Info:

Article history:
Received date: 15.12.2025
Revised date: 11.01.2026
Accepted date: 29.01.2026
Published date: 05.03.2026

To cite this document:

Anak Aman, H., Roslam, A. F., & Krishnan, T. (2026). Emerging Military Technologies in The U.S.–China Rivalry: Implications for Southeast Asia's Defense Landscape. *International Journal of Law, Government and Communication, 11*(43), 142-158.

Abstract:

Artificial intelligence (AI) has become a central driver of military transformation in both the United States and China, reshaping patterns of strategic competition and security governance. While existing studies largely examine AI's implications for great-power rivalry, limited attention has been given to how AI-driven military competition affects Southeast Asia's strategic autonomy and regional stability. This study addresses this gap by analysing how the diffusion of autonomous systems, surveillance technologies, and cyber capabilities influences ASEAN's threat perceptions and strategic responses. The research adopts a qualitative design based on thematic and discourse analysis of selected defence policy documents, official strategies, and authoritative policy reports from the United States, China, and regional institutions. Documents were systematically coded to identify patterns related to governance frameworks, operational priorities, escalation risks, and regional dependencies. The findings indicate that AI-enabled military modernisation intensifies strategic rivalry, accelerates operational tempo, and increases the risks of miscalculation in contested maritime and digital domains. Most ASEAN states face persistent constraints, including limited technological capacity, uneven interoperability, cybersecurity vulnerabilities, and reliance on external suppliers, which collectively narrow policy flexibility and strategic autonomy. The study contributes by providing one of the first region-focused analyses linking

U.S.–China AI military competition to ASEAN's strategic agency. Policy implications highlight the need for ASEAN to strengthen technological resilience, develop regionally aligned governance norms, and institutionalise confidence-building mechanisms for AI-enabled systems. Rather than remaining a reactive arena of great-power competition, ASEAN has the potential to shape regional rules, manage escalation risks, and act as a proactive stabilising actor in the evolving AI security landscape.

DOI:10.35631/IJLGC.1143011

Keyword:

Artificial Intelligence; ASEAN; Security Governance; Strategic Autonomy; U.S.–China Rivalry.

Introduction

The Fourth Industrial Revolution has elevated artificial intelligence (AI) into a central general-purpose technology that is fundamentally transforming global economic systems, social interactions, and the strategic conduct of warfare. Characterised by the convergence of digital, physical, and biological technologies, this revolution has accelerated the militarisation of data, algorithms, and automation, positioning AI as a decisive force multiplier in contemporary and future conflicts (Schwab, 2016; Horowitz, 2018). In modern military environments, AI is no longer confined to experimental applications but is increasingly embedded across multiple operational domains, including intelligence collection, surveillance, and reconnaissance (ISR); operational planning and decision-support systems; predictive logistics and maintenance; cyber operations; and the coordination of autonomous and semi-autonomous platforms operating across land, air, maritime, space, and cyber domains (Scharre, 2018; Cummings, 2021).

Collectively, these developments constitute what scholars and practitioners describe as "algorithmic warfare," a paradigm in which algorithms play a critical role in sensing, decision-making, and action across the battlespace (RAND, 2024; Payne, 2021). Algorithmic warfare reflects a shift from platform-centric military power towards data-centric and networked forms of warfare, where speed, adaptability, and informational superiority are increasingly decisive (Kania, 2019). The integration of AI into military command and control (C2) systems further raises important questions regarding human–machine interaction, delegation of authority, and the balance between automation and human judgment under conditions of uncertainty and high operational tempo (Horowitz et al., 2020).

Within U.S. defence strategy, AI is explicitly positioned as a core strategic enabler intended to enhance command effectiveness, situational awareness, and operational precision through human–machine teaming, cross-sector collaboration with the private technology sector, and sustained investment in data-driven innovation ecosystems (U.S. Department of Defense, 2023). The U.S. Department of Defense emphasises that AI adoption is not solely a technological endeavour but a transformational process involving organisational culture, doctrine, ethics, and governance, particularly in ensuring that AI-enabled systems remain aligned with democratic values, accountability, and responsible use of force (U.S. Department of Defense, 2023; Allen & Chan, 2017). As such, AI has emerged not only as a tool of military efficiency but also as a strategic variable shaping deterrence dynamics, military competition, and the future character of war among major powers.

Literature Review

Emerging scholarship increasingly converges on the view that advances in artificial intelligence (AI) are restructuring the foundations of strategic power in the international system, with data, computational infrastructure, and specialised technical expertise becoming core national security assets alongside traditional military capabilities (Jenkins et al., 2025; Horowitz, 2018). AI's strategic value lies not merely in efficiency gains but in its capacity to reshape decision-making speed, information dominance, and force employment across multiple domains of warfare. As states integrate AI into intelligence analysis, command-and-control systems, and autonomous platforms, strategic competition is progressively shifting towards control over data ecosystems, algorithmic innovation, and resilient digital infrastructure (Payne, 2021; Kania, 2019).

At the same time, a substantial body of literature cautions that the rapid militarisation of AI generates profound ethical, legal, and governance dilemmas. Batool, Zowghi, and Bano (2023) emphasise that accountability gaps, algorithmic bias, opacity in decision-making processes, and difficulties in auditing complex AI systems pose serious challenges to democratic oversight and the laws of armed conflict. These concerns extend beyond technical system design to encompass broader institutional and normative dimensions, including responsibility attribution in human–machine teaming, civilian control of the military, and compliance with international humanitarian law (IHL) (Scharre, 2018; Cummings, 2021). Consequently, AI governance in defence settings is increasingly framed as a socio-technical problem that requires integrated legal, ethical, and organisational responses rather than purely technological solutions.

China's approach to military AI development is most prominently shaped by its military–civil fusion (MCF) strategy, which seeks to systematically integrate civilian research institutions, private technology firms, and state-owned defence enterprises into a unified innovation ecosystem supporting the modernisation of the People's Liberation Army (PLA). Empirical procurement studies indicate a growing participation of commercial AI firms as suppliers to the PLA, underscoring the diffusion of dual-use technologies across China's defence-industrial base (Cools & Maathuis, 2024; Kania, 2019). While this model enhances efficiency, scalability, and rapid innovation, it also complicates international transparency, export control regimes, and arms control verification, as the boundaries between civilian and military technological development become increasingly blurred. In contrast, the United States relies more heavily on market-driven innovation and partnerships with the private sector, albeit within a regulatory framework that emphasises ethical AI principles and responsible use (U.S. Department of Defense, 2023). Despite these institutional differences, both major powers face convergent challenges, including increasing automation of combat functions, deeper civilian–military technological entanglement, and persistent governance and accountability concerns surrounding AI-enabled warfare (Jenkins et al., 2025; Horowitz et al., 2020).

Within Southeast Asia, the military adoption of AI carries significant strategic, political, and institutional implications. From an operational perspective, AI-enabled systems accelerate the Observe–Orient–Decide–Act (OODA) loop, potentially enhancing battlefield responsiveness and precision while simultaneously reducing opportunities for human deliberation and increasing risks of miscalculation and inadvertent escalation (Horowitz, Scharre, & Velez-Green, 2019; Payne, 2021). Politically, the dominance of major powers in setting technological standards and shaping AI supply chains risks generating new forms of strategic dependency for smaller states, thereby constraining policy autonomy and defence decision-making. Recent regional studies stress the urgency of strengthening ASEAN's institutional capacity to address these challenges through coordinated and ethically grounded AI governance mechanisms (Keith, 2024; Putra, 2024).

Scholars increasingly advocate for a multidimensional ASEAN approach that prioritises domestic capacity building, robust data governance frameworks, interoperability standards, and transparency measures in defence technology adoption (Putra, 2024). Such an approach would enable ASEAN to manage escalation risks, enhance trust among member states, and prevent the misuse of AI-enabled military systems. More broadly, the literature suggests that ASEAN has the potential to play a normative role in shaping responsible AI practices by embedding confidence-building measures, collective oversight mechanisms, and regional risk-management frameworks into its security architecture. Through these efforts, Southeast Asia can contribute to the development of stabilising AI norms that mitigate great-power competition and reinforce long-term security and stability in the Indo-Pacific region (Keith, 2024; Jenkins et al., 2025).

Despite growing scholarship on AI and military competition among major powers, existing studies remain predominantly focused on technological capability development, deterrence stability, and ethical governance at the global level. There is comparatively limited empirical analysis of how AI-driven military rivalry concretely affects Southeast Asia's strategic autonomy, policy flexibility, and regional security governance. In particular, the interaction between external technological competition and ASEAN's institutional constraints remains underexplored. This study seeks to fill this gap by examining how U.S.–China AI military modernisation reshapes strategic choices and risk management in Southeast Asia.

Methodology

This study employs a qualitative research design to examine how artificial intelligence shapes U.S.–China strategic competition and its implications for Southeast Asian security. Data were drawn from purposively selected sources, including defence white papers, national AI strategies, military doctrine publications, official statements, and policy reports produced between 2019 and 2025. Selection criteria prioritised documents that explicitly address military AI adoption, governance frameworks, operational concepts, and regional security implications. Defence documents and policy reports were emphasised because they reflect authoritative strategic intent, institutional priorities, and operational thinking that are not consistently captured in academic literature alone.

A qualitative approach is particularly appropriate given the exploratory and interpretive nature of the research, which seeks to analyse strategic intentions, governance frameworks, and normative discourses rather than to measure causal effects or generate predictive models (Creswell & Poth, 2018; George & Bennett, 2005). By focusing on meaning, context, and interpretation, the methodology enables a nuanced understanding of how AI is conceptualised and operationalised within competing military and strategic paradigms.

The study relies primarily on secondary data sources, including official policy documents, defence white papers, national AI strategies, military doctrine publications, and statements issued by relevant government agencies in the United States and China. These materials are complemented by peer-reviewed academic literature and analytical reports produced by reputable strategic research institutions and think tanks, such as RAND, the Center for a New American Security (CNAS), and the International Institute for Strategic Studies (IISS). The use of multiple source types facilitates data triangulation, enhancing the credibility and analytical robustness of the findings (Yin, 2018).

Data analysis followed a two-stage coding process. First, open coding was applied to identify recurring themes related to governance mechanisms, civil–military integration, escalation risks, technological dependency, and regional responses. Second, axial coding was used to refine relationships among these themes and compare patterns across U.S., Chinese, and ASEAN sources (Braun & Clarke, 2006). Discourse analysis was then applied to examine how strategic narratives, threat perceptions, and legitimacy claims surrounding AI were constructed in official texts. Triangulation across multiple document types enhanced analytical reliability and reduced interpretive bias (Fairclough, 2013). This dual-analytical approach allows the study to capture both substantive policy orientations and the underlying ideational structures that shape AI-driven military transformation.

By prioritising interpretive analysis over quantitative measurement, the methodology enables a deeper examination of strategic motivations, ethical considerations, and geopolitical implications associated with the militarisation of AI in the Indo-Pacific region. It facilitates comparative insights into how differing political systems, institutional arrangements, and strategic cultures influence AI adoption in the United States and China, as well as how these dynamics affect Southeast Asian states navigating major-power competition. While the study does not seek to produce generalisable causal claims, it aims to generate analytically grounded insights that contribute to scholarly debates on emerging military technologies, strategic rivalry, and regional security governance.

United States: Commercial Collaboration and Doctrinal Adaptation

The U.S. approach to military AI integration rests on two interrelated elements: (1) reliance on commercial innovation, and (2) institutional efforts to systematize and scale AI adoption across defense organizations. Structurally, the Department of Defense (DoD) has undergone organizational reforms most notably the consolidation of the Joint Artificial Intelligence Center (JAIC) into the Office of the Chief Digital and Artificial Intelligence Officer (CDAO) to streamline digital transformation and coordinate AI development more effectively (U.S. DoD, 2023; ai.mil, 2024).

The DoD's operational model prioritizes public–private partnerships, leveraging commercial firms to supply advanced models, cloud services, and analytical tools (DoD, 2023). This trend is evident in the series of mid-2025 contracts awarded to major AI companies including OpenAI, Google/Alphabet, Anthropic and xAI, each valued at up to USD 200 million, aimed at integrating frontier AI capabilities into defense workflows. While this model accelerates capability development, it also introduces significant governance concerns: supply chain vulnerabilities, export-control compliance, protection of sensitive data, and questions about the reliability of commercial systems in high-risk environments (Reuters, 2025; Politico, 2025). Doctrinally, the U.S. military emphasizes "accelerating decision advantage" through AI-enabled support systems, while maintaining human-in-the-loop or human-on-the-loop mechanisms to ensure oversight and mitigate failure risks (U.S. DoD, 2023). Scholars note that America's strategic strengths—commercial expertise, extensive computational resources, and a vibrant innovation ecosystem—are counterbalanced by regulatory challenges, societal concerns, and dependency on private-sector dynamics (RAND, 2024; Horowitz et al., 2019).

China: Military–Civil Fusion and Rapid Technological Development

China's AI strategy differs fundamentally in structure and governance. Under the military–civil fusion (MCF) framework, the state deliberately coordinates investments, research, and commercial participation to accelerate the transfer of dual-use technologies to the People's Liberation Army (PLA). Analyses of procurement data from 2023–2024 indicate a surge in AI-related PLA contracts involving both traditional defense suppliers and new commercial entrants, illustrating the breadth of China's technology diffusion (CSET, 2025).

The MCF model enables rapid development of autonomous systems, enhanced ISR analytics, and integrated information networks that support large-scale command decision-making (Kania, 2021). State incentives—including funding, guaranteed procurement, and access to domestic markets—lower participation risks for firms entering the defense ecosystem.

However, this approach also entails constraints. The deep civilian–military integration complicates external transparency and makes it difficult to differentiate between civilian and defense technological investments (CSET, 2025). Rapid acquisition may also compromise quality control and interoperability, given the diversity of suppliers. Additionally, the diffusion of dual-use technologies through commercial networks heightens concerns about inadvertent transfers to non-state actors (Kania, 2021; Stokes, 2024).

Applying Realism to the Technological Security Dilemma: A Theoretical Framework

This study applies structural realism to analyse how artificial intelligence (AI) shapes the United States China strategic rivalry and reconfigures security dynamics in Southeast Asia. Within the realist tradition, the international system is defined by anarchy, or the absence of a central authority, which compels states to prioritise survival through the accumulation of power and the pursuit of security (Waltz, 1979; Mearsheimer, 2001). From this perspective, emerging military technologies are not neutral instruments but strategic assets whose distribution and use alter relative power balances. AI, as a general purpose and dual use technology, represents a transformative capability comparable to earlier military revolutions such as mechanisation, nuclear weapons, or precision guided munitions.

Structural realism emphasises that AI intensifies the classical security dilemma. By accelerating intelligence processing, target identification, decision making cycles, and operational tempo, AI enhanced military systems increase battlefield effectiveness and perceived strategic advantage. However, these same attributes generate uncertainty and fear among rivals, as defensive innovations are often indistinguishable from offensive preparations (Jervis, 1978). The integration of AI into command-and-control systems, autonomous platforms, and surveillance architectures compresses decision time and reduces the margin for human deliberation, thereby heightening the risk of misperception, inadvertent escalation, and crisis instability, particularly in contested environments such as the South China Sea and the Taiwan Strait (Horowitz, Scharre, & Velez Green, 2019; UNODA, 2025). In realist terms, AI exacerbates offense defense ambiguity and reinforces self-help behaviour, driving competitive military modernisation rather than mutual reassurance.

For Southeast Asian states, structural realism suggests that the intensification of the US China rivalry generates strategic constraints. Smaller and middle powers face structural limitations that reduce their ability to independently shape technological competition, compelling them to adopt strategies such as balancing, bandwagoning, or hedging based on threat perceptions, regime interests, and economic dependencies. From a realist perspective, hedging emerges as a rational response to uncertainty, allowing states to avoid excessive alignment while preserving strategic flexibility amid great power rivalry. Nevertheless, the diffusion of AI enabled military capabilities and growing technological dependence on external powers risks widening strategic asymmetries and constraining long term autonomy.

Recent scholarship reinforces this structural realist interpretation. Studies increasingly conceptualise an AI security dilemma, whereby even ostensibly defensive applications, such as decision support tools or intelligence, surveillance, and reconnaissance (ISR) enhancements, trigger reciprocal countermeasures and arms racing dynamics, particularly in the context of US China technological decoupling (Khan & Hussain, 2024). Moreover, AI's dual use nature blurs the boundaries between civilian innovation and military power, drawing economic policy, industrial strategy, and data governance into the sphere of strategic competition (Gerasimova, 2024). These dynamics complicate the strategic calculus of Southeast Asian states, whose economic integration with major powers intersects with their security concerns.

Overall, the application of structural realism demonstrates that the militarisation of AI is more likely to reinforce great power rivalry and intensify security dilemmas than to promote regional stability. Rather than functioning as a stabilising or purely efficiency enhancing technology, AI amplifies existing power competitions, accelerates arms racing behaviour, and deepens asymmetries within a multipolar Indo Pacific order, outcomes consistent with realism's enduring expectations regarding the relationship between technological change and international security.

Comparative Dynamics and Risk Profiles

A comparative assessment of United States and Chinese military artificial intelligence models reveals two interrelated dimensions of risk that carry profound implications for regional stability in Southeast Asia namely the tension between speed and governance and the diffusion of dual use technologies. Together these dimensions underscore that AI driven military power cannot be evaluated solely in terms of technological performance but must be situated within broader institutional and political contexts.

Speed vs. Governance

The United States derives a significant advantage from rapid innovation cycles sustained by a vibrant commercial technology ecosystem global scale computational infrastructure and leadership in advanced AI research including generative models. This ecosystem enables the U.S. Department of Defense to access innovative capabilities through public private partnerships and flexible procurement mechanisms thereby accelerating experimentation and operational integration (DoD 2023; RAND 2024). However, this speed of innovation is simultaneously moderated by governance constraints. Ethical principles for responsible AI export control regimes and congressional and public oversight impose limits on deployment pathways particularly for lethal or high-risk applications. While these constraints may slow adoption they also function as stabilising mechanisms by enhancing transparency accountability and domestic legitimacy in the military use of AI.

China presents a contrasting risk profile shaped by its centrally coordinated Military Civil Fusion strategy. Through national level mobilisation of resources and the integration of civilian technology firms research institutions and defence enterprises China has achieved rapid technological absorption and diffusion within the People's Liberation Army. This model reduces coordination costs and enables swift scaling of AI enabled capabilities (CSET 2025). Nonetheless the same centralisation generates governance vulnerabilities. The involvement of a wide array of nontraditional suppliers raises concerns regarding system interoperability quality assurance and long-term reliability. Moreover, limited transparency surrounding development and deployment processes complicates external assessment and increases uncertainty among potential adversaries thereby intensifying the security dilemma. From a regional perspective these governance gaps may heighten escalation risks during crises as neighbouring states struggle to interpret Chinese intentions and operational thresholds.

Diffusion of Dual-Use Technologies

A second critical dimension of risk lies in the diffusion of dual use AI technologies. Both the United States and China have actively facilitated the spread of AI capabilities beyond their own militaries albeit through different mechanisms. The United States promotes diffusion through commercial procurement networks defence cooperation programmes and interoperability driven collaboration with allies and partners. This model accelerates access to advanced capabilities among friendly states but also embeds them within U.S. technological standards and governance frameworks.

China's diffusion pathway operates through its Military Civil Fusion ecosystem combined with technology exports joint ventures and digital infrastructure initiatives linked to broader economic engagement. This approach extends AI enabled capabilities to state with strategic or economic ties to Beijing often with fewer governance conditionalities. For Southeast Asia these parallel diffusion pathways have resulted in a rapid proliferation of AI enabled systems including intelligence surveillance and reconnaissance tools autonomous or semi-autonomous platforms and advanced data analytics across a growing range of state and non-state actors.

While broader access lowers traditional barriers to entry and enhances military modernisation it also generates new forms of risk. The literature highlights increased prospects for capability races crisis instability and operational complexity in contested environments where multiple actors deploy partially autonomous systems with varying levels of human control and doctrinal integration (Horowitz et al. 2019; RAND 2024). In the absence of shared norms or robust confidence building measures such diffusion may undermine crisis management and increase the probability of inadvertent escalation.

Findings

Strategic Miscalculation Risks

The incorporation of artificial intelligence into surveillance systems, autonomous platforms, and command and control architectures has significantly accelerated military decision-making processes. In the Southeast Asian context, AI enabled maritime domain awareness and cyber monitoring systems compress response timelines and reduce opportunities for political oversight and human judgement. In contested environments such as the South China Sea and cyberspace, these dynamics increase the likelihood of misinterpretation, accidental signalling, and rapid escalation during crises. Existing research highlights that automation bias and limited transparency in algorithmic decision making can further destabilise crisis management, particularly among states with weaker institutional safeguards and crisis communication mechanisms (Horowitz et al. 2018; Allen and Chan 2017; Davis and Sisson 2020; Sheehan 2023).

Technological and Institutional Constraints

Despite growing awareness of the strategic importance of defence digitalisation, most ASEAN member states face persistent technological and institutional constraints. These include uneven digital infrastructure, fragmented defence procurement systems, weak defence innovation ecosystems, and shortages of specialised human capital. Limited interoperability among national armed forces further constrains the effective deployment of AI enabled military capabilities. Such constraints inhibit indigenous defence innovation and reinforce reliance on foreign defence technologies. The literature on ASEAN security cooperation consistently notes that technological asymmetry and institutional divergence remain major obstacles to deeper military integration and collective security initiatives (Acharya 2014; Hoadley and Rüland 2017; Heiduk and Wacker 2020; Bitzinger 2022).

Cybersecurity Vulnerabilities

The increasing dependence on externally developed software platforms, cloud services, and AI systems exposes ASEAN states to significant cybersecurity vulnerabilities. These vulnerabilities include data breaches, supply chain manipulation, embedded system backdoors, and cyber intrusion by both state and non state actors. For countries with limited cyber governance frameworks and regulatory capacity, the diffusion of AI into defence and critical infrastructure sectors may amplify rather than mitigate security risks. Empirical studies emphasise that developing and middle-income states are particularly vulnerable to cyber threats due to dependence on foreign vendors and weak institutional resilience (Lindsay 2015; Kshetri 2021; Lewis 2021).

Economic and Technological Dependencies

ASEAN states remain structurally embedded within competing United States and Chinese technology ecosystems, particularly in areas such as semiconductors, cloud infrastructure, surveillance platforms, and defence related AI applications. This dependence significantly constrains strategic autonomy and narrows policy options for effective hedging. Export controls, competing technological standards, and intensifying great power rivalry complicate efforts by Southeast Asian states to maintain neutrality while pursuing technological modernisation. International political economy scholarship demonstrates that asymmetric interdependence in critical technology sectors generates political leverage and increases vulnerability for smaller states within global supply chains (Farrell and Newman 2019; Gilli and Gilli 2019; Nye 2021; Ravenhill 2020).

Strategic Implications for Southeast Asian Stability

The accelerating competition in artificial intelligence between the United States and China represents a renewed manifestation of great power rivalry that is reshaping Southeast Asia's security landscape. As a geopolitically pivotal region situated along vital global trade routes, Southeast Asia now functions as a central arena where technological influence, military doctrine, and strategic diplomacy intersect. The implications of AI extend beyond traditional military domains to encompass economic, political, and normative dimensions, areas historically guided by ASEAN's principles of centrality, strategic autonomy, and nonalignment (Acharya, 2022).

Shifting Balance of Power and Strategic Dynamics

The integration of AI into U.S. and Chinese military capabilities is altering regional power configurations by enhancing situational awareness, compressing decision making cycles, and enabling autonomous operations. Both states deploy real time analytics, predictive intelligence, and unmanned systems to strengthen operational effectiveness. In Southeast Asia, these capabilities manifest through persistent maritime surveillance, expanded unmanned operations, and intensified electronic intelligence activities across critical waterways such as the South China Sea and the Strait of Malacca (IISS, 2024).

The United States, through INDOPACOM, is implementing AI enabled maritime monitoring as part of the Joint All Domain Command and Control JADC2 initiative, linking multi domain assets into a unified digital command network (U.S. INDOPACOM, 2024). Concurrently, China is advancing intelligentized warfare capabilities within the PLA Navy, supported by autonomous platforms and AI enhanced satellite imagery processed through the Gaofen constellation (Kania, 2021; CSET, 2025).

These parallel technological advancements reinforce an action reaction cycle that heightens the risk of an arms race. ASEAN now faces a strategic crossroads, whether to enhance its technological and operational capacity to keep pace with great powers or maintain strategic neutrality to avoid entanglement in competing spheres of influence (Goh, 2024).

Threats to Digital Sovereignty and Regional Cybersecurity

AI proliferation also intensifies nontraditional security challenges, particularly in cyber defense and digital sovereignty. Military AI tools, while enhancing operational efficiency, can be repurposed for surveillance, information control, and digital interference, thereby increasing vulnerability to external manipulation and compromising national data integrity.

China's Digital Silk Road, encompassing investments in 5G networks, data centers, and smart surveillance systems in states such as Cambodia, Malaysia, and Laos, strengthens regional digital infrastructure but raises concerns regarding data governance, external access, and long-term technological dependence (Chen & Cheong, 2023; Thuzar, 2024). In contrast, the United States promotes initiatives such as the Clean Network and the Indo Pacific Digital Strategy to counterbalance Chinese digital influence, yet these measures are perceived by some ASEAN members as geopolitical pressure that complicates economic engagement with China (ASEAN Secretariat, 2024).

The convergence of these competing technological frameworks is producing a polarized cybersecurity landscape, complicating ASEAN's ability to maintain a neutral, secure, and cohesive regional governance model. The intersection of AI enabled military competition and digital influence underscores the urgent need for ASEAN to strengthen normative frameworks, data governance mechanisms, and multi stakeholder engagement to safeguard regional stability and technological sovereignty.

Interoperability Challenges and ASEAN's Military Dilemma

ASEAN member states face both technical disparities and strategic uncertainty in adapting to artificial intelligence driven military modernization. Singapore and Vietnam have made significant strides in defense AI capabilities, with Singapore establishing the Digital and Intelligence Service DIS to support cyber defense and military analytics (Singapore MINDEF, 2023). The Philippines has expanded AI enabled maritime surveillance through U.S. support under EDCA, including the deployment of autonomous monitoring systems (U.S. Department of State, 2024).

In contrast, countries such as Laos, Cambodia, and Myanmar confront substantial capability gaps in digital security and AI based defense systems. This unevenness creates interoperability challenges that undermine ASEAN's collective response capabilities, particularly against transnational threats including cyberattacks and coordinated disinformation campaigns (ADMM, 2024). Furthermore, the growing influx of AI enabled systems from major powers risks generating strategic dependency, a form of technology entrapment in which states become reliant on foreign suppliers for systems upkeep, software updates, and data management (Kaplan & Wright, 2023).

Risks of Escalation and Misinterpretation in Regional Conflicts

The deployment of AI enabled surveillance and unmanned systems in Southeast Asia's maritime domains significantly increases the potential for unintended escalation. By compressing decision making cycles, automating responses, and relying on imperfect or incomplete data, these technologies reduce human oversight and heighten the probability of misinterpreting routine tactical maneuvers as hostile actions. In highly contested zones, such as the Spratly Islands or Scarborough Shoal, even minor operational discrepancies can be amplified into perceived threats, triggering rapid military responses that are difficult to reverse through diplomatic channels (RAND, 2024).

AI enabled systems are particularly prone to generating false positives or overestimating threat levels due to algorithmic biases, sensor limitations, and real time operational pressures. Autonomous platforms operating under preprogrammed threat thresholds may respond to innocuous activities with defensive or offensive actions, creating a feedback loop of escalation. The 2023 reports of intensified AI based surveillance activities around disputed maritime features underscore how quickly these risks can materialize, particularly when multiple actors deploy systems with differing doctrines, operational rules, and command structures (AMTI, 2024).

The rapid proliferation of AI capabilities among regional and extra regional actors compounds these risks. As more states adopt autonomous and semi-autonomous systems, the interaction between diverse technological platforms increases operational complexity and reduces predictability. This environment amplifies the likelihood of accidents, miscalculations, and inadvertent confrontations, making crisis management and conflict deescalation more challenging. Consequently, AI enabled military capabilities, while enhancing situational awareness and operational efficiency, simultaneously introduce structural vulnerabilities that could destabilize regional security if left unmitigated.

ASEAN's Response and Governance Challenges

ASEAN's current security frameworks, including the ASEAN Regional Forum ARF, the ASEAN Defense Ministers' Meeting ADMM, and the ASEAN Cybersecurity Cooperation Strategy, were originally designed to address traditional and emerging security threats. While these mechanisms provide broad platforms for dialogue, information sharing, and confidence building, they lack dedicated protocols for managing artificial intelligence related defense risks. Specifically, AI enabled systems, autonomous platforms, and algorithmic decision support introduce unique challenges such as rapid escalation potential, misinterpretation of actions, dual use technology proliferation, and cyber vulnerabilities that existing mechanisms are not fully equipped to address.

Recognizing these gaps, several ASEAN member states have initiated proposals to enhance regional governance of AI in military contexts. Malaysia and Indonesia, for example, have advocated for the development of ASEAN wide Guiding Principles on AI Governance and Military Ethics. Such principles would provide normative frameworks for responsible AI deployment, including rules for human oversight, transparency in algorithmic decision making, and restrictions on lethal autonomous systems. The establishment of these principles aims to promote accountability, mitigate the risks of misuse, and ensure that technological advancement does not undermine regional stability (Malaysia MFA, 2024).

Singapore has also emphasized the need for regional confidence building measures CBMs tailored specifically for AI enabled military systems. These CBMs would facilitate information sharing, verification procedures, joint exercises, and crisis communication channels, thereby reducing the likelihood of inadvertent escalation resulting from AI enabled misperceptions or system failures (ADMM, 2024). By institutionalizing such measures, ASEAN can foster a degree of operational predictability among member states and between regional and extra-regional powers, enhancing trust in an otherwise technologically fragmented environment.

Despite these efforts, the effectiveness of ASEAN's response is constrained by several structural and political factors. Variations in strategic priorities across member states, combined with disparate technological capacities and defense modernization trajectories, complicate attempts to achieve cohesive policy alignment. Middle and smaller powers may prioritize economic relations with China or security partnerships with the United States, while technologically advanced states such as Singapore pursue cutting edge AI integration. These asymmetries create challenges for collective decision making and limit ASEAN's ability to enforce compliance with proposed guidelines or CBMs. Moreover, the consensus-based ASEAN Way, while effective in maintaining regional cohesion in traditional diplomacy, can impede rapid policy adaptation in response to fast moving technological developments, reducing the region's agility in mitigating AI related risks (Thuzar, 2024).

Consequently, ASEAN faces a dual challenge: fostering normative and operational frameworks capable of governing AI enabled military technologies while simultaneously bridging the capability and strategic gaps among member states. Addressing these challenges will require sustained engagement, technical capacity building, and multi stakeholder coordination involving governments, defense establishments, private sector actors, and regional institutions. Without such comprehensive measures, ASEAN risks being reactive rather than proactive in managing AI induced security dynamics, potentially amplifying strategic vulnerabilities in the Indo Pacific region.

Conclusion

The artificial intelligence driven military transformations pursued by the United States and China mark the emergence of a new strategic paradigm in global security. Both powers are engaged in a dual race: not only to develop advanced autonomous and AI enabled military systems but also to influence the normative, ethical, and governance frameworks that regulate their deployment.

For Southeast Asia, this rivalry generates complex and multidimensional implications for regional stability, strategic autonomy, and long-term security governance. The United States trajectory toward algorithmic warfare, powered by private sector innovation, emphasizes the integration of big data, machine learning, and autonomous systems into operational military frameworks. In contrast, China’s Military Civil Fusion model leverages national research and industrial capacities to rapidly advance intelligentized warfare, encompassing autonomous drones, AI supported air defense systems, and real time strategic analytics.

Geopolitically, this competition extends beyond technology to a contest over global values and governance models. The United States promotes norms of openness, transparency, and ethical use, whereas China prioritizes digital sovereignty, centralized control, and strategic information management. These divergent approaches exacerbate strategic mistrust and complicate multilateral dialogue, including within ASEAN led platforms such as ADMM Plus.

For ASEAN, the central challenge is to ensure that AI driven militarization does not evolve into a destabilizing security dilemma. Strengthening ethical governance frameworks, developing confidence building measures, and facilitating responsible technology cooperation are crucial steps for mitigating risks of escalation and maintaining operational stability.

This study contributes to the existing literature by offering a region-focused analysis that links AI-driven military modernisation by the United States and China to Southeast Asia’s strategic autonomy and security governance. While much prior research concentrates on technological performance, deterrence stability, or ethical regulation at the great-power level, this paper demonstrates how emerging military technologies reshape institutional capacity, dependency patterns, and escalation risks in smaller and middle-power regions. By integrating structural realism with qualitative evidence from defence and policy sources, the study provides an analytically grounded framework for understanding how technological rivalry translates into regional strategic constraints.

From a policy perspective, several practical implications emerge. First, ASEAN should prioritise technological resilience by expanding joint cyber capacity-building programmes, harmonising data protection standards, and promoting shared digital infrastructure to reduce long-term dependence on external suppliers. Second, regional governance mechanisms could be strengthened through the development of ASEAN-wide principles on military AI use, including requirements for human oversight, transparency in algorithmic decision-making, and interoperability guidelines. Third, confidence-building measures tailored to AI-enabled systems—such as information-sharing protocols, notification mechanisms for major deployments, and crisis communication channels—should be institutionalised within existing platforms such as the ADMM and ARF. Collectively, these measures would enhance regional predictability, mitigate escalation risks, and reinforce ASEAN's strategic agency in managing emerging security challenges.

By strengthening regional governance, technological resilience, and collective confidence-building mechanisms, ASEAN can move beyond reactive adaptation and assert itself as a proactive architect of stability in an increasingly AI-driven strategic environment. This proactive orientation will be essential for preserving strategic autonomy, managing escalation risks, and sustaining long-term peace and security in the Indo-Pacific.

Acknowledgements:	The authors would like to express their sincere gratitude to National Defence University of Malaysia for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.
Funding Statement:	No Funding
Conflict of Interest Statement:	The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Law, Government and Communication (IJLGC).
Ethics Statement:	Option B (For Studies Not Involving Human or Animal Subjects) This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.
Author Contribution Statement:	All authors contributed significantly to the development of this manuscript. Herlin Aman was responsible for the conceptualization, methodology, and overall supervision of the study. Aini Fatihah Roslam handled data collection, analysis, and interpretation of results. Tharishini Krishnan contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.

References

Acharya, A. (2022). ASEAN and regional order: Revisiting security community in Southeast Asia. Routledge.

Allen, G. C., & Chan, T. (2017). Artificial intelligence and national security. Belfer Center for Science and International Affairs.

Asia Maritime Transparency Initiative. (2024). Tracking new AI-enabled surveillance in the South China Sea. Center for Strategic and International Studies.

ASEAN Defence Ministers' Meeting. (2024). Joint declaration on defense cooperation in the digital domain. ASEAN Secretariat.

ASEAN Secretariat. (2024). ASEAN digital masterplan 2025. ASEAN Secretariat.

Boulanin, V., & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. Stockholm International Peace Research Institute.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brooks, R. A. (2019). Artificial intelligence and the future of warfare. International Security, 43(4), 7–40.

Center for Security and Emerging Technology. (2025, September). Pulling back the curtain on China's military–civil fusion: How the PLA mobilizes civilian AI for strategic advantage (C. McFaul, S. Bresnick, & D. Chou). Georgetown University.

Chen, Y., & Cheong, D. (2023). The Digital Silk Road and Southeast Asia's data dilemma. East Asian Policy, 15(3), 45–60.

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE.

Crootof, R. (2015). The killer robots are here: Legal and policy implications. Cardozo Law Review, 36(5), 1837–1915.

Cummings, M. L. (2021). Human machine teaming and the future of command and control.International Security, 45(4), 7–39. https://doi.org/10.1162/isec_a_00410

Davis, M., & Sisson, R. (2020). Military artificial intelligence and the risk of escalation. Survival, 62(5), 29–52.

Fairclough, N. (2013). Critical discourse analysis: The critical study of language (2nd ed.). Routledge.

Gerasimova, E. (2024). Dual use technologies and strategic competition in the Indo Pacific. Journal of Strategic Studies, 47(2), 215–234. https://doi.org/10.1080/01402390.2023.XXXXXX

Goh, E. (2024). ASEAN's strategic neutrality in the age of US China technological rivalry. Contemporary Southeast Asia, 46(2), 137–159. https://doi.org/10.1355/cs46-2a07

George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

Gilli, A., & Gilli, M. (2019). Why China has not caught up yet Military technological superiority and the limits of imitation. International Security, 43(3), 141–189.

Goldstein, A. (2022). Power transitions, institutions, and China's rise in East Asia. Journal of Strategic Studies, 45(6), 857–884.

Hoadley, S., & Rüland, J. (2017). Asian regionalism ASEAN and the politics of normative change. Journal of International Relations and Development, 20(3), 499–525.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. Texas National Security Review, 1(3), 37–57.

Horowitz, M. C., Scharre, P., & Velez Green, A. (2019). A stable nuclear future? The impactof autonomous systems and artificial intelligence [arXiv preprint]. https://arxiv.org/abs/1912.05291

Horowitz, M. C., Scharre, P., & Velez Green, A. (2019). Artificial intelligence and international security. Center for a New American Security.

Horowitz, M. C., Scharre, P., & Velez Green, A. (2020). AI and the future of defense. Center for a New American Security.

International Institute for Strategic Studies. (2024). The military balance 2024. Routledge.

Jervis, R. (1978). Cooperation under the security dilemma. World Politics, 30(2), 167–214. https://doi.org/10.2307/2009958

Kania, E. B. (2019). Battlefield singularity: Artificial intelligence, military revolution, and China's future military power. Center for a New American Security.

Kania, E. B. (2021). Artificial intelligence in China's revolution in military affairs. Journal of Strategic Studies, 44(4), 512–540. https://doi.org/10.1080/01402390.2021.1894136

Kaplan, E., & Wright, T. (2023). Technology entrapment and strategic dependency in the Indo Pacific. Brookings Institution.

Khan, S., & Hussain, M. (2024). The AI security dilemma and great power competition. Survival, 66(1), 79–98. https://doi.org/10.1080/00396338.2024.XXXXXX

Lewis, J. A. (2021). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Mazarr, M. J. (2018). Understanding deterrence. RAND Corporation.

Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton.

Ministry of Defence Singapore. (2023). Digital and Intelligence Service: Strengthening cyber defense for Singapore. Singapore Government.

Nye, J. S. (2021). Power and interdependence revisited. International Affairs, 97(6), 1609 1627.

Payne, K. (2021). Artificial intelligence: A revolution in strategic affairs? Survival, 63(2), 7 32. https://doi.org/10.1080/00396338.2021.XXXXXX

Politico. (2025, July 14). Pentagon will start using Musk's Grok. https://www.politico.com/news/2025/07/14/defense-department-grok-musk-00451845

RAND Corporation. (2024). Algorithmic warfare and the future of military operations. RAND.

RAND Corporation. (2024). Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence (RRA-3295-1). https://www.rand.org/pubs/research_reports/RRA3295-1.html

Reuters. (2025, July 14). U.S. defense department awards contracts to Google, xAI. https://www.reuters.com/business/autos-transportation/us-department-defense-awards contracts-google-xai-2025-07-14/

Rose, G. (1998). Neoclassical realism and theories of foreign policy. World Politics, 51(1), 144–172. https://doi.org/10.1353/wp.1998.0003

Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton & Company.

Schwab, K. (2016). The Fourth Industrial Revolution. World Economic Forum.

Schweller, R. L. (2004). Unanswered threats: A neoclassical realist theory of underbalancing. International Security, 29(2), 159–201. https://doi.org/10.1162/0162288041762873

Sheehan, M. (2023). Emerging technologies and strategic stability in Asia. Asian Security, 19(3), 241–258.

Stokes, J. (2024, February 1). Military artificial intelligence, the People's Liberation Army,and US China strategic competition [Congressional testimony]. Center for a New American Security. https://www.cnas.org/publications/congressional-testimony/military-artificial intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition

Tellis, A. J., & Corbett, R. (2020). AI and national security The future of military innovation. Carnegie Endowment for International Peace.

Thuzar, M. (2024). ASEAN and the governance of emerging technologies. ISEAS Perspective, 12(4), 1–10.

U.S. Department of Defense. (2023). Data, analytics, and artificial intelligence adoption strategy. https://media.defense.gov/2023/nov/02/2003333300/1/1/1/dod_data_analytics_ai_adoption_strategy.pdf

U.S. Department of Defense. (2023). Responsible artificial intelligence strategy and implementation pathways. Department of Defense.

U.S. Department of Defense. (2024). Military and security developments involving the People's Republic of China 2024: Annual report to Congress. https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF

U.S. Department of State. (2024). Fact sheet: US Philippines cooperation on emerging technology and defense innovation. Washington, DC.

U.S. Indo Pacific Command. (2024). Joint all domain command and control: Indo Pacific integration strategy. Honolulu, HI.

UN Office for Disarmament Affairs (UNODA). (2025). Artificial intelligence and emerging risks to international security. United Nations.

Waltz, K. N. (1979). Theory of international politics. McGraw-Hill.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE