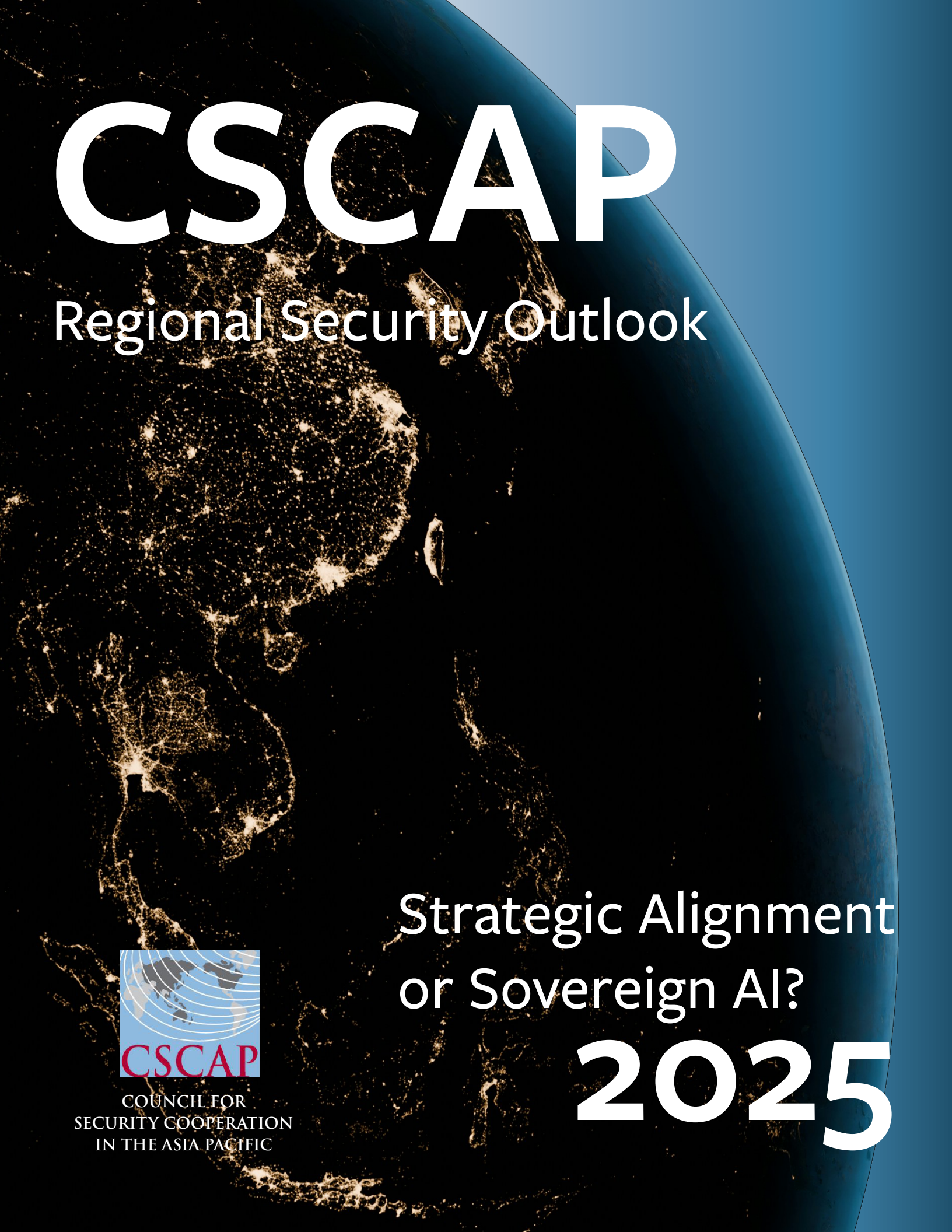

CSCAP

Regional Security Outlook

Strategic Alignment or Sovereign AI?

2025

CSCAP

COUNCIL FOR SECURITY COOPERATION IN THE ASIA PACIFIC

Former South Korean President Yoon at the 2024 AI Seoul Summit on May 21, 2024. | Photo: Handout, Office of the President. Official Photographer: Kang Min Seok.

STRATEGIC ALIGNMENT OR SOVEREIGN AI?

THE GLOBAL AI RACE, THE NEW CULT OF THE OFFENSIVE, AND THE TWO STRATEGIC PATHS FOR MIDDLE POWERS IN THE INDO-PACIFIC

Yang Gyu Kim

Assistant Professor, Graduate School of National Security, Korea National Defense University

We are at an inflection point, and the geopolitics of artificial intelligence (AI) development is shifting rapidly. In February 2025, France hosted the AI Action Summit, a high-level gathering of global stakeholders in AI governance, in Paris. The summit followed the AI Safety Summit in the UK in 2023 and the AI Seoul Summit in 2024, yet ended without any meaningful deliverables. The United States and the United Kingdom declined to sign the final document, *Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet*, while China did. Most notably, the formal disappearance of the term "AI safety" from official summit documents signalled a fundamental shift: from efforts to establish governance for the responsible use of AI to an open race for global AI dominance. This change in tone and ambition comes at a critical moment. Just three weeks before the AI Summit convened in Paris, DeepSeek-R1 was released—a Chinese-developed large language model (LLM) with

performance rivalling GPT-4, yet reportedly trained with only a fraction of the computational resources and financial investment.

The rise of DeepSeek has redefined eligibility for AI competition. It revealed that the ability to develop cutting-edge generative AI is no longer exclusive to countries with access to the most advanced high-performance graphics processing units (GPUs), massive investment, and top-tier talent. By making its methods open source, DeepSeek effectively invited any state with a baseline of AI capacity to consider entering the global AI race. In response, the Trump administration issued an executive order on January 23, 2025, entitled Removing Barriers to American Leadership in Artificial Intelligence, directing federal agencies to submit action plans by July this year for securing US global dominance in AI (White House 2025). This development makes clear that competition over AI leadership has become central to strategic rivalry among great powers.

This article proceeds in three parts. First, it explains why DeepSeek matters and how the United States has responded, assessing whether this marks a Sputnik moment for AI competition. Second, to correctly gauge the significance of this competition, it explores how the military use of AI may transform the offense-defence balance in international security, drawing on recent scholarship and evolving national-security doctrines. Third, it considers the fundamental choice facing states in the region—between joining US-led efforts to restrict China's AI access and advancing sovereign AI development—and argues that middle powers in the Indo-Pacific must position themselves to balance innovation, autonomy, and strategic stability.

DeepSeek and the New Phase in the Global AI Race

The release of DeepSeek-R1 represents a profound disruption in the AI development landscape. Produced by a Chinese firm established in 2023, DeepSeek's model achieved performance on par with GPT-4 without access to NVIDIA chips or elite engineering teams in the US. This event, which many have described as an "AI Sputnik moment," shook the assumption that frontier AI models demand enormous computational capability, capital, and talent.

DeepSeek's innovation lies in its unique training approach. It employed large-scale reinforcement learning (RL) rather than traditional supervised fine-tuning. The initial model, DeepSeek-R1-Zero, was trained using rule-based reward functions and demonstrated emergent reasoning capabilities, such as self-verification and reflection. The firm later incorporated a small "cold start" dataset and adopted a three-stage training process—RL for reasoning, supervised fine-tuning for alignment, and a final RL pass to integrate safety and usability. Finally, it distilled its large model into compact versions with as few as 1.5 billion parameters (Guo et al. 2025).

The implications of its success are far-reaching. First, the DeepSeek case reveals the limits of US export controls. As analysts have noted, "export controls cannot kill innovation," and cutting off access to computer chips cannot fully block AI development due to black markets, cloud-based compute leasing, and the incentive structures created by scarcity (Villasenor 2025). Second,

it underscores the risks of over-relying on large technology firms for national AI leadership (Wheeler 2025). Third, it increases pressure on the United States to coordinate more closely with its allies to maintain technological superiority and prevent China from closing the gap (Shivakumar et al. 2024; Allen and Goldston 2025).

Despite the shock, DeepSeek has not fundamentally upset the US–China balance in AI. US firms still generally lead in six core areas: capital, talent, intellectual property, data, energy, and compute infrastructure (Lang et al. 2024). Yet the performance gap is narrowing. According to Stanford University's 2025 AI Index, China significantly reduced the benchmark performance gap between 2023 and 2024—on metrics such as multitask language understanding (MMLU) and math, the gap narrowed from double-digit margins to near parity.

Beyond demonstrating the limitations of export controls, DeepSeek also signals opportunity for non-US players. Its success could lower the barriers to entry for countries or organizations previously excluded from the frontier of AI due to resource constraints. French AI champion Mistral AI, for instance, welcomed the development and framed DeepSeek as "China's Mistral," highlighting the parallels between the two. But this apparent invitation to new competitors also raises risks. The race to develop smaller, faster models may incentivize companies to bypass essential safety protocols in pursuit of market advantage. Without international guardrails, the innovation race could devolve into a "race to the bottom" (Caroli 2025). The exclusion of the term "safety" from the official lexicon of the Paris AI Summit suggests that this race may have already begun.

The AI Race and Its Security Implications: The Rise of a New Cult of the Offensive

As the AI race intensifies, its most consequential impacts are likely to manifest in the realm of national security—where decisions concern not only strategic advantage, but the fundamental conditions of peace, war, and state survival.

In security studies, the offense-defence balance is a core structural variable that shapes the probability of war, alliance formation, and arms races. When offense dominates, crises escalate more easily; when defence prevails, stability is more likely (Jervis 1978). AI influences this balance not through a single mechanism, but through multiple, intersecting pathways. Its nature as a general-purpose, dual-use technology and "force multiplier" blurs the boundaries between civilian and military use. Militarily, AI is expected to accelerate the tempo of operations, enhance target identification, and increase the precision of strikes—amplifying overall combat effectiveness (Horowitz 2018; Johnson 2019; Bode et al. 2024).

Both Washington and Beijing are embedding AI into their national defence strategies—through "integrated deterrence" and "intelligentized warfare," respectively. In the US case, these frameworks envision a "seamless integration of capabilities" across domains, regions, and levels of conflict—and even among allied partners—with AI playing a central role in addressing joint capability gaps from the operational to the strategic level. Chinese strategic documents

"As the AI race intensifies, its most consequential impacts are likely to manifest in the realm of national security—where decisions concern not only strategic advantage, but the fundamental conditions of peace, war, and state survival."

articulate a similar concept, positioning AI as a foundational enabler of multidomain operations by facilitating cross-platform coordination (Ministry of Foreign Affairs of the People's Republic of China 2022; White House 2022; US Department of Defense 2023).

Three military domains exemplify how AI may transform future warfare: cyber operations, autonomous systems, and nuclear weapons.

In cyber operations, AI enhances both offensive and defensive capabilities. It enables stealthier and more adaptive cyber attacks, such as DeepLocker, while also improving intrusion detection and anomaly monitoring. However, efforts to strengthen systems by integrating cyber defenses across domains can inadvertently expand the "attack surface," introducing new vulnerabilities. As a result, the net effect of AI on the offense-defence balance in the cyber realm remains ambiguous (Jacobsen and Liebetrau 2023).

In autonomous weapons systems, AI lowers the cost of conflict and reduces reliance on human personnel. Systems like drone swarms and robotic combat platforms can be scaled rapidly, enabling one operator to control multiple assets. These capabilities may incentivize first-mover strategies and reduce the domestic political costs associated with human casualties. However, defenders may still hold an advantage in localized environments due to their familiarity with the terrain and superior contextual data—especially as large language models rely on dense, high-quality training datasets (King 2024; Schneider and Macdonald 2024).

In the upcoming era of the AI–nuclear nexus, technology enhances both first-strike and second-strike capabilities. AI improves intelligence, surveillance, and reconnaissance, enabling the detection of hidden nuclear forces and supporting precision counterforce targeting. AI-enabled electronic warfare may also paralyze command-and-control systems, producing non-kinetic effects with strategic equivalence. At the same time, AI strengthens early-warning systems, cyber defenses, and automated retaliatory protocols—such as Russia's "Dead Hand." This simultaneous enhancement of both first- and second-strike capabilities introduces strategic ambiguity, and it remains premature to conclude whether the introduction of AI will fundamentally disrupt the stability traditionally sustained by the logic of mutual assured destruction (Johnson 2023).

Thus, AI does not decisively tip the balance toward offense or defence. Instead, its effects are context-dependent and will evolve through action-reaction cycles of innovation. Yet a distorted perception is emerging among policymakers—a new "cult of the offensive." Enticed by AI's promise of speed, precision, and automation, decision-makers may prioritize efficiency over control, heightening the risk of inadvertent escalation. The resulting effectiveness-safety dilemma reflects a troubling trade-off: as military operations grow more effective, they may simultaneously become harder to regulate or halt.

Recent research highlights that this perception gap is driven by a self-reinforcing cycle of beliefs: ambiguous technological progress, coupled with rising expectations of conflict, reinforces elite assumptions about offensive dominance (Selden 2024). Drawing on US and Chinese leadership statements, strategy documents, military publications, and media discourse between 2014 and

2022, this study finds that both countries' elites increasingly view great-power war as inevitable. If this trend continues—while the objective effects of AI remain unclear—then policy-makers on both sides may behave as though AI creates an offense-dominant world. This recalls the pre-World War I security dilemma, where exaggerated confidence in offensive advantage led to catastrophic miscalculation (Van Evera 1984). The spectre of such strategic misjudgment suggests that the AI arms race may not just reshape warfare, but also tilt the world closer to great-power conflict.

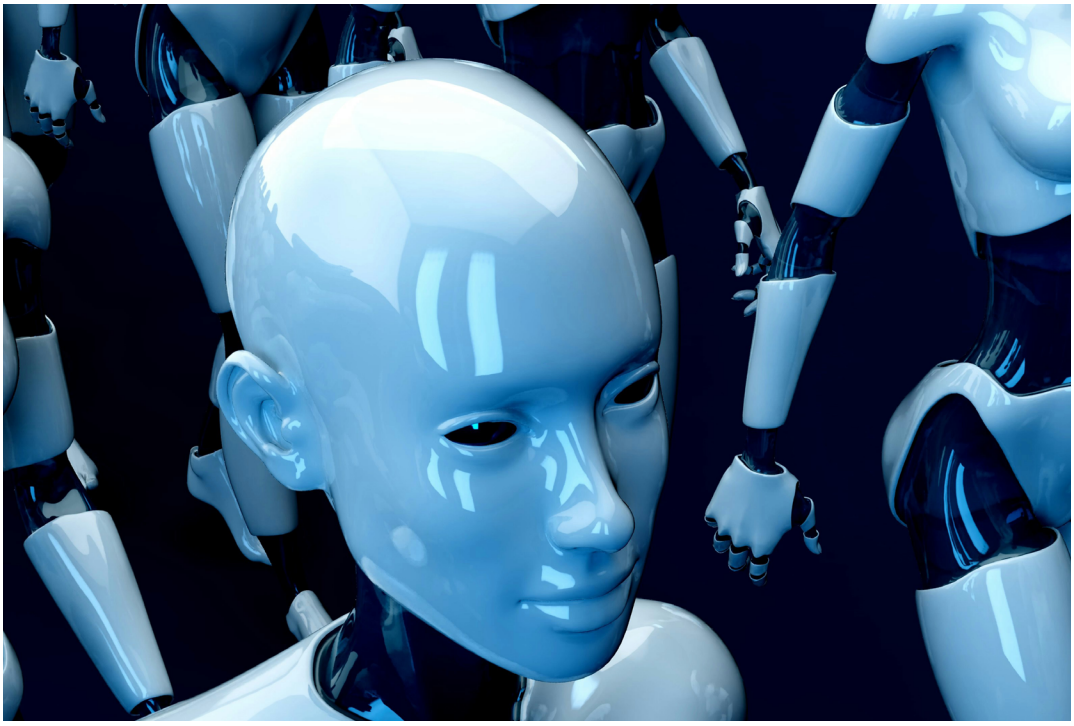

Photo by Julien Tromeur via Unsplash.

Two Futures for AI: Between Strategic Alignment and Sovereign Autonomy

As the global race for AI development accelerates, the world is approaching a strategic crossroads. One path aligns with the vision of the United States: restricting China's access to advanced AI components through strengthened export controls and developing a tighter, US-led technological ecosystem. The other path warns of the long-term risks associated with such restrictions—including the erosion of international collaboration, fragmentation of global innovation, deterioration of strategic trust, and, above all, diminished national autonomy in AI strategies and action plans. Both perspectives offer compelling arguments and raise urgent questions about the future of AI governance in the Indo-Pacific and beyond.

Advocates of the first pathway argue that limiting access to critical technologies is essential for preserving military advantage, preventing misuse, and maintaining a rules-based order—particularly given concerns about China's challenge to the current international system. From this perspective, alignment with the United States offers access to cutting-edge innovation,

enhanced security partnerships with the world's most capable military power, and safeguards against the authoritarian use of AI. Closer coordination among like-minded countries—through list-based controls, end-use monitoring, and services restrictions—could reinforce US-led efforts to constrain China's access to critical components (Shivakumar et al. 2024; Allen and Goldston 2025). In return, participating countries could expect greater support from Washington in developing their own AI ecosystems, particularly in terms of semiconductor access, computing infrastructure, and the cultivation of elite talent.

Critics, however, caution that these restrictions risk entrenching technological hegemony and deepening global divides. The rise of "sovereign AI" reflects not only a desire for strategic autonomy but also growing unease with exclusion and overdependence on US platforms. Open-source breakthroughs like DeepSeek-R1 show that states can circumvent traditional chokepoints long dominated by American firms. Over-reliance on coercive measures could accelerate the fragmentation of AI development into rival blocs—undermining cooperative frameworks for safety, interoperability, and inclusive innovation across both state and non-state stakeholders (Ray 2025; Wheeler 2025).

Rather than choosing between alignment and autonomy, many countries are pursuing a hybrid strategy—partially engaging in US-led initiatives while hedging by investing in homegrown AI capacity. Even the Indo-Pacific region's three pivotal US allies—South Korea, Japan, and Taiwan—are navigating this middle path. South Korea has committed to acquiring 10,000 GPUs to bolster national computing infrastructure. Japan is investing in projects like ABCI 3.0 and SB OpenAI Japan, as well as instituting regulatory frameworks tailored to specific sectors. Taiwan continues to support domestic models like FoxBrain, rooted in its advanced semiconductor base. For these and other regional actors, the core challenge is not only how to remain competitive, but how to prevent strategic competition from spiralling into technological decoupling and mistrust. Without a credible framework for transparency and restraint, the Indo-Pacific risks becoming a proving ground for digital blocs, exclusionary governance, and misperception-driven military escalation.

"Rather than choosing between alignment and autonomy, many countries are pursuing a hybrid strategy—partially engaging in US-led initiatives while hedging by investing in homegrown AI capacity."

At this juncture, regional actors—whether they are US allies or not—share a broader responsibility: to shape a future for AI that upholds both innovation and security. This means reinforcing global norms of transparency, resisting the erosion of cooperative guardrails, and ensuring that short-term advantage does not come at the cost of long-term peace. Framing the AI race purely as a zero-sum contest between the great powers risks overlooking the vital role middle powers can play as stabilizers, bridge-builders, and norm entrepreneurs in this emerging domain.

REFERENCES

Allen, Gregory C., and Isaac Goldston. 2025. "Understanding U.S. Allies' Current Legal Authority to Implement AI and Semiconductor Export Controls." Center for Strategic and International Studies, March 14. *https://www.csis.org/analysis/understanding-us-allies-current-legal-authority-implement-ai-and-semiconductor-export*.

Bode, Ingvild, Hendrik Huelss, Anna Nadibaidze, Guangyu Qiao-Franco, and Tom F. A. Watts. 2024. "Algorithmic Warfare: Taking Stock of a Research Programme." Global Society 38 (1): 1–23.

Caroli, Laura. 2025. "DeepSeek: A Problem or an Opportunity for Europe?" Center for Strategic and International Studies, February 14. *https://www.csis.org/analysis/deepseek-problem-or-opportunity-europe*.

Guo, Daya, et al. 2025. "DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning." ArXiv abs/2501.12948, submitted on January 22. *https://doi.org/10.48550/arXiv.2501.12948*.

Horowitz, Michael C. 2018. "Artificial Intelligence, International Competition, and the Balance of Power." Texas National Security Review 1 (3): 36–57.

Jacobsen, Jeppe T., and Tobias Liebetrau. 2023. "Artificial Intelligence and Military Superiority." In Artificial Intelligence and International Conflict in Cyberspace, edited by Fabio Cristiano, Dennis Broeders, François Delerue, Frédérick Douzet, and Aude Géry. Routledge.

Jervis, Robert. 1978. "Cooperation under the Security Dilemma." World Politics 30 (2): 167–214.

Johnson, James. 2019. "Artificial Intelligence & Future Warfare: Implications for International Security." Defense & Security Analysis 35 (2): 147–69.

Johnson, James. 2023. AI and the Bomb: Nuclear Strategy and Risk in the Digital Age. Oxford University Press.

King, Anthony. 2024. "Robot Wars: Autonomous Drone Swarms and the Battlefield of the Future." Journal of Strategic Studies 47(2): 185–213.

Lang, Nikolaus, Leonid Zhukov, David Zuluaga Martínez, Marc Gilbert, Meenal Pore, and Etienne Cavin. 2024. "How CEOs Can Navigate the New Geopolitics of GenAI." Boston Consulting Group, December 9. *https://www.bcg.com/publications/2024/how-ceos-navigate-new-geopolitics-of-genai*.

Ministry of Foreign Affairs of the People's Republic of China. 2022. "Report to the 20th National Congress of the Communist Party of China." October 16.

Ray, Trisha. 2025. "Sovereign Remedies: Between AI Autonomy and Control." Atlantic Council, April 3. *https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sovereign-remedies-between-ai-autonomy-and-control/*.

Schneider, Jacquelyn, and Julia Macdonald. 2024. "Looking Back to Look Forward: Autonomous Systems and the Importance of Cost." Journal of Strategic Studies 47 (2): 162–84.

Selden, Zachary. 2024. "A New 'Cult of the Offensive?' Elite Perceptions of Artificial Intelligence in Military Affairs." Foreign Policy Analysis 20 (4).

Shivakumar, Sujai, Charles Wessner, and Thomas Howell. 2024. "Balancing the Ledger: Export Controls and U.S. Chip Technology to China." Center for Strategic and International Studies, February 21. *https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china*.

Stanford Institute for Human-Centered AI. 2025. AI Index Report. Stanford University. *https://hai.stanford.edu/ai-index/2025-ai-index-report*.

US Department of Defense. 2023. "Data, Analytics, and Artificial Intelligence Adoption Strategy." July 27. *https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF*.

Van Evera, Stephen. 1984. "The Cult of the Offensive and the Origins of the First World War." International Security 9 (1): 58–107.

Villasenor, John. 2025. "DeepSeek Shows the Limits of US Export Controls on AI Chips." Brookings, January 29. *https://www.brookings.edu/articles/deepseek-shows-the-limits-of-us-export-controls-on-ai-chips/*.

Wheeler, Tom. 2025. "DeepSeek Is Not a Good Reason for Big Tech to Become More Powerful." Brookings, February 11. *https://www.brookings.edu/articles/deepseek-ai-big-tech-competition/*.

White House. 2022. "National Security Strategy." October 12. *https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf*.

White House. 2025. "Removing Barriers to American Leadership in Artificial Intelligence." January 23. *https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/*.

COUNCIL FOR SECURITY COOPERATION IN THE ASIA PACIFIC

Established in 1993, the Council for Security Cooperation in the Asia Pacific (CSCAP) is the premier Track Two organisation in the Asia Pacific region and counterpart to the Track One processes dealing with security issues, namely, the ASEAN Regional Forum (ARF), the East Asia Summit (EAS) and the ASEAN Defence Ministers Plus Forum. It provides an informal mechanism for scholars, officials and others in their private capacities to discuss political and security issues and challenges facing the region. It provides policy recommendations to various intergovernmental bodies, convenes regional and international meetings and establishes linkages with institutions and organisations in other parts of the world to exchange information, insights and experiences in the area of regional political-security cooperation. *www.cscap.org*

This is an individual paper of the 2025 Regional Security Outlook.

You can access the full version *here*.

LETTER FROM THE CO-EDITORS

On behalf of CSCAP, we are pleased to present the CSCAP Regional Security Outlook (CRSO) 2025. Inaugurated in 2007, the CRSO volume is now in its nineteentth year. The CRSO brings expert analysis to bear on critical security issues facing the region and points to policy-relevant alternatives for Track One (official) and Track Two (non-official) to advance multilateral regional security cooperation. The views in the CRSO 2025 do not represent those of any Member committee or other institutions and are the reseponsibility of the individual authors and the Editors. Charts and images in the CRSO 2025 do not necessarily reflect the views of the chapter authors.

Credits

Design: Prueksachat Kongthong

Cover and back image: Photo by Hartono Creative Studio via Unsplash

ISBN: 978-1-0694173-0-5

COUNCIL FOR
SECURITY COOPERATION
IN THE ASIA PACIFIC