BTTN Journal, Vol 4, Issue 2, December 2025 | PP. 1-38
Journal Homepage: https://bttn.org.pk/ojs/index.php/BTTN_Journal

BTTN Journal
p-ISSN 2958-1214
e-ISSN 2958-1222

RESEARCH ARTICLE

Unintended Beneficiaries of Military AI: How Third-Party States Reshape Strategic Stability

Cuihong Cai[1], Luyao Zhang[2]

Article Info

Article History:

Received: *October 15, 2025*

Revised: *November 30, 2025*

Accepted: *December 31, 2025*

Keywords:

Military AI, Third-Party Strategy, Dual-Use Technology, Strategic Stability, Artificial Intelligence

Abstract

While major powers such as the United States, China, and Russia are rapidly advancing military AI, with initiatives like NATO's AI Strategy shaping a new competitive landscape, this study examines a critical yet underexplored question: How do third-party states acquire strategic autonomy in the military AI era, and how their behavior reshapes strategic stability? Using a qualitative case study approach, this research employs a two-dimensional analytical framework characterized by technological capability foundation and strategic positioning choice to analyze strategic decisions across multiple third-party states. The study finds that four traits of military AI reshape their strategic options: its general-purpose nature lowers entry barriers across domains; dual-use ambiguity expands acquisition pathways; low marginal cost enables rapid capability diffusion; and data-dependency turns local datasets into critical absorptive assets. Together, these properties erode traditional great-power technology monopolies. Based on these features, five patterns of third-party behavior are emerging. The US allies, such as Japan and Australia, build interdependence through co-development and data sharing. Transfer recipients like Pakistan and the UAE localize AI by exploiting its general-purpose character. Hedgers such as Singapore and India diversify through flexible procurement of software-layer services. Chokepoint controllers, including the Netherlands and South Korea, gain influence via critical supply-chain roles. Autonomous developers like France pursue strategic independence. Overall, regarding strategic stability, third-party behavior creates dual effects: power decentralization enhances constraint mechanisms through supply chain interdependence, yet simultaneously introduces destabilizing forces such as compressed decision-making timelines. Military AI diffusion is facilitating a technology-driven, quasi-multipolar security order.

[1] Cuihong Cai is a professor of international relations at the Center for American Studies, Fudan University. Her research focuses on Sino–U.S. relations, cyber politics, digital strategy, and global technology governance. The author can be reached at chcai@fudan.edu.cn
[2] Ms Luyao Zhang, is a PhD. Candidate, at the School of International Relations and Public Affairs, Fudan University.

Introduction

Artificial intelligence is becoming the most disruptive military technology of the 21st century. Yet, this disruption manifests not merely in technological breakthroughs but more profoundly in its impact on the global distribution of power. In September 2020, a scene from the Nagorno-Karabakh conflict stunned international military observers: Turkish-made TB2 drones operated by Azerbaijan, coordinated with Israeli Harop loitering munitions, systematically destroyed Armenian Soviet-era air defense systems and armored forces[1]. During this conflict, drone swarms employing AI-driven target recognition, coordinated attacks, and real-time intelligence processing enabled a medium-sized military power to achieve overwhelming battlefield superiority at minimal cost. More notably, Turkey itself was not a traditional military-technological powerhouse. Its drone technology heavily relied on commercial off-the-shelf components, open-source algorithmic frameworks, and localized data accumulation through rapid battlefield iteration.

The Nagorno-Karabakh war was not an isolated case. On the 2022 Ukrainian battlefield, inexpensive commercial quadcopter drones equipped with simple AI visual recognition systems provided defenders with unprecedented battlefield transparency.[2] During the 2023-2024 Red Sea crisis, Yemen’s Houthi forces used low-cost drones and unmanned boats to attack commercial and military ships, compelling the US Navy to deploy expensive Aegis systems for interception, creating a cost asymmetry.[3] These cases collectively point to a

[1] Davit Khachatryan, “Beyond the Drone Hype: Unpacking Nagorno-Karabakh’s Real Lessons,” EVN Report, March 27, 2024, https://evnreport.com/opinion/beyond-the-drone-hype-unpacking-nagorno-karabakhs-real-lessons/.
[2] David Kirichenko, “The Rush for AI-Enabled Drones on Ukrainian Battlefields,” *Lawfare*, December 5, 2024, https://www.lawfaremedia.org/article/the-rush-for-ai-enabled-drones-on-ukrainian-battlefields.
[3] Lara Seligman and Matt Berg, “A $2M Missile vs. a $2,000 Drone: Pentagon Worried over Cost of Houthi Attacks,” *POLITICO*, December 19, 2023, https://www.politico.com/news/2023/12/19/us-missile-houthi-attacks-00131730.

reality long underestimated by academia: the militarization of artificial intelligence is opening an unprecedented strategic window of opportunity for third-party states, with implications far exceeding the historical experience of traditional technology diffusion.

Meanwhile, the AI arms race among major powers is accelerating at full speed. The US Department of Defense established the Joint Artificial Intelligence Center (JAIC) in 2018, which was reorganized into the Chief Digital and Artificial Intelligence Office (CDAO) in 2022, and released the DoD AI Strategy in 2022, designating AI as a game-changing technology for military applications[4]. NATO adopted its first Artificial Intelligence Strategy on October 22, 2021, during the Brussels Defence Ministers Meeting, emphasizing collective capability building in command and control, autonomy, cyber defence, and related domains through responsible adoption principles[5]. Russia, despite gaps in computing power and algorithms, has demonstrated its determination to catch up through projects such as the AI guidance system for the Kinzhal hypersonic missile and the S-70 Okhotnik unmanned combat aircraft.

Beneath the surface of this great power competition, a more profound structural transformation is occurring: the speed, pathways, and consequences of technology diffusion are fundamentally changing. Unlike the nuclear age, with its strict controls over uranium enrichment facilities and plutonium reactors, and unlike precision-guided weapons that relied on complex industrial

[4] Department of Defense, *Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington, DC: US Department of Defence, 2019), https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF; Department of Defense, *Data, Analytics, and Artificial Intelligence Adoption Strategy* (Washington, DC: US Department of Defense, 2023), https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

[5] North Atlantic Treaty Organization, *Summary of the NATO Artificial Intelligence Strategy* (North Atlantic Treaty Organization, 2021), https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

systems for linear diffusion, the spread of military AI technology exhibits new characteristics: multi-sourced, rapid, and difficult to control. The free flow of open-source algorithms on GitHub and arXiv, the dual-use attributes of commercial chips and cloud computing services, and the global supply chains of civilian technology giants have collectively created an unprecedented ecosystem for technology acquisition. More critically, the four distinctive attributes of AI technology, as a general-purpose nature, dual-use ambiguity, low marginal cost, and data dependency, are systematically lowering technological barriers, enabling third-party states to participate in this technological revolution at lower costs, faster speeds, and through more diversified pathways.

Although the militarization of AI has become a prominent topic in international relations scholarship, existing research exhibits a significant bias towards great power centrism[6]. Mainstream literature focuses on the strategic competition between China and the United States, the impact of AI on nuclear deterrence stability, and the ethical dilemmas of autonomous weapon systems. Yet, it rarely systematically examines how third-party states benefit from this technological revolution and how such benefits, in turn, reshape the global strategic landscape. Furthermore, international relations research has long treated technology diffusion as an externality or byproduct of great power competition rather than as a structural variable with independent explanatory

[6] Ingvild Bode, "AI Technologies and International Relations: Do We Need New Analytical Frameworks?," *The RUSI Journal*, Vol. 169, No. 5 (2024), pp. 66–74; Liu Shengxiang and Li Zhihao, "Artificial Intelligence in U.S. Military Strategy: Trends and lmpact," *Global Review,* Vol. 16, No. 3 (2024), pp. 51-73+155-156, https://doi.org/10.13851/j.cnki.gjzw.202403004; Eric Lofgren, Whitney M. McNamara, and Peter Modigliani, *Atlantic Council Commission on Defense Innovation Adoption Interim Report,* (Atlantic Council, 2023), https://www.atlanticcouncil.org/in-depth-research-reports/report/atlantic-council-commission-on-defense-innovation-adoption-interim-report/; Matthijs M. Maas, "How Viable Is International Arms Control for Military Artificial Intelligence? Three Lessons from Nuclear Weapons," *Contemporary Security Policy,* Vol. 40, No. 3 (2019), pp. 285–311, https://doi.org/10.1080/13523260.2019.1576464.

power[7]. Third-party states are reduced to technology recipients or market actors, and their strategic choices are viewed as passive responses to major-power policies. This perspective cannot explain: why, facing similar conditions of technology supply, Japan chooses deep integration into the US system while India insists on a hedging strategy of multi-source procurement; why a small country like the Netherlands can obtain disproportionate bargaining power in the Sino-American technological competition; why France persists in advancing the FCAS project despite knowing the technological gap is substantial. Clearly, third-party states are not simple recipients but strategic actors with agency, whose choices are shaped by multiple factors, including national scale, technological foundation, geopolitical environment, historical path, and strategic culture.

Based on these observations, the study employs a qualitative case study approach to examine the strategic choices of third-party states in military AI diffusion and attempts to answer three interrelated core questions: First, why is the diffusion pattern of military technology in the AI era fundamentally different from the diffusion of traditional strategic weapons such as nuclear weapons and missile technology? Second, how do third-party states positioned at the margins of great power competition transform apparent technological disadvantages into strategic assets? Third, will this extensive and rapid diffusion of technology stabilize or destabilize the existing strategic equilibrium?

Theoretical Framework: The Disruptive Attributes of Military AI Technology

Understanding the strategic opportunities available to third-party states in the process of AI militarization requires first clarifying the unique attributes that

[7] Jeffrey Ding, *Technology and the Rise of Great Powers: How Diffusion Shapes Economic Competition*, (Princeton University Press, 2024).

distinguish AI technology from traditional strategic weapons. The history of nuclear proliferation provides a valuable point of comparison. A series of complex technical barriers, including uranium enrichment, reactor construction, and precision manufacturing capabilities, has constrained nuclear diffusion[8]. Even today, fewer than ten countries possess complete nuclear weapons manufacturing capability. The diffusion of precision-guided weapons, while faster than nuclear weapons, still requires a complete industrial system, from inertial navigation systems to terminal guidance technology, with each component presenting a technical threshold[9]. However, military AI technology is rewriting this logic of diffusion. This chapter systematically explains the four primary distinctive attributes of AI technology: general-purpose nature, dual-use ambiguity, low marginal cost, and data dependency. It is the combinatorial effect of these attributes that enables third-party states to acquire strategic capabilities in unique ways.

General-Purpose Nature

The first disruptive attribute of military AI technology lies in its general-purpose nature. Unlike the highly specialized characteristics of traditional weapon systems, deep learning algorithm frameworks exhibit significant cross-domain transferability. PyTorch and TensorFlow, the two mainstream frameworks, were initially developed for civilian applications such as image recognition and natural language processing, yet can be directly applied to military scenarios, including drone target recognition, radar signal processing, and battlefield situational awareness. This general-purpose nature stems from the underlying logic of deep learning. The way convolutional neural networks process image

[8] Robert Jervis, “Why Nuclear Superiority Doesn’t Matter,” *Political Science Quarterly,* Vol. 94, No. 4 (1979), pp. 617–33, https://doi.org/10.2307/2149629.
[9] National Research Council, *Dual-Use Technologies and Export Control in the Post-Cold War Era* (Washigton, DC: National Academies Press, 1994).

data, the mechanisms by which recurrent neural networks model sequential information, and the principles of attention allocation in Transformer architectures are fundamentally independent of specific application domains. Once a country masters these foundational frameworks, it can apply them relatively easily across different military fields.

The strategic implication of this general-purpose nature is a systematic lowering of technical barriers. In the AI era, the same algorithm framework could simultaneously support multiple military applications[10]. In contrast, the specialized characteristics of traditional military technology constitute insurmountable barriers. Nuclear weapons technology involves four independent technical chains: uranium enrichment, plutonium production, implosion lens design, and delivery vehicles, each requiring specialized research teams and industrial facilities[11]. Even if a country masters nuclear material production technology, it still needs to tackle warhead miniaturization and missile technology separately. Precision-guided weapons are similar.

From inertial navigation to GPS reception, from infrared seekers to semi-active radar guidance, the technical principles of different guidance methods differ fundamentally, making technology reuse difficult. This specialization causes technology diffusion to exhibit significant domain segmentation, where breakthroughs in one military field are difficult to translate rapidly into capabilities in other fields. But AI technology breaks this constraint. After the UAE imported drone technology from Turkey and China, its local EDGE Group rapidly applied the acquired AI algorithms to ground robots, maritime patrol

[10] Adib Bin Rashid, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, and Mehedy Hassan Bappy, “Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges,” *International Journal of Intelligent Systems* Vol. 2023 (November 2023), pp. 1-31, https://doi.org/10.1155/2023/8676366.

[11] Koichi ARIE, “New Domains and Nuclear Weapons Systems: The Implications for Nuclear Deterrence and Arms Control,” in *Nuclear Weapons in the 21st Century*, ed. Sukeyuki ICHIMASA (National Institute for Defense Studies, 2024), https://www.nids.mod.go.jp/english/publication/perspectives/e2024.html.

boats, and urban air defense systems, forming a full-spectrum unmanned combat capability [12]. This cross-domain transfer capability enables an exponential increase in technology return on investment for third-party states.

Dual-Use Ambiguity

The second unique attribute of military AI technology is its high degree of dual-use ambiguity. This dual-use nature differs from the traditional concept of dual-use technology. While GPS systems can be used for both civilian and military purposes, there is a clear distinction in precision levels between the two, with military signals encrypted and strictly controlled. But the dual-use nature of AI technology manifests as a more profound boundary ambiguity. Training a target recognition algorithm uses the same deep learning framework, similar data annotation methods, and universal computing chips [13]. An object detection model designed for autonomous vehicles can be applied to battlefield target recognition for drones after minimal data retraining. This technological isomorphism poses fundamental challenges to traditional export control mechanisms.

This dual-use ambiguity manifests at multiple levels. At the algorithmic level, open-source communities such as GitHub host tens of thousands of deep learning projects, ranging from image classification and semantic segmentation to object tracking and path planning. These codes are civilian research outputs, but with slight modifications, can be used for military purposes. At the hardware level, commercial GPU chips are the preferred choice for both gamers and the core computing power source for training military AI models. NVIDIA A100 and H100 chips were initially designed for data centers and scientific

[12] Staff Writer With AFP, "UAE Invests in Drones, Robots as Unmanned Warfare Takes Off," February 23, 2022, https://thedefensepost.com/2022/02/23/uae-drones-robots/.
[13] Judith Reppy, "Managing Dual-Use Technology in an Age of Uncertainty," *The Forum,* Vol. 4, No. 1 (2006), p. 1, https://doi.org/10.2202/1540-8884.1116.

computing, but are equally suitable for training drone swarm coordination algorithms or missile interception systems[14]. The proliferation of cloud computing services further amplifies this dual-use nature. A small country does not need to build its own supercomputing center but can rent computing power through Amazon AWS, Microsoft Azure, or Google Cloud to train military models[15]. While cloud service providers claim to review user purposes, it is technically challenging to distinguish whether an image classification task is for medical diagnosis or military reconnaissance.

The strategic consequence of this dual-use ambiguity is the systematic failure of traditional export control mechanisms. The Wassenaar Arrangement, established during the Cold War, targets physical products and clearly defined technical parameters. For a high-precision machine tool or laser operating at a specific wavelength, it can be determined whether it falls within the controlled scope by examining its physical specifications. But maintaining a piece of Python code or a pre-trained model is technically nearly impossible. The intangibility and ease of replication of software make border inspections and end-user verification meaningless. In 2020, the US Commerce Department attempted to include certain geographic image analysis software in export controls.[16]But within a year, this was effectively abandoned due to the inability to enforce.

---

[14] Klas Government Inc., "Graphics Processing Unit (GPU) to Bring Artificial Intelligence (AI) to the Tactical Edge Introduced by Klas," *Military & Aerospace Electronics*, June 15, 2021, https://www.militaryaerospace.com/computers/article/14205885/graphics-processing-unit-gpu-to-bring-artificial-intelligence-ai-to-the-tactical-edge-introduced-by-klas.

[15] Mohd Nadeem et al., "Identification of Security Factors in Cloud Computing: Defence Security Perspective," Computational Intelligence Applications in Cyber Security, 1st ed. (CRC Press, 2024).

[16] Bureau of Industry and Security, *Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series*, Interim Final Rule Docket No. 191217-0116, RIN 0694-AH89 (U.S. Department of Commerce, 2020), pp. 85:459–61, https://www.federalregister.gov/documents/2020/01/06/2019-27649/addition-of-software-specially-designed-to-automate-the-analysis-of-geospatial-imagery-to-the-export.

Low Marginal Cost

The third distinctive attribute of AI technology is its extremely low marginal cost of replication and deployment. This characteristic fundamentally differs from the cost structure of traditional military technology. The replication of AI software is essentially cost-free. Once a deep learning model is trained, deploying it to thousands of drones or command systems requires only copying the code and loading model parameters. The computation required for inference is orders of magnitude lower than that needed for training. This means that once an AI capability is developed, its widespread dissemination faces almost no economic barriers.

The more profound impact is that low marginal cost changes the economics of arms races. Traditional arms races are wars of attrition, with major powers relying on robust finances and industrial bases to gradually accumulate advantages. But in the AI era, latecomer countries can rapidly catch up through algorithm replication. When the United States invests massive resources in developing next-generation drone-swarm coordination algorithms, adversaries can deploy similar capabilities once they obtain the research results. This asymmetry has long been evident in cybersecurity.

Low marginal cost also changes the sustainability of technological monopoly. In traditional domains, technological leaders can maintain advantages by controlling key manufacturing facilities, rare-material supply chains, or core-component exports. But AI capability is essentially algorithms and data; once this information is acquired, it cannot be retrieved. Unlike production lines that can be physically destroyed or key components that can be embargoed, disseminated algorithms cannot be recalled. Even if original developers discover technology leakage and develop next-generation algorithms, already-disseminated old versions retain their combat value. More critically, the cost of incremental improvements based on old versions is far lower than creating from scratch, causing technological catch-up to exhibit accelerating rather than decelerating trends.

Therefore, low marginal cost is not merely a techno-economic phenomenon but represents the dissolution of a strategic equilibrium mechanism. Massive R&D investments can no longer ensure durable capability advantages, as such benefits can be offset by low-cost replication. The strategic value of technological leadership shifts from sustained control to a temporary window, with the duration of this window determined by the fragility of information security rather than by gaps in economic and industrial capacity.

Data Dependency

The fourth distinctive attribute of military AI technology is its high dependency on data, a characteristic that may paradoxically become a strategic asset for third-party states. This data dependency manifests across multiple dimensions. In terms of geographic environmental data, every region has unique terrain, climate, and vegetation. Singapore's urban counter-drone system needs to accurately identify small targets in densely built environments, which are markedly different from US training data in open terrain. The Singapore Defence Science and Technology Agency invested substantial resources to collect drone flight data in its own urban environment, enabling the training of AI models adapted to local combat scenarios[17]. This data is a valuable asset for Singapore but of limited value to other countries, because Singapore's special urban structure and climatic conditions are difficult to replicate elsewhere. Adversary behavior data is another critical dimension. AI-driven tactical

[17]Bryan Ng et al., "From Robot Dogs to Special Drones, SAF Tests Unmanned Platforms in US Exercise," *The Straits Times*, September 25, 2023, https://www.straitstimes.com/singapore/military/from-robot-dogs-to-special-drones-saf-tests-unmanned-platforms-in-us-exercise.

decision systems need to learn enemy tactical patterns, weapon characteristics, and response strategies. The UAE's large-scale drone operations in Yemen and Libya conflicts cover how to maintain communications in electronic jamming environments, how to identify camouflaged armed personnel, and how to conduct precision strikes in densely populated areas. When these experiences are encoded into AI algorithms, they become a unique component of the UAE military capability.

This data dependency breaks traditional technological dependency relationships. In the nuclear weapons or precision-guided weapons era, technology recipient countries were utterly dependent on technology supplier countries, because the latter held core technology and production capabilities. But in the AI era, technology transfer became a more equal relationship. While third-party countries obtain basic algorithms and hardware platforms from major powers, major powers equally need third-party countries' localized data to improve their own technology.

Five Strategic Models of Third-Party Countries Based on Technological Capability and Strategic Positioning

Traditional theories of military technology diffusion have long focused on technological competition and transfer controls between major powers. In *"The Diffusion of Military Power*," Horowitz proposed an adoption-capacity theory arguing that the adoption of military innovations depends on two key factors: financial resources and organizational capacity. According to this logic, technology diffusion follows a linear path from innovators to early adopters to latecomer states, with major powers maintaining technological leadership through resource advantages[18]. However, when we turn our attention to military

[18] Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton University Press, 2010), pp. 30–64, http://www.jstor.org/stable/j.ctt7sqwd.

AI technology, this explanatory framework begins to reveal structural limitations. The general-purpose nature, dual-use attributes, low marginal costs, and data dependence of AI technology are fundamentally reshaping the logic of technology diffusion and challenging the traditional mechanisms that sustain major-power technology monopolies.

So, the core problem facing third-party states in AI military technology competition is how to achieve strategic autonomy amid the gap between major-power technological competition. This involves three dimensions of power. First are technology acquisition rights, namely, whether they can break through major power technology blockades to obtain advanced AI capabilities through legal or gray channels. Second is technology shaping rights, namely, whether they can participate in setting technical standards and governance rules, influencing the direction of the international AI arms control agenda. Third is technology leverage rights, namely, whether they can establish irreplaceability in the technology ecosystem to constrain major power behavior. To systematically analyze the strategic choices of third-party states, this study proposes a two-dimensional analytical framework. The first dimension is the technological capability foundation, which refers to a country’s capability positioning in the AI military technology ecosystem, ranging from complete dependence on external supply to controlling key nodes to pursuing full-chain autonomy. The second dimension is strategic positioning, which refers to a country's geopolitical alignment with major powers, ranging from high alignment with a single major power to maintaining a flexible balance in the competitive landscape to pursuing complete strategic independence. The intersection of these two dimensions constitutes a continuous strategic spectrum, with different countries seeking optimal positions on this spectrum based on their own conditions and environmental constraints.

This framework reveals five main patterns of third-party state strategic choices in the AI era:

Table 1. Spectrum Framework for Third-Party State AI Military Technology Strategies

	Low Technological Capability Foundation	**Medium Technological Capability Foundation**	**High Technological Capability Foundation**
High Alignment Position		**Allied Strategy**: Japan, Australia	
Flexible Balance Position	**Transfer Strategy**: Pakistan, UAE	**Hedging Strategy**: Singapore, India; **Chokepoint Strategy**: Netherlands, South Korea	
Independent Autonomy Position			**Autonomous Strategy**: France, Germany

As shown in Table 1, the unique attributes of AI technology mean that third-party state strategic choices are no longer simple binary oppositions but continuous choice spaces across two dimensions: technological capability foundation and strategic positioning choice. Allied states can establish relatively independent technological capabilities while maintaining alignment, transfer states can flexibly acquire advanced technology while avoiding complete dependence, hedging states gradually enhance system integration capabilities through diversified procurement, chokepoint states gain extraordinary leverage through supply chain monopolies, and autonomous states achieve collective autonomy through regional cooperation under limited resources. Different strategic choices reflect different trade-offs between costs and benefits, risks and opportunities, which are deeply rooted in each country's historical experience, geopolitical environment, resource endowments, and value orientations.

Allied Strategy: Japan and Australia

The allied strategy represents a path of pursuing limited autonomy within a highly aligned framework. These countries choose to deeply embed themselves in alliance systems dominated by major powers, establishing their capability nodes within technical networks through joint research and development, data sharing, and specialized division of labor. Japan, with its expertise in sensors and precision manufacturing, and Australia, relying on Indo-Pacific data resources and strategic position, enable them to develop technological cooperation with the United States, becoming indispensable partners. Alliance relationships have acquired new meanings in the era of AI military technology. Traditional security alliances mainly revolved around deterrence commitments and military protection, while technology alliances shift focus to joint development, data sharing, and capability complementarity.

Japan, AI, and three levels of institutionalized cooperation

First is the Defense Innovation Technology Research Institute established following the model of the US Defense Advanced Research Projects Agency

(DARPA). Officially operational in October 2024, this organization has a budget of approximately $140 million and 100 personnel, half of whom are from private companies and universities, focusing on frontier technologies, including artificial intelligence, robotics, and autonomous systems[19]. Research priorities include developing unmanned vehicles capable of autonomous navigation in complete darkness and new underwater surveillance technologies for submarine detection. While this organizational structure design clearly borrows from the DARPA model, its substantive significance lies in Japan's creation of a more symmetrical negotiation foundation for technological cooperation with the US by establishing an equivalent institutional platform.

Second is the balanced consideration in the joint development of fighter jets. Japan initially selected Lockheed Martin as the integration support partner for the F-X fighter project, hoping to leverage its experience in stealth technology. However, the coordination process encountered major difficulties. Lockheed Martin was reserved about sharing key stealth technologies, touching upon Japan's core concerns about pursuing technological autonomy. In 2022, Japan turned to cooperation with Britain’s BAE Systems, finally announcing in December of that year joint advancement of the Global Combat Air Programme with Britain and Italy, merging the original F-X project with Britain’s Tempest fighter and Italy’s next-generation fighter projects[20]. This turning point reveals the internal tension of allied strategy: even among the closest allies, when it comes to core technology transfer, the United States still sets strict limits. Japan had to seek alternative paths for technology acquisition outside the US-dominated framework by expanding cooperation partners.

[19] DSEI Japan Executive Committee, “Japan Is Rethinking Defence Technology (and Why It Matters),” *DSEI Japan*, April 7, 2025, https://www.dsei-japan.com/news/japan-rethinking-defence-technology-matters.
[20] Kosuke Takahashi, “Why Japan Chose Britain and Italy for Its F-x Fighter Program,” *The Diplomat*, December 9, 2022, https://thediplomat.com/2022/12/why-japan-chose-britain-and-italy-for-its-f-x-fighter-program/.

Third is institutional construction in data-sharing legal frameworks. Japan revised information security-related laws, establishing legal foundations for the sharing of sensitive data with the United States and other allies[21]. However, as a non-Five Eyes member, Japan still faces institutional restrictions in accessing the highest-level intelligence. Although Tokyo maintains close intelligence exchanges with Five Eyes countries on specific issues, this cooperation is temporary and issue-oriented, lacking institutionalized long-term mechanisms. When AI system training requires integrating sensitive data from multiple countries, Japan's exclusion severely limits the depth of joint development. This situation highlights the structural dilemma of allied strategy: deepening technological cooperation requires institutionalized information sharing, but existing intelligence alliance systems set insurmountable thresholds for this.

Australia's specific projects under the AUKUS framework

In AI underwater warfare capability building, Australia is not only a technology recipient but also demonstrates technological contribution capability in specific domains. The MQ-28 Ghost Bat project represents Australia's breakthrough progress in autonomous systems. This unmanned combat aerial vehicle, jointly developed by Boeing Australia and the Royal Australian Air Force, integrates artificial intelligence technology and can operate cooperatively with manned aircraft.[22] As of 2024, eight first-batch prototypes have been built, with over 100 hours of flight testing completed. The Australian Government has committed over AUD 6 billion to the MQ-4C Triton program and plans to acquire 13 of these high-altitude, long-endurance unmanned aircraft. The first aircraft was delivered in 2024, with the whole fleet expected to be operational

[21] International Comparative Legal Guides, "Cybersecurity Laws and Regulations Japan 2025," November 6, 2024, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan.
[22] Boeing, "MQ-28 Ghost Bat: Uncrewed Collaborative Combat Aircraft," 2025, https://www.boeing.com/defense/mq-28.

by the late 2020s, enhancing maritime domain awareness in the Indo-Pacific in partnership with the United States[23].

The significance of the Ghost Bat project lies not only in its technological breakthrough but also in the collaborative model it demonstrates. Boeing Australia, the Australian Defence Science and Technology Group, and the U.S. Air Force Research Laboratory jointly develop the project's underlying software[24]. This trilateral cooperation mechanism ensures technology sharing while giving Australia a voice at the algorithm level. In 2025 testing, the Ghost Bat successfully executed missions under the control of an E-7 Airborne Early Warning and Control aircraft, validating the feasibility of manned-unmanned teaming operations. Australia plans to conduct live-fire testing of air-to-air missiles by the end of 2025, transforming the Ghost Bat from a reconnaissance platform into a genuine combat platform[25]. The US Air Force and Navy have shown strong interest in the project, acquiring at least one aircraft to support unmanned aircraft research, reflecting the bidirectional nature of technology flow: capabilities developed by allies can also feed back into US military forces.

Australia's efforts to participate in the US Department of Defense's Joint All-Domain Command and Control (JADC2) system reveal another dimension of the alliance-type strategy. JADC2 requires allied nations' data infrastructure to achieve seamless integration with US military systems, meaning Australia must not only share data but also reform its domestic data collection, storage, and

[23] Australian Department of Defence, "Australia's First MQ-4C Triton," July 31, 2024, https://www.minister.defence.gov.au/media-releases/2024-07-31/australias-first-mq-4c-triton.
[24] Army Recognition, "Australia Conducts First Flight of MQ-28A Ghost Bat Drone to Validate Mission Readiness beyond Test Range Limits," *Army Recognition*, June 24, 2025, https://armyrecognition.com/news/aerospace-news/2025/australia-conducts-first-flight-of-mq-28a-ghost-bat-drone-to-validate-mission-readiness-beyond-test-range-limits.
[25] Aaron Mehta and Michael Marrow, "Australia's Ghost Bat Eyes Live Air-to-Air Weapons Test by End of Year," *Breaking Defense*, March 25, 2025, https://breakingdefense.com/2025/03/australias-ghost-bat-eyes-live-air-to-air-weapons-test-by-end-of-year/.

processing systems according to US standards. This deep integration enhances interoperability but also raises concerns about data sovereignty. Once Australia's military data infrastructure is fully integrated with US systems, to what extent can Canberra maintain independent control over its own data? This question becomes increasingly real as technical alliances deepen, yet a satisfactory answer has yet to be found.

Transfer Strategy: Pakistan and the UAE

The transfer strategy represents a pragmatic path to rapidly build military AI capabilities through flexible technology procurement and localized adaptation. Unlike the allied strategy's deep integration, the transfer strategy countries maintain greater flexibility in technology sourcing, avoiding complete lock-in to any single major power's technology ecosystem. The core logic lies in leveraging the competition among major power technology suppliers to obtain advanced capabilities at lower costs and with looser political conditions.

Pakistan: China-Pakistan Drone Cooperation

Pakistan represents a typical case of a transfer strategy. Facing traditional US technology restrictions and budgetary constraints, Pakistan turned to China for advanced drone technology. This cooperation began in the early 2010s and has achieved significant results by the 2020s. The core of China-Pakistan drone cooperation centers on the Chinese-made CH-series and Wing Loong series unmanned systems. The Pakistan Air Force procured 5 CH-4 combat drones in January 2021, followed by an additional 10 units in May 2024. SIPRI data shows that between 2008 and 2018, China exported 14% of its combat/strike-capable drones to Pakistan, encompassing both the CH-series and Wing Loong family, which remain central to this bilateral partnership[26]. What's more significant is that Pakistan is not merely purchasing finished products but pursuing localized production and capability building. In 2018, Pakistan and China signed an agreement to co-produce the Wing Loong II drone at the Pakistan Aeronautical Complex (PAC) in Kamra, which established a dedicated assembly and testing line for this system[27].

This localization strategy has yielded practical results. Pakistan used Chinese-made drones extensively in counterterrorism operations in border regions, accumulating valuable operational data. This data was used to train AI systems for Pakistan's specific operational environment, improving target recognition accuracy and mission success rates. For instance, identifying targets in mountainous terrain differs significantly from that in desert environments, and Pakistan's locally trained models perform better than the original Chinese systems in this context. Pakistan has attempted to further enhance autonomy by expanding cooperation partners. Besides China, Pakistan maintains military technology cooperation with Turkey, particularly in drone technology. Pakistan procured Turkey's Anka drones and explored joint development opportunities[28]. This diversified sourcing strategy aims to avoid excessive dependence on any single supplier while leveraging competition among suppliers to gain better terms.

[26] Abhishek Kumar Darbey, "China's Increasing Global Drone Footprint – Analysis," *Eurasia Review*, November 24, 2024, https://www.eurasiareview.com/24112024-chinas-increasing-global-drone-footprint-analysis/.
[27] Franz-Stefan Gady, "China, Pakistan to Co-Produce 48 Strike-Capable Wing Loong II Drones," *The Diplomat*, October 9, 2018, https://thediplomat.com/2018/10/china-pakistan-to-co-produce-48-strike-capable-wing-loong-ii-drones/.
[28] Inder Singh Bisht, "Pakistan, Turkey to Co-Produce Anka Combat Drones," *The Defense Post*, August 24, 2021, https://thedefensepost.com/2021/08/24/pakistan-turkey-anka-drones/.

UAE: From Technology Recipient to Regional Integration Hub

The UAE's transfer strategy is more ambitious, aiming to transform from a pure technology recipient into a regional technology integration center. Leveraging abundant financial resources and strategic positioning, the UAE is rapidly building comprehensive AI military capabilities through large-scale technology procurement and industrial investment.

In 2019, the UAE established EDGE Group, integrating domestic defense enterprises to form a comprehensive defense technology conglomerate[29]. EDGE actively absorbs foreign technology through cooperation with international partners while promoting indigenous innovation. The UAE is also building an AI research and development ecosystem. It has established the Mohamed bin Zayed University of Artificial Intelligence (MBZUAI), recruiting internationally renowned scholars to conduct cutting-edge research. Although this university currently focuses on civilian AI, the boundary between civilian and military technology is blurred, and research results can be quickly applied to military domains.

Through these efforts, the UAE is transforming its role. It is no longer merely a buyer of weapons but an integrator and re-exporter of technology. The UAE companies are exporting drones and surveillance systems to other Middle Eastern and African countries, becoming regional technology suppliers. This transformation enhances the UAE's strategic value, no longer simply dependent on major-power technology provision but capable of establishing a certain irreplaceability within the regional security architecture.

[29] Agnes Helou, "UAE Launches 'Edge' Conglomerate to Address Its 'Antiquated Military Industry,'" *Defense News*, November 6, 2019, https://www.defensenews.com/global/mideast-africa/2019/11/06/uae-launches-edge-conglomerate-to-address-its-antiquated-military-industry/.

Hedging Strategy: Singapore and India

The hedging strategy seeks to maintain maximum strategic flexibility in major power competition. Its core logic is to avoid complete dependence on any single major power through diversified technology sourcing, while preserving diplomatic and strategic maneuvering room during geopolitical shifts. This strategy is particularly suited for countries positioned in geopolitically sensitive regions, facing security threats from multiple directions, but reluctant to fully choose sides in major power competition.

Singapore: Comprehensive Multi-Source Technology Strategy

Singapore's hedging strategy is reflected in its comprehensive multi-source technology procurement and flexible diplomatic positioning. As a small city-state, Singapore faces complex security challenges but maintains economic ties with both major powers, making hedging its optimal choice. In military procurement, Singapore maintains close cooperation with the United States while not excluding other suppliers. Singapore will receive its first F-35 stealth fighters in 2026, with an initial batch of four F-35Bs marking the Republic of Singapore Air Force's entry into fifth-generation airpower. The city-state has committed to a total of 20 aircraft (12 F-35Bs and 8 F-35As), with full deliveries extending to 2030[30]. This demonstrates Singapore's deep alignment with the US technology system. However, Singapore simultaneously cooperates with France on autonomous aerial refueling technology, explores anti-drone systems

[30] Sebastian Strangio, "Singapore's First F-35 Fighter Set for Delivery by End of 2026, Defense Minister Says," *The Diplomat*, September 15, 2025, https://thediplomat.com/2025/09/singapores-first-f-35-fighter-set-for-delivery-by-end-of-2026-defense-minister-says/.

with Israel, and even engages with Chinese enterprises on dual-use technology exchanges[31].

Singapore's hedging strategy is particularly evident in AI and unmanned systems. Singapore actively participates in U.S.-led technology alliances but maintains an independent attitude in domestic AI development. Singapore's Defense Science and Technology Agency established AI Labs to research autonomous systems, swarm intelligence, and human-machine collaboration. Singapore also builds domestic AI research capabilities through civilian means. Singapore's universities and research institutions conduct cutting-edge AI research, attracting international talent. While this research primarily targets civilian applications, technological spillovers can serve military needs. Through this civilian-military dual approach, Singapore reduces direct dependence on foreign military technology while maintaining system compatibility with major powers.

Singapore's diplomatic flexibility provides strong support for its hedging strategy; it maintains close security cooperation with the United States while preserving good economic relations with China. In regional security architecture, Singapore actively participates in ASEAN mechanisms, avoiding being seen as completely aligned with any major power. This diplomatic positioning enables Singapore to procure technology from multiple sources without facing excessive pressure.

[31] Hong Liu and Jonathan Goh, "Emerging Business Transnationalism in Singapore and China: Governance, Networks, and Strategies," *Asia Pacific Business Review*, Vol. 30, No. 4 (2022), pp. 640–66, https://doi.org/10.1080/13602381.2022.2136232.

India: Strategic Autonomy Under Diversified Procurement

India's military technology sourcing is highly diversified. Traditionally, India relied heavily on Soviet/Russian equipment, but in recent decades it has increased procurement from the United States, Europe, and Israel. In AI military technology, India maintains this diversification strategy. India procured U.S. MQ-9 Reaper drones for maritime patrol and border surveillance while strengthening cooperation with Russia in other domains and advancing indigenous UAV projects[32].

India's indigenous development efforts are reflected in multiple projects. India is developing the Ghatak stealth combat drone, aiming to establish independent combat UAV capabilities. Although this project faces technical challenges and delays, it reflects India's pursuit of strategic autonomy. India also established a Defense AI Council to coordinate AI technology development across military services.

However, India's hedging strategy faces unique challenges. First is insufficient indigenous innovation capability. Many indigenous projects experience severe delays and cost overruns, with final performance often falling short of expectations[33]. Second is the complex coordination challenges in multi-source procurement. India's military equipment comes from different countries, creating serious interoperability issues[34]. Third is India's geopolitical environment, constraining hedging space. Despite these challenges, India

[32] Dinakar Peri, "India, U.S. Conclude $3.5bn Deal for 31 MQ-9B Armed UAVs," *The Hindu*, October 15, 2024, https://www.thehindu.com/news/national/india-us-conclude-35bn-deal-for-31-mq-9b-armed-uavs/article68754321.ece.
[33] Laxman Kumar Behera, "Examining India's Defence Innovation Performance," *Journal of Strategic Studies*, Vol. 44, No. 6 (2021), pp. 830–53, https://doi.org/10.1080/01402390.2021.1993829.
[34] C. Vinodan and A. L. Kurian, "Strategic Autonomy and India's Hedging Policies in the Indo-Pacific," *Journal of Asian Security and International Affairs,* Vol. 11, No. 4 (2024), pp. 475–95, https://doi.org/10.1177/23477970241282095.

persists with a hedging strategy because it aligns with India's strategic culture and geopolitical reality. India has long pursued a non-aligned foreign policy tradition, maintaining independence in major power competition. In AI military technology, this tradition manifests as diversified procurement and indigenous development.

Chokepoint Strategy: Netherlands and South Korea

Chokepoint strategy represents a unique power logic: gaining disproportionate geopolitical bargaining power by monopolizing critical nodes in technology supply chains, rather than through comprehensive technological capabilities. The core of this strategy lies in the highly specialized and concentrated nature of modern technology supply chains, where only a few companies or countries control specific key components or processes. These chokepoint holders thereby gain strategic leverage in major power competition, enabling them to shape the competitive landscape rather than merely passively adapt to it.

Netherlands: ASML's Lithography Monopoly

The Netherlands' chokepoint position primarily stems from ASML's monopoly in extreme ultraviolet (EUV) lithography technology. EUV lithography development began in the 1990s, jointly advanced by European research institutions, the US government, and major chip manufacturers[35]. ASML integrated resources from multiple countries through international cooperation, ultimately becoming the sole successful player. This process involved breakthroughs in optics, laser technology, precision control, and software

[35] ASML, "Making EUV: From Lab to Fab," March 30, 2022, https://www.asml.com/en/news/stories/2022/making-euv-from-lab-to-fab.

algorithms, creating a technological depth that latecomers would have difficulty replicating in the short term.

This monopoly position grants the Netherlands significant strategic leverage in Sino-American technological competition. Facing US export restriction pressures since 2019, the Dutch government adopted a layered bargaining approach: imposing a de facto ban on the most advanced EUV lithography systems to China, while preserving export licenses for older-generation DUV equipment until 2023-2024, and explicitly pursuing "de-risking, not decoupling" to safeguard ASML's market access and Dutch economic interests [36]. This position is not a passive compromise but instead the Netherlands actively leveraging its irreplaceability as a calculated move to maximize its own financial and strategic interests while fulfilling transatlantic alliance obligations.

The Netherlands' bargaining power operates on three levels: technologically, ASML's monopoly cannot be broken in the short term; economically, the Chinese market represents a significant share of ASML's revenue; strategically, the EU needs to maintain a degree of autonomy in its China policy. Leveraging its control over ASML's EUV and DUV lithography systems, the Netherlands holds a "case-by-case" export licensing regime, enabling it to resist blanket U.S. demands for comprehensive restrictions while preserving policy flexibility for incremental adjustments in response to evolving geopolitical pressures.[37]

[36] Sebastiaan Bennink, "Netherlands: Unilateral Export Controls as a Tool to Safeguard National Security and Foreign Policy Objectives," *Global Investigations Review*, July 16, 2025),https://globalinvestigationsreview.com/review/the-european-middle-eastern-and-african-investigations-review/2025/article/netherlands-unilateral-export-controls-tool-safeguard-national-security-and-foreign-policy-objectives

[37] Minister for Foreign Trade and Development Cooperation and Minister of Foreign Affairs, *Dutch Export Policy on Strategic Goods in 2024: Annual Report on Dual-Use Export Control* (Netherlands Ministry of Foreign Affairs, 2025), https://www.government.nl/binaries/government/documenten/reports/2025/06/27/dutch-export-policy-on-strategic-goods-in-2024/annual-report-on-dual-use-export-control-2024.pdf.

South Korea: HBM Memory Monopoly

South Korea's chokepoint position stems from Samsung and SK Hynix's dominance in high-bandwidth memory (HBM). This specialized memory is crucial for AI chip performance, with AI training and inference heavily dependent on HBM. Currently, Samsung and SK Hynix control over 90% of the global HBM market, forming a de facto technology-market dual monopoly[38]. HBM technology development requires breakthroughs in semiconductor manufacturing, packaging technology, and thermal management. Samsung and SK Hynix, through years of R&D investment and accumulated production experience, have established leading positions in this field. Although the US and Japan also have memory manufacturers, they lag significantly in HBM. This technological gap grants South Korea structural leverage in AI competition: when U.S. tech giants like NVIDIA and AMD need HBM for AI chips, they rely on Korean suppliers; when China attempts to develop indigenous AI chips, it similarly needs to procure HBM from Korea. This bilateral dependency makes South Korea an unavoidable strategic node in the global AI supply chain.

In the face of U.S. requests to restrict HBM exports to China, South Korea has demonstrated highly sophisticated strategic and operational capabilities. In the 2022 Chip 4 Alliance negotiations, South Korea neither accepted nor rejected, but transformed the talks into a process of securing maximum strategic benefits[39]. South Korea successfully negotiated exemptions for its companies' existing factories in China, ensuring continuity of already-invested projects.

---

[38] TrendForce, "News SK Hynix U.S. Revenue More than Doubles amid Surging HBM Demand," March 5, 2025, https://www.trendforce.com/news/2025/03/05/news-sk-hynix-us-revenue-more-than-doubles-amid-surging-hbm-demand.
[39] Charles Mok, "The Other Half of 'Chip 4': Japan and South Korea's Different Paths to de-Risking," *The Diplomat*, June 3, 2024, https://thediplomat.com/2024/06/the-other-half-of-chip-4-japan-and-south-koreas-different-paths-to-de-risking/.

While these exemptions carry time limits and conditions, they preserve crucial strategic buffer space for Korean enterprises.

This chokepoint position places South Korea in a unique position in technological geopolitics: it is neither a great power nor a mere technological follower. Instead, it becomes an indispensable variable in rule-making processes by controlling critical technological nodes. South Korea’s strategic wisdom lies in converting this technological monopoly into sustained political bargaining power, carving out autonomous strategic space amid the interstices of great-power competition.

Autonomous Strategy: France and Germany

Autonomous strategies pursue maximum technological independence and strategic autonomy. Its core logic is to establish indigenous innovation systems to minimize dependence on major power technology suppliers. This strategy is typically adopted by countries with certain technological foundations but unwilling to become technological vassals of major powers. In the field of AI military technology, European countries, led by France, are the main practitioners of this strategy.

France: Technology Sovereignty in the Gaullist Tradition

France’s autonomous strategy is deeply influenced by Gaullist tradition. De Gaulle believed France must maintain strategic independence, not become a vassal of any major power. This tradition continues in the AI era, with France insisting on developing indigenous AI military capabilities. France’s autonomous strategy is embodied in multiple levels. First is the Future Combat Air System (FCAS) project, jointly advanced by France, Germany, and Spain, aiming to develop a sixth-generation fighter to replace the current Rafale and

Eurofighter aircraft[40]. This project emphasizes manned-unmanned teaming, with AI systems coordinating manned fighters and multiple unmanned wingmen for combat. Although the project faces delays and cost overruns, it represents Europe's ambition for strategic autonomy in advanced military technology.

Second, at the enterprise level, France has cultivated a dual-use AI ecosystem centered on Thales and Dassault Systèmes. Thales is one of Europe's largest defense electronics companies, with leading technology in radar, communications, and cybersecurity[41]. Its AI applications cover electronic warfare, intelligence collection, automatic image recognition, collaborative combat, autonomous navigation robots, cybersecurity, and predictive equipment maintenance. Dassault Systèmes, though primarily known for industrial software, sees its 3D modeling and simulation technology widely applied in military system design. This civilian-military integration ecosystem enables France to maximize technology spillover effects with limited resources.

Moreover, in March 2024, French Defense Minister Sébastien Lecornu announced the establishment of the Military Applications AI Agency (Amiad) at École Polytechnique. The agency's mission is to enable France to sovereignly master these technologies without depending on other major powers, as General de Gaulle hoped when launching our deterrence policy in 1945[42]. The agency headquarters is at École Polytechnique (responsible for research), with a production base in Bourges that eventually employs 300 people, including

[40] Aaron Spray, "France Demands 80% Share in FCAS 6th Generation Fighter Jet Program," *Aerospace Global News*, July 9, 2025, https://www.aerospacesg.com/news/defence/france-demands-80-share-in-fcas-6th-generation-fighter-jet-program.
[41] Kevin Martin and Louis Liversain, "A Winding Road before Scaling-up? Defense AI in France," The Very Long Game, ed. Heiko Borchert et al., Contributions to Security and Defence Studies (Springer, 2024), https://doi.org/10.1007/978-3-031-58649-1_11.
[42] École Polytechnique, "French Minister of the Armed Forces at École Polytechnique to Boost AI in Defense," March 9, 2024, https://www.polytechnique.edu/en/news/french-minister-armed-forces-ecole-polytechnique-boost-ai-defense.

researchers and military personnel. Lecornu emphasized: AI represents a technological leap that will undoubtedly completely transform how we wage war, or more importantly, like the atomic bomb, help us avoid war. This comparison to nuclear deterrence again shows France views AI autonomy as core to strategic independence.

Germany: Finding Balance Between Ethical Constraints and Technical Needs

Germany's autonomous strategy is profoundly influenced by its unique historical memory and political culture. World War II lessons made German society extremely sensitive to the ethics of military technology[43], while the Cold War experience taught Germany the strategic risks of technological dependence. This dual consciousness shapes Germany's special path in AI militarization: pursuing technological autonomy while setting strict ethical red lines for autonomous weapon systems.

The digital transformation plan of the German Federal Armed Forces began with the 2016 White Paper on Defense, but truly accelerated after the 2022 Russia-Ukraine conflict[44]. Of Chancellor Scholz's €100 billion special fund, 15–25% (€15–25 billion) is allocated to AI and digitization for the Bundeswehr, including cyber defense, data centers, and AI training[45]. Most important is the Uranos AI project. Uranos' system design concept is creating a digital combat command that collects and analyzes data in real-time from radar systems,

[43] Thomas U. Berger, "The Past in the Present: Historical Memory and German National Security Policy," *German Politics,* Vol. 6, No. 1 (1997), pp. 39–59, https://doi.org/10.1080/09644009708404463.
[44] Bundesministerium der Verteidigung, *Sechster bericht zur digitalen transformation des geschäftsbereichs des bundesministeriums der verteidigung* (Bundesministerium der Verteidigung, 2024), https://www.bmvg.de/resource/blob/5729842/44f9fc60325fb62bf9665cd53d771dc6/download-6-digitalbericht-data.pdf.
[45] Alexander Luck, "Does 'Zeitenwende' Represent a Flash in the Pan or Renewal for the German Military?," 2022, https://www.fpri.org/article/2022/06/does-zeitenwende-represent-a-flash-in-the-pan-or-renewal-for-the-german-military/.

drones, cameras, satellites, lasers, and other reconnaissance units. AI's role is to provide early warning of potential threats from Russian forces, creating a strategic advantage. However, these projects also reflect Germany's cautious attitude. The system is explicitly designed as a decision support tool rather than an autonomous weapon: AI can analyze data, identify threats, and recommend actions, but final decision authority always remains with human commanders[46]. This aligns with the German Defense Ministry's consistent position of refusing to develop fully autonomous weapon systems.

Currently deployed AI applications in the German Federal Armed Forces primarily focus on C4ISR domains. For example, the GhostPlay project uses AI to develop tactics; UAV system projects use AI to generate battlefield situational maps; AI support systems are used for potential target detection and identification; vehicles for my countermeasures; and projects improving situational awareness through data fusion. These applications all follow the human-ultimate-control principle, with AI's role enhanced rather than replacing human decision-making.

Third-Party States and the Reconstruction of Strategic Stability

The preceding sections have conducted a horizontal analysis of the strategic choices of five types of third-party states, revealing how allied strategy states create interdependence through technological cooperation, transfer strategy states leverage great power competition for capability building, hedging strategy states maintain diversified supply chains to avoid singular dependencies, chokepoint strategy states acquire leverage through their critical supply chain positions, and autonomous strategy states pursue control over complete industrial chains. However, while typological analysis illuminates the

[46] Rafal Ulatowski, "The Illusion of Germany's Zeitenwende," *The Washington Quarterly,* Vol. 47, No. 3 (2024), pp. 59–76, https://doi.org/10.1080/0163660X.2024.2398318.

diversity of third-party state behavior, it fails to address a more fundamental question adequately: when these states pursue their respective strategic objectives, how does their collective behavior reshape the underlying logic of the international security landscape? In other words, we must shift from micro-level behavioral patterns to macro-level structural effects, from individual strategic choices to the evolutionary mechanisms of the broader configuration.

Mechanisms of Enhanced Strategic Stability

Traditional strategic stability theory focuses on whether military balances between great powers remain robust, whether nuclear deterrence is reliable, and whether crisis escalation can be controlled[47]. When third-party states move from the periphery to the center, transitioning from passive adaptation to active shaping, the stability mechanisms of the entire international security landscape inevitably undergo profound transformation. The central theoretical puzzle is whether this transformation enhances or undermines stability.

The simple answer is both, but this dialectical relationship is far more complex than it appears. The rise of third-party states simultaneously creates new stability mechanisms and new destabilization risks, and these dual effects do not coexist statically but interact and transform through dynamic strategic interaction. Deepening interdependence can enhance strategic constraints yet may also convert into systemic vulnerabilities through technical failures or policy disagreements. Diversification of technological sources can reduce monopoly risks but may also lead to standard fragmentation and interoperability dilemmas. Enhanced regional capabilities can strengthen deterrence effects but may also compress the temporal windows for crisis management. More critically, the current international order finds itself at a critical juncture, with

[47] Paul H Nitze, "Assuring Strategic Stability in an Era of Détente," *Foreign Affairs,* Vol. 54, No. 2 (1976), pp. 207–32.

great-power technological monopolies collapsing. At the same time, new multipolar equilibria remain unformed, leaving the balance between stability and instability in a state of violent flux.

The core of stability-enhancement mechanisms lies in the constraining effects brought by power decentralization. The new power resources that third-party states have acquired in the AI era dilute, to some extent, great decision-making monopolies while increasing systemic redundancy and resilience. The technological monopoly positions held by supply chain node states impose practical constraints on any attempts at strategic coercion through technological blockades. When the United States seeks to cut off China's access to advanced semiconductors, it must persuade the Netherlands to restrict ASML exports and South Korea to limit HBM supplies. Yet, these node states have their own interest calculations and will not cooperate unconditionally. This multi-node control structure in supply chains objectively increases the difficulty of unilateral technological blockades, compelling great powers to consider greater costs and consequences before adopting extreme measures.

Diversification of technological sources similarly possesses stabilizing effects. When non-US-China actors, such as Europe, Israel, and Turkey, develop capabilities in military AI, third-party states gain more procurement and cooperation options. This diversification reduces dependence on single suppliers and decreases the likelihood of being forced to alter strategic positions due to technological supply cutoffs or political pressure. India can simultaneously procure drones from the United States, obtain counter-drone systems from Israel, and import air defense systems from Russia. While this multi-source procurement strategy increases system integration complexity, it also maintains strategic flexibility amid great power competition. For great powers, third-party states' diversified choices mean that technological control alone cannot ensure strategic loyalty; alliance consolidation requires more complex exchanges of interests and the maintenance of relationships. This shift from coercion to consultation, to some degree, reduces the great powers' propensity for adventurous actions.

The proliferation of regional denial capabilities enhances stability from another dimension. As an increasing number of regional powers acquire AI-driven anti-access capabilities, the costs of significant military intervention rise significantly. This does not mean smaller states can defeat great powers, but rather that they can create sufficient uncertainty and attrition to compel more prudent strategic calculations before intervention decisions. The proliferation of low-cost small drones in the Middle East, as observed in Ukraine, erodes US air superiority by enabling asymmetric, high-cost intercepts that constrain low-cost operations and freedom of action[48]. This capability diffusion, to some extent, suppresses great-power adventurism and increases incentives to maintain the status quo.

Mechanisms of Diminished Strategic Stability

However, destabilizing mechanisms prove equally potent and demand serious attention. The most immediate risk emerges from the systemic compression of decision-making time. AI system integration significantly accelerates military operational tempo, with the entire cycle from intelligence collection through target identification to fire engagement completed within minutes or even seconds. While AI's rapid decision-making capabilities enhance combat efficiency, they may lack sufficient contextual judgment and ethical

[48] Dominika Kunertova, "Drones Have Boots: Learning from Russia's War in Ukraine," *Contemporary Security Policy,* Vol. 44, No. 4 (2023), pp. 576–91, https://doi.org/10.1080/13523260.2023.2262792.

considerations, thereby increasing the risk of misperception[49]. When AI early-warning systems deployed by third-party states experience technical malfunctions or are targeted by deceptive attacks, they may generate erroneous threat assessments that trigger automatic responses without adequate human review. More dangerously, because third-party state AI systems often lag behind great power systems in technological maturity, their misperception probabilities may be higher. Once decisions are made, they may rapidly escalate regional conflicts into crises involving great powers. Traditional strategic stability relies on adequate response time and communication channels. Still, the AI era's high-speed decision cycles compress these buffer spaces, significantly elevating risks of accidental conflict and misperception-driven escalation.

The uncontrollability of technological diffusion constitutes another primary risk dimension. Third-party states acquiring AI military technologies cannot always effectively control their further proliferation. Yemen's Houthi forces' use of drone technology demonstrates how capabilities diffuse from state to non-state actors. Although AI-related capabilities acquired by these armed groups remain relatively rudimentary, they are sufficient to cause severe regional security impacts. The crux is that once technology diffuses among non-state actors, traditional deterrence and arms control mechanisms become completely ineffective. One cannot impose retaliatory strikes on an organization lacking fixed territory and government structures, nor limit its behavior through diplomatic negotiations[50]. When such organizations employ AI-enhanced drones to attack critical infrastructure or conduct terrorist attacks, attacked states may attribute responsibility to state supporters behind them, thereby triggering

[49] Cuihong Cai and Luyao Zhang, "Escaping the Trap: Adapting the U.S.-China Arms Race to the Dynamics of Artificial Intelligence," *North South Journal of Peace and Global Studies*, ahead of print, August 2024, https://doi.org/10.47126/nsjpgs.v2i1.02.

[50] Elke Krahmann, "From State to Non-State Actors: The Emergence of Security Governance," in *New Threats and New Actors in International Security*, ed. Elke Krahmann (Palgrave Macmillan, 2005), https://doi.org/10.1057/9781403981660_1.

interstate conflicts. The longer the technological diffusion chain, the weaker control capabilities become, and the higher the probability of loss of control.

This technological diffusion challenge extends beyond the state-to-non-state transfer problem to encompass more subtle forms of horizontal proliferation among state actors themselves. The AI era witnesses not merely vertical diffusion downward through traditional hierarchies, but lateral diffusion through commercial channels, cyber espionage, reverse engineering, and open-source intelligence. Unlike nuclear weapons technology, which required massive physical infrastructure and left detectable signatures, AI capabilities can be acquired through software downloads, academic paper implementations, and commercial cloud computing resources. This ease of diffusion means that even states with modest resources can rapidly close capability gaps once others demonstrate proof of concept[51]. Furthermore, the dual-use nature of AI technologies renders export controls and non-proliferation regimes extraordinarily difficult to enforce. What emerges is a proliferation landscape characterized by multiple simultaneous diffusion pathways, each with distinct dynamics and control challenges.

In summary, third-party state involvement in the diffusion of military AI produces a dual effect on strategic stability. While power decentralization creates new constraint mechanisms and reduces monopoly risks, it simultaneously introduces destabilizing forces through accelerated decision cycles, uncontrolled proliferation, and the erosion of traditional arms control frameworks. The net effect on stability depends on whether institutional

[51] David M. Allison and Stephen Herzog, "Artificial Intelligence and Nuclear Weapons Proliferation: The Technological Arms Race for (in)Visibility," *Risk Analysis*, ahead of print, September 25, 2025, https://doi.org/10.1111/risa.70105.

adaptations and governance mechanisms can keep pace with technological diffusion.

Conclusion

The militarization of artificial intelligence is catalyzing a fundamental transformation in the distribution of global strategic power, with third-party states emerging as active shapers rather than passive recipients in this technological revolution. The four distinctive attributes of military AI technology, such as general-purpose nature, dual-use ambiguity, low marginal cost, and data dependency, are systematically dismantling the technological monopoly mechanisms that major powers have long relied upon. Unlike the nuclear age, where technological barriers confined strategic capabilities to a handful of states, the AI era enabled diverse actors to acquire advanced military capabilities through multiple pathways at unprecedented speed.

The implications for strategic stability are profoundly ambiguous. On the one hand, power decentralization creates new constraints: supply chain interdependence limits unilateral coercion, technological diversification reduces monopoly risks, and regional denial capabilities deter great-power adventurism. On the other hand, destabilizing forces are equally potent: compressed decision-making timelines heighten misperception risks, uncontrolled technological diffusion to non-state actors erodes traditional deterrence, alliance fragmentation undermines collective security, and the globalization of arms races exceeds existing control frameworks. The critical question is not whether AI diffusion stabilizes or destabilizes the international order, but rather how these dual dynamics interact and evolve under varying conditions.

The contemporary international order finds itself in a liminal phase, with traditional great-power technological monopolies collapsing while new multipolar equilibria remain unformed. This transitional uncertainty itself constitutes the most significant challenge to stability. Third-party states have transformed from peripheral variables into central actors whose strategic choices fundamentally shape the trajectory of international security architecture. Any analysis that treats them as mere technological recipients or passive objects in great-power competition fails to grasp the structural transformation underway.

Looking ahead, the future of strategic stability depends on competitive outcomes among several key variables: the pace of technological diffusion versus the establishment of arms control norms, enhanced great-power coordination versus accelerated alliance fragmentation, interdependence's constraining effects versus technical failure's systemic risks. These questions lack predetermined answers and instead depend on strategic choices and historical contingencies over the coming decade. What remains certain is that understanding third-party states' agencies in the diffusion of military AI is no longer optional but essential for comprehending and managing international security in the algorithmic age. The unintended beneficiaries of disruptive technology may ultimately determine whether the AI revolution reinforces or revolutionizes the foundations of global order.