Issue Brief

July 2026
No : 532

CENTRE FOR LAND WARFARE STUDIES
CLAWS
अन्वेषणं ज्ञानस्य मुख्यम्।

Project Glasswing, Semiconductor Dependency and the Sovereignty of Indian Military LLMs: An International Relations and Strategic Security Analysis

Ishika Mandal

Project Glasswing, Semiconductor Dependency and the Sovereignty of Indian Military LLMs: An International Relations and Strategic Security Analysis

Ishika Mandal

Abstract

The strategic environment of international security has drastically changed with the advent of cutting-edge artificial intelligence (AI) systems that can conduct independent cyber operations. One of the most important advancements in AI-driven cybersecurity is Anthropic's Project Glasswing, introduced in 2026, which allows Large Language Models (LLMs) to independently identify and assess software vulnerabilities across infrastructure ecosystems. Project Glasswing presents issues of cyber sovereignty, technology dependence, military AI vulnerability, and geopolitical imbalance while being publicly presented as a defensive cybersecurity initiative.

The ramifications of Project Glasswing for India's defence ecosystem are examined in this article, with a focus on the strategic military AI infrastructure and the sovereignty of Indian Military LLMs. The paper makes the case that India's reliance on foreign semiconductors, frontier AI ecosystems, and cloud infrastructure creates structural vulnerabilities that could jeopardise long-term military autonomy. It does this by taking on recent news, semiconductor supply chain studies, International Relations (IR) theories, sovereign AI literature, and cybersecurity research. To safeguard India's strategic autonomy in the developing AI-driven security order, the report suggests a sovereignty-centred framework that integrates indigenous AI systems, semiconductor self-reliance, sovereign compute infrastructure, and cyber-defence modernization.

Keywords: AI, Project Glasswing, Sovereignty, Semiconductor, Indian Military, LLMs.

Introduction

What is Project Glasswing?

Project Glasswing is an initiative launched by Anthropic on April 7, 2026. The concept is simple enough for a sophisticated AI model to identify potentially harmful security flaws in viral software before attackers can use the same type of AI to identify and exploit them.
The Glasswing butterfly, which conceals in plain sight and has almost transparent wings, is the source of the name. The comparison is that software flaws can go unnoticed for decades. There are other organisations involved besides Anthropic. As launch partners, the project brought together a sizable coalition of businesses like CrowdStrike, Apple, Broadcom, CISCO, Amazon Web Services, Google, JPMorgan Chase, Palo Alto Networks, Microsoft, NVIDIA, and the Linux Foundation (Anthropic, 2026).

Claude Mythos Preview (The Model Behind It):

(No Time, 2026) explains that to understand Project Glasswing, we need to understand what Claude Mythos Preview is. According to Anthropic, it is their best model to date for agentic and coding tasks. The crucial point is that Anthropic did not provide it with cybersecurity-specific training. Its proficiency in general coding and security capabilities. After asking Mythos to identify remote code execution vulnerabilities overnight, Anthropic's own engineers, some of whom lacked formal security training- woke up in the morning with functional exploits. The model had completed the task independently. Mythos received an 83.1% score on CyberGym, a test for reproducing vulnerabilities, in official benchmark testing. On the same test, Opus 4.6, the previous Claude model, had a score of 66.6%. Mythos was 181 times more successful than Opus 4.6 at writing Firefox exploits. That is a significant advancement. It was the first model to complete both of its sophisticated, multi-step cyberattack simulations from beginning to conclusion, according to the UK's AI Security Institute. Anthropic chose not to make it available to the wider public as a result.

Historical Background of Claude AI

In April 2026, Anthropic unveiled Project Glasswing, a massive cybersecurity project intended to defend vital software infrastructure from increasingly complex AI-enabled cyberattacks. Anthropic's discovery that frontier AI systems had advanced to the point where they could detect and exploit software flaws on par with or better than top-tier human security researchers gave rise to the project. The effort was developed, according to Anthropic, to guarantee that defensive actors have access to sophisticated AI-assisted vulnerability identification prior to bad actors being able to weaponise comparable skills. The glasswing butterfly, whose transparent wings represent weaknesses in software that can go unnoticed for years or even decades, served as the inspiration for the project's name (Anthropic, 2026).

Major cybersecurity and technology companies, such as Amazon Web Services, Apple, Broadcom, Cisco, CrowdStrike, Google, JPMorgan Chase, Microsoft, NVIDIA, Palo Alto Networks, and the Linux Foundation, came together to form Project Glasswing. The program aims to find and fix key software system vulnerabilities before attackers can take advantage of them. According to Anthropic, the project's AI system found thousands of high-severity vulnerabilities in popular operating systems and web browsers, including ones that had been undetected for decades despite thorough automated testing and human review.

The realisation that artificial intelligence is turning cybersecurity into an arms race is what makes Project Glasswing strategically significant. According to Anthropic, proactive defence is becoming more and more important because AI has significantly decreased the knowledge and work needed to identify software vulnerabilities. As a result, Project Glasswing exemplifies a "defence-first" strategy in which sophisticated AI capabilities are employed to safeguard software ecosystems prior to the widespread availability of equivalent attack capabilities.

Claude AI and the emergence of Claude Mythos Preview

Anthropic's Constitutional AI paradigm, which prioritises safety, openness and conformity with human values, was initially used to construct the Claude family of large language models (LLMs). Anthropic has gradually increased the reasoning, coding, and agentic capabilities of the model family since the Claude model was released in 2023. According to research, Claude serves as a foundation model for complicated thinking and software engineering applications in addition to complex to conversational tasks (Priyanshu et al., 2024).

The foundation of Project Glasswing is an unreleased frontier model called Claude Mythos Preview, which Anthropic describes as a general-purpose AI system with exceptional cybersecurity capabilities. During testing, Mythos autonomously found thousands of previously undiscovered vulnerabilities, including zero-day vulnerabilities affecting major operating systems and browsers; the model reportedly found a 27-year-old vulnerability in OpenBSD and demonstrated the ability to generate sophisticated exploit chains with minimal human assistance. Due to the dual-use nature of these capabilities, Anthropic decided not to make Mythos public (No Time, 2026).

Growing worries about cutting-edge AI systems that can conduct offensive cyber operations are reflected in Anthropic's decision. Although these methods can significantly improve software security, if they are widely used, they may also make it easier for hackers and state-sponsored threat actors to operate. Thus, Project Glasswing serves as a model for the responsible administration of advanced AI capabilities as well as a cybersecurity initiative.

Semiconductors and Computing Infrastructure Behind Claude AI

The precise semiconductor arrangement utilised to train Claude Mythos Preview has not been made public by Anthropic. The evidence that is currently available, however, suggests that Anthropic's AI models mostly rely on sophisticated AI accelerators provided by top 3 semiconductor manufacturers, especially NVIDIA and Amazon Web Services. Given its crucial role in providing the high-performance graphics processing units (GPUs) needed for frontier AI training and inference, NVIDIA is a launch partner in Project Glasswing. Larger clusters of AI accelerators based on cutting-edge semiconductor manufacturing technologies produced by foundries like TSMC are typically used to train modern Claude models.

Additionally, Anthropic has a close relationship with AWS, which has contributed billions of dollars to the business. For large-scale AI training, AWS has created a unique family of AI semiconductors dubbed Trainium. According to research, AWS Trainium accelerators are an affordable substitute for conventional GPU infrastructures that can efficiently train frontier-scale language models with billions of parameters (Fan et al., 2024). Future Claude systems might make use of combinations of NVIDIA GPUs and AWS Trainium accelerators, as Anthropic has increasingly used AWS infrastructure within its model development pipeline.

From a semiconductor standpoint, Claude AI relies on an international supply chain that includes cutting-edge chip designers, manufacturing plants, packaging innovation, and cloud computing infrastructure. Therefore, the creation of models like Claude Mythos Preview shows how AI capabilities are becoming more closely associated with semiconductor sovereignty and strategic technology competitiveness between states. Control of cutting-edge AI chips, production capacity, and cloud infrastructure has emerged as a crucial component of cybersecurity, digital resilience, and national competitiveness.

Development of Large Language Models (LLMs)

The development of Large Language Models (LLMs) from conversational systems into autonomous cyber-capable infrastructures has increased concerns about national security and digital sovereignty. Frontier AI models are now capable of advanced reasoning, vulnerability discovery, exploit analysis, and strategic cyber operations. In April 2026, Anthropic launched Project Glasswing, a cybersecurity initiative that brought together major technology companies like Amazon Web Services (AWS), Microsoft, Google, Apple, Cisco, NVIDIA, CrowdStrike, and Palo Alto Networks (Anthropic, 2026).

Anthropic claims that Mythos Preview found vulnerabilities "in every major operating system and browser," including several issues that had gone unnoticed for decades. (Anthropic, 2026). Within weeks of deployment, the algorithm found over 10,000 significant vulnerabilities in open-source software projects, according to a later report by The Economic Times(2026).

These developments point to a significant shift in cyberwarfare: These days, AI algorithms can find strategic flaws more quickly than human cybersecurity teams can fix them. This development raises serious issues for India regarding AI infrastructure autonomy, cyber-defence reliance, semiconductor vulnerabilities, military AI sovereignty, and strategic technology imbalance. This article makes the case that a more comprehensive framework linking AI governance, semiconductor self-reliance, sovereign compute infrastructure, and cyber-defence resilience is necessary to safeguard the sovereignty of Indian Army LLMs.

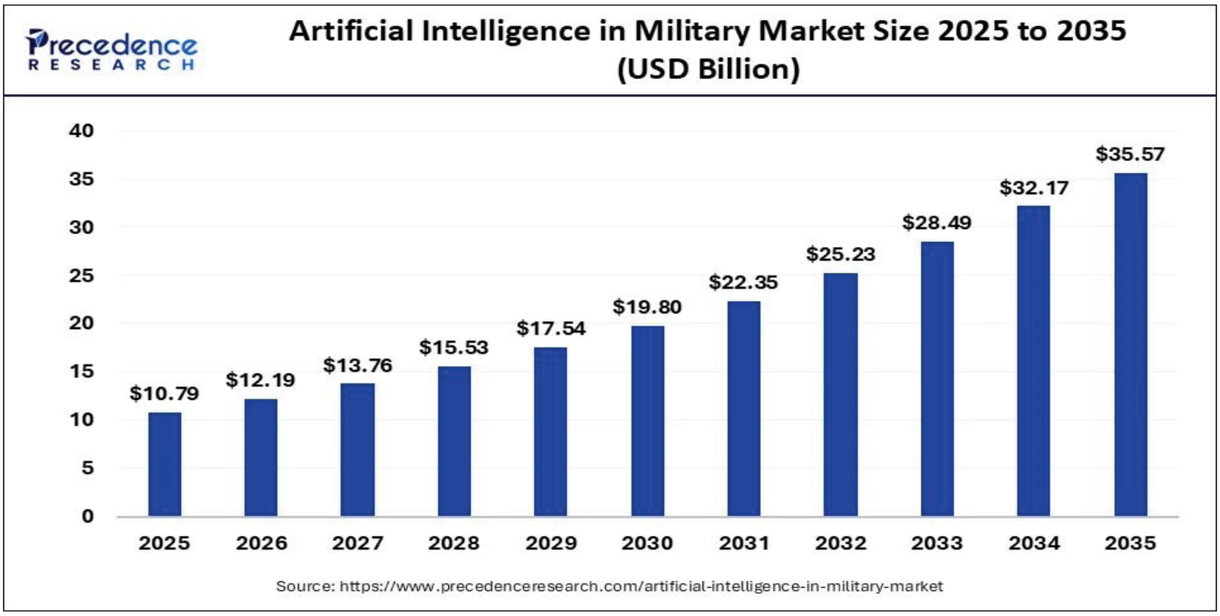
The strategic environment of International security and military affairs has changed as a result of the quick development of artificial intelligence (AI), semiconductor technologies, and autonomous cyber capabilities. Algorithmic decision-making, AI-powered cyber operations, semiconductor supply chains, and independent digital infrastructures are becoming more and more important in modern warfare (Husain, 2021). Concerns over AI-enabled vulnerability discovery systems that can independently find and exploit zero-day vulnerabilities across international software ecosystems were heightened in 2026 with the launch of Anthropic's Project Glasswing (Collins, 2026). Scholarly interest in AI militarisation, strategic autonomy, semiconductor sovereignty, and cyber deterrence has increased as a result of these advancements.

The research and policy literature on AI militarisation, cyberwarfare facilitated by AI, strategic sovereignty, semiconductor dependence, India's military AI ecosystem, and international relations theories related to rivalry for technological dominance. The research combines academic journals, policy reports, defence analyses, and contemporary news sources.
Identify the evolving debates surrounding AI sovereignty and the strategic implications of Project Glasswing for India's defence infrastructure.

AI as a Strategic Instrument of Power

In the late 2010s, the notion that AI is a revolutionary geopolitical force gained significant interest. The growing belief that AI would play a major role in the distribution of global power was epitomised by Russian President Vladimir Putin's declaration that "whoever leads in AI will rule the world" (RT News, 2017). The global AI competition, especially between the US and China, is a rebuilding of the international order through technical superiority, according to Kai-Fu Lee's AI Superpowers.

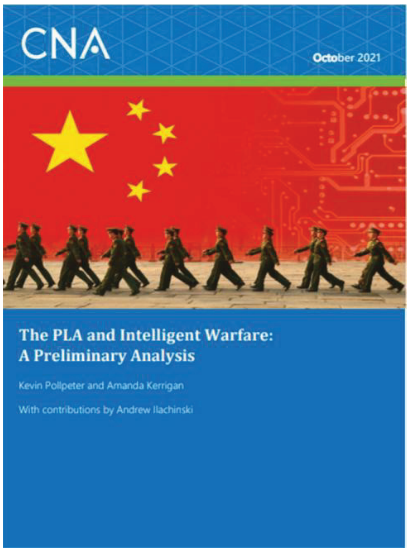
This view is consistent with realist and offensive realist theories of international relations, which contend that in anarchic international systems, nations constantly strive for technological dominance to maximise their chances of survival and strategic impact. A growing body of recent research views AI capabilities as strategic assets on par with nuclear or industrial power.
The global compound semiconductor market size was worth around USD 59.44 billion in 2025 and is expected to grow from USD 66.10 billion in 2026 to approximately USD 169.06 billion by 2035, expanding at a CAGR of 11.02% from 2026 to 2035. (Precedence Research, 2026).



These advancements show that AI is increasingly seen as a factor that determines geopolitical strength and strategic autonomy rather than just a technological advancement.

AI Militarisation and Modern Warfare

A growing number of academics contend that AI is radically changing the nature of combat. According to Husain (2021), AI speeds up operations by providing machine-speed battlefield analysis and shortening military decision-making cycles. Future intelligence, surveillance, and reconnaissance (ISR) systems are expected to rely more on AI-enabled autonomous processing systems than on conventional human-centric intelligence workflows, according to Roberts and Payne (2016, p. 12). Similarly, King (2024) emphasised that AI warfare systems increasingly blur distinctions between combatants and algorithms, human and machine decision-making, offence and defence. AI-enabled warfare also includes autonomous targeting. China is actively seeking "intelligentized warfare," where AI systems become essential to military operations, decision superiority, and strategic domination, according to the Eurasia Review's appraisal of the People's Liberation Army (PLA) (Ranjan, 2022).



AI militarization has heightened India and Pakistan's strategic rivalry in South Asia. By increasing automation and decreasing human oversight, Saeed (2023) contended that the incorporation of AI into South Asian military systems could undermine deterrence. In a similar vein, Amir (2024) noted that AI is transforming the defence industries of India and Pakistan through cyber capabilities, autonomous ISA systems, and predictive military analytics.

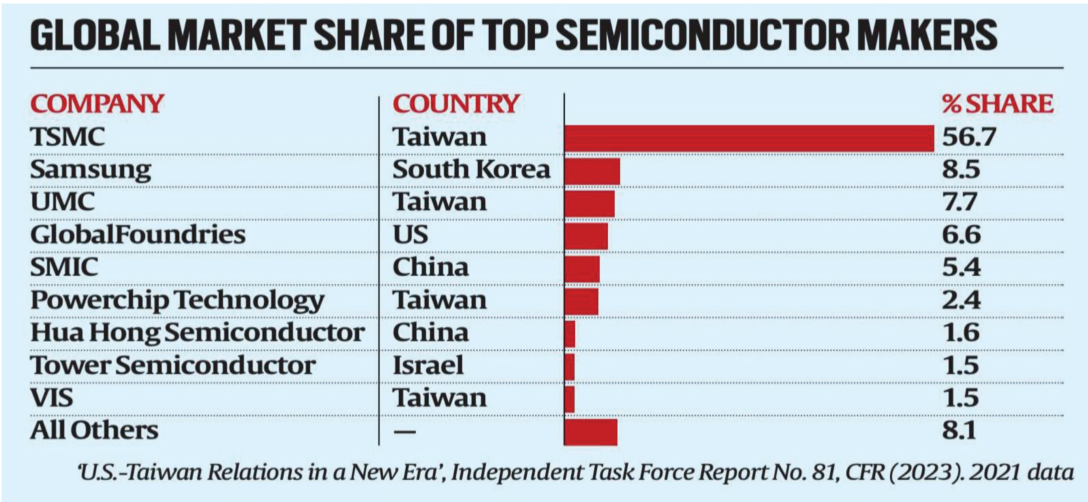
India's AI modernization is increasingly portrayed in Pakistani strategic literature as a cause of regional instability and escalation of danger (Mansoor, 2024). Khurshid and Zaman (2024) added that the use of AI in Indian military systems raises further security concerns in South Asia because of the hazards associated with autonomous warfare, cyber escalation, and asymmetric capabilities.

Project Glasswing and AI-Enabled Cyber Warfare

A major change in AI-enabled cybersecurity is represented by Project Glasswing. According to reports, Anthropic's initiative used the Claude Mythos Preview approach to automatically find vulnerabilities and zero-day exploits in significant software ecosystems (Anthropic, 2026). According to (Fadilpašić, 2026), the system found thousands of vulnerabilities, operating system issues, vulnerabilities in popular browsers, and security hazards that were previously unidentified. The dual-use aspect of such technologies has raised concerns among cybersecurity researchers, according to Kachwala (2026), Glasswing is presented as a defensive cybersecurity infrastructure, but if it were weaponised, its capabilities might allow for aggressive cyber operations. This dual-use paradox is consistent with the Security Dilemma theory in international relations, which holds that defensive technical advancements inadvertently cause competing states to become strategically insecure. Autonomous AI systems may undermine cyber deterrence and raise escalation risks, according to a steadily increasing amount of research on strategic stability (Rickli, 2019). In a similar vein, Topychkanov (2020, pp. 12-13) cautioned that AI-enabled strategic systems shorten response times and may limit chances for diplomatic de-escalation in times of crisis.

Semiconductor Sovereignty and Strategic Dependency

The research progressively highlights how semiconductor sovereignty is crucial to AI sovereignty. Semiconductors serve as the basis for: autonomous military infrastructure, cloud computing, GPUs, AI training systems, and cyber-defence technologies. The concentration of semiconductor market power among a small number of companies and nations was brought to light by (Lu, 2025a; Visual Capitalist, 2023b).



A variety of key minerals, such as cobalt, lithium, gallium,germanium, and rare earth elements, are crucial for the production of semiconductors and are necessary for advanced electronics, chip fabrication, and developing technologies. Berg et al. (2024) mentioned that substantial supply-chain risks result from the concentration of these resources and their processing facilities in a small number of nations. China controls the refining and processing phases of key essential materials needed for the creation of semiconductors, even though some minerals are produced in multiple regions. This concentration exposes semiconductor-producing nations to geopolitical risks, trade restrictions, and possible supply disruption while giving China significant control over global supply chains. The authors stress that competition for these resources will get more intense due to the growing demand for semiconductors, which is being pushed by sophisticated manufacturing, renewable energy technologies, and artificial intelligence. In order to lessen reliance on geographically concentrated mineral processing networks, governments and businesses are attempting to diversify supply sources, improve local processing capabilities, and create robust supply chains (Berg et al., 2024).

FIGURE 4

Summary of the Disruption Potential for Five Key Minerals

Raw Material	Distruption Potential
Gallium	High
Germanium	Moderate-High
Fluorspar	Moderate
Arsenic	Moderate
Copper	Low

Source: Authors' analysis.

CSIS | AMERICAS PROGRAM

CRITICAL MINERALS IN SEMICONDUCTOR SUPPLY CHAINS AND INDIA'S STRAT GIC DEPENDENCY

CRITICAL MINERAL	SEMICONDUCTOR / AI USE	MAJOR GLOBAL PRODUCERS	INDIA'S DEPENDENCY STATUS	STRATEGIC RISK FOR INDIA	POTENTIAL INDIAN ALTERNATIVES / DOMESTIC SOURCES
Gallium (Ga)	Used in gallium nitride (GaN) chips, radar systems, 5G, military electronics, AI processors	China (~98% refining dominance), Germany, Kazakhstan	Highly import dependent	China's export restrictions may disrupt defense electronics and AI chip manufacturing	Bauxite residues and zinc processing waste in Odisha and Andhra Pradesh
Germanium (Ge)	Fiber optics, infrared optics, satellites, military sensors, semiconductors	China, Canada, Russia	Mostly imported	Vulnerability in defense surveillance and ISR systems	Zinc ore processing byproducts in Rajasthan
Rare Earth Elements (REEs)	Permanent magnets, missile guidance, AI hardware, defense electronics	China (~70% global production), Myanmar, Australia	Partial domestic reserves but heavy refining dependence	Supply chain coercion risk and military electronics dependency	Monazite sands in Kerala, Tamil Nadu, Odisha
Cobalt (Co)	Semiconductor alloys, batteries, AI servers, military energy systems	Democratic Republic of Congo, Indonesia, Russia	Nearly fully imported	Energy storage and defense battery vulnerability	Nickel-cobalt deposits in Odisha and Jharkhand (limited capacity)
Lithium (Li)	AI data centers, batteries, military drones, energy storage	Australia, Chile, China, Argentina	Highly import dependent	Critical for AI infrastructure and autonomous defense systems	Lithium reserves identified in Jammu & Kashmir and Rajasthan
Silicon (Ultra-Pure)	Semiconductor wafers, AI chips, processors	China, Japan, Taiwan, South Korea	Domestic raw silicon available but lacks advanced purification	Fabrication ecosystem vulnerability	Quartz reserves in Rajasthan, Andhra Pradesh
Copper (Cu)	Semiconductor interconnects, military electronics, power systems	Chile, Peru, China	Moderate import reliance	Critical infrastructure and electronics exposure	Rajasthan, Madhya Pradesh, Jharkhand
Nickel (Ni)	Semiconductor plating, AI battery systems	Indonesia, Philippines, Russia	Import dependent	Strategic battery and defense electronics risk	Odisha nickel deposits
Tantalum (Ta)	Capacitors in military electronics and semiconductors	Rwanda, DRC, Brazil	Imported	Precisgic defense electronics dependency	Minor reserves in Chhattisgarh and Jharkhand
Helium & Neon Gas	Semiconductor lithography and chip fabrication	U.S., Qatar, Ukraine, Russia	Imported	Vulnerability in advanced semiconductor manufacturing	Limited domestic production capacity

● High Dependency / High Risk ● Moderate Dependency / Moderate Risk ● Low Dependency / Lower Risk

Source: *CSIS (2021) – From Mine to Microchip: Critical Minerals and Semiconductor Supply Chains*

These worries gave rise to the idea of "Pax Silica." By creating alternate supply chains for semiconductors and essential minerals, India and its allies are attempting to lessen their reliance on China (Smith, 2026). Nonetheless, several studies have shown that fabrication facilities alone cannot accomplish semiconductor sovereignty. Compute infrastructure, semiconductor-grade chemical refinement, and processing ecosystems continue to be equally important (Cruzes, 2026).

In the era of digital warfare and artificial intelligence, semiconductor and computing sovereignty have become fundamental cornerstones of national security. Because advanced AI systems, such as military large language models (LLMs), rely significantly on secure semiconductor ecosystems, high-performance computing infrastructure, and trusted data networks, AI sovereignty cannot exist without computer sovereignty. Long-term defence autonomy may be jeopardised by strategic vulnerabilities brought about by India's increasing reliance on imported semiconductors, GPUs, and essential minerals. Therefore, to lessen reliance on foreign-controlled supply chains, India needs to speed local semiconductor manufacture and GPU infrastructure development, as well as crucial mineral refining and defence-grade chip manufacturing. According to Cruzes (2026), control over data centres, optical communication networks, computational infrastructure, and energy systems increasingly determines modern AI sovereignty. This is an illustration of a larger geopolitical change in which technology infrastructure has evolved into a tool of strategic power. During times of geopolitical unrest, India's sovereign Indian Army LLLMs and Military AI systems cannot continue to rely on foreign cloud ecosystems or outside semiconductor suppliers. Thus, in order to ensure strategic autonomy, cyber resilience, and secure military AI deployment in future multidomain warfare environments, it is imperative to develop sovereign compute infrastructure, reliable semiconductor supply chains, domestic chip fabrication ecosystems, and indigenous AI accelerators (Cruzes, 2026).

AI sovereignty and Indian Defence

India's growing defence modernisation increasingly depends on AI systems integrated into surveillance, logistics, battlefield intelligence, cyber defence, and decision-support systems. However, scholars increasingly argue that India's AI infrastructure remains structurally dependent on imported semiconductors, foreign GPUs, foreign cloud ecosystems, and external LLM architectures.

This poses a challenge to "decision sovereignty," according to Wei & Shu (2026), since military AI systems continue to rely on outside vendors for operational functioning. Project Glasswing raises this issue since AI-enabled vulnerability discovery tools may find flaws in Indian defence communication networks, autonomous AI systems, and military networks. The concept of "material zero-day vulnerability" emerges here, where vulnerabilities exist simultaneously across software, hardware, firmware, and semiconductor supply chains. They also proposed model replaceability frameworks where supplier models remain interchangeable analytical modules while command authority remains sovereign. This framework is particularly relevant for the Indian Army's AI modernisation. Tucker (2019) further warned that AI-driven information warfare might use synthetic media and AI-generated intelligence manipulation to control not only digital systems but also strategic perception itself.

AI, Nuclear Stability, and Escalation Risks

A significant amount of research looks at how AI affects nuclear deterrence and strategic stability. According to Rickli and Jean-Marc (2019), AI systems could undermine nuclear deterrence by decreasing strategic ambiguity, shortening decision-making deadlines, and increasing automation pressure. Similarly, Boulanin (2019) cautioned that incorporating machine learning systems into command structures raises the possibility of computational errors, unintentional escalation, and poor human-machine coordination. These issues are especially serious in South Asia because of cyber vulnerability, political instability, shortened escalation windows, and past India-Pakistan confrontations. Yusuf's (2019) study of the Pulwama crisis showed how quickly crises can worsen even in the absence of sophisticated AI-enabled systems. In order to ensure strategic stability, Liang & Klare (2024) stressed the significance of retaining significant human control in AI-enabled military systems.

sipri **SIPRI Insights on Peace and Security**
No. 2025/06 June 2025

IMPACT OF MILITARY ARTIFICIAL INTELLIGENCE ON NUCLEAR ESCALATION RISK

VLADISLAV CHERNAVSKIKH AND JULES PALAYER

The deterioration of the international security environment over the past decade has resulted in heightened concerns about the risk of nuclear war as nuclear-armed states and their allies renew their reliance on nuclear deterrence.[1] All nine nuclear-armed states—China, France, Israel, India, North Korea, Pakistan, the Russian Federation, the United Kingdom and the United States—are modernizing their nuclear forces, with some also increasing the size of their nuclear arsenals.[2] At the same time, these states are investing in the development and deployment of military artificial intelligence (AI), using it to pursue better and faster decision-making and increased autonomy in military systems.[3]

Just over half of nuclear-armed states have stated explicitly that they intend to maintain human control over decisions related to the use of nuclear weapons in order to minimize the risk of nuclear escalation.[4] Yet, even when used in non-nuclear-related military applications, military AI may have an impact on the operating environment in which nuclear decision-making takes place—for example, in a crisis situation, it may reduce the time required for threat detection and response coordination.[5] If military decision-support systems (DSSs) and automated capabilities push policymakers and military decision makers towards faster reaction times, this may increase the risk of miscalculation and errors and may affect decisions that could result in nuclear escalation. However, the ways in which military AI can influence the

[1] SIPRI, 'Role of nuclear weapons grows as geopolitical relations deteriorate—New SIPRI Yearbook out now', 17 June 2024.

[2] Kristensen, H. M. and Korda, M., 'World nuclear forces', *SIPRI Yearbook 2025: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, forthcoming 2025).

[3] Chernavskikh, V., 'Nuclear weapons and artificial intelligence: Technological promises and practical realities', SIPRI Background Paper, Sep. 2024; Boulanin, V. et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk* (SIPRI: Stockholm, June 2020), p. 16; and Probasco, E. S. et al., 'AI for military decision-making: Harnessing the advantages and avoiding the risks', Issue brief, Georgetown University, Center for Security and Emerging Technology (CSET), Apr. 2025.

[4] Responsible AI in the Military Domain (REAIM) Summit, 'REAIM Blueprint for Action', 9–10 Sep. 2024, para. 5; Chinese Ministry of Foreign Affairs, 'President Xi Jinping meets with US President Joe Biden in Lima', 17 Nov. 2024; and 10th NPT Review Conference, 'Principles and responsible practices for nuclear weapon states', Working paper submitted by France, the UK and the USA, NPT/CONF.2020/WP.70, 29 July 2022, para. 5(vii).

[5] Boulanin et al. (note 3); and Su, F., Chernavskikh V. and Wan, W., 'Advancing governance at the nexus of artificial intelligence and nuclear weapons', SIPRI Insights on Peace and Security no. 2025/03, Mar. 2025.

SUMMARY

● Increasing integration of artificial intelligence (AI) into military systems has the potential to influence nuclear escalation even when that integration occurs outside nuclear weapon systems. Non-nuclear applications of military AI may compress decision-making timelines, potentially increasing miscalculation risks during a crisis. Opaque recommendations from an AI-powered decision-support system can bias a decision-maker towards acting, while autonomy in a system with counterforce potential may undermine strategic stability by threatening the integrity of second-strike capabilities.

Such uses of AI raise the fundamental question of whether they introduce new risks, exacerbate existing ones or fundamentally alter the nature of nuclear escalation. Contextual and socio-technical factors that might affect nuclear escalation pathways can help to answer this question. Understanding these dynamics is essential for using current risk-reduction measures or developing new strategies to address nuclear escalation risks posed by military AI.

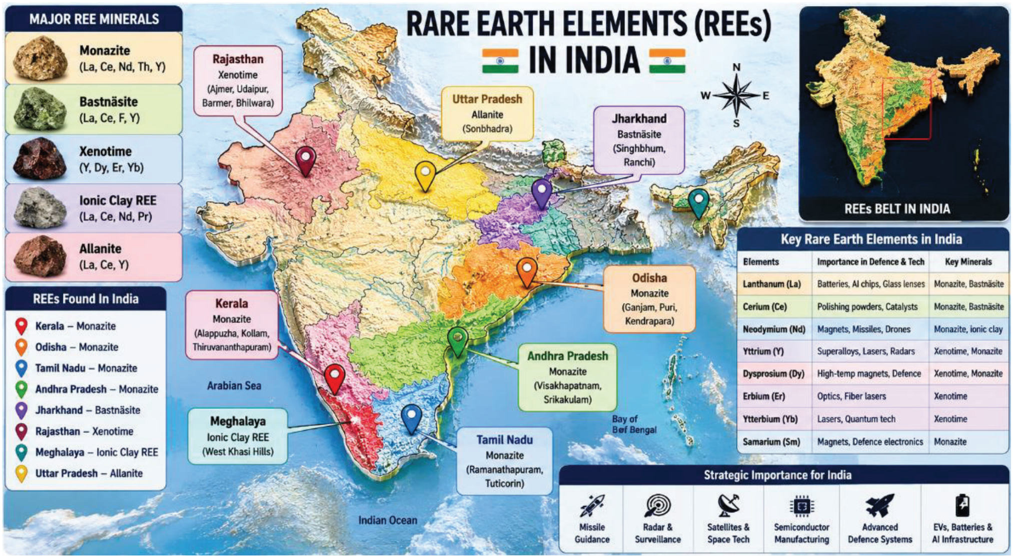
Ethical Frameworks and International Governance—the necessity of International governance frameworks for autonomous military systems is emphasised more and more in literature. Regulations about autonomous weapons systems under the Convention on Certain Conventional Weapons (CCW) are still being discussed by the UN Office for Disarmament Affairs (2025). In a similar vein, governance principles for autonomous and intelligent systems have been proposed by the IEEE Standards Association, n.d. (2025), with a focus on openness, responsibility, human supervision, and the ethical application of AI. Nonetheless, academics contend that governance structures are still disjointed and unable to control quickly developing AI military technologies.

India's Domestic Alternative & Self-Reliance

India's Lithium Discovery in Jammu and Kashmir- A major step toward lowering strategic reliance on imported battery minerals necessary for AI infrastructure and autonomous military systems has been taken by India with the discovery of lithium mines in Jammu and Kashmir (Ministry of Mines, 2023).

Rare Earth Sands in Odisha and Kerala- India possess monazite-rich beach sands containing rare earth elements, thorium, and titanium minerals. Major reserves exist in Odisha, Kerala, Tamil Nadu and Andhra Pradesh. The rare-earth elements are essential for semiconductors, missile systems, and defence electronics (IREL, 2025).

Quartz and Silicon Reserves for Semiconductor Manufacturing- AI processors and semiconductor wafers are built on ultra-pure silicon. India has substantial reserves of quartz in Andhra Pradesh and Rajasthan. The availability of raw quartz is not the problem; rather, wafer fabrication environments and semiconductor-grade purification are. India lacks the large-scale semiconductor-grade purification and wafer fabrication facilities required for advanced chip manufacture, while having an abundance of quartz reserves suited for silicon production (IBM Research, 2024).



According to NITI Aayog (2024), mining constraints alone are not the main cause of India's strategic vulnerability, but rather shortcomings in downstream semiconductor integration, processing, and refining. Therefore, in addition to strategic International partnerships like the India-Australia Critical Mineral Partnership, India will need to develop domestic semiconductor-grade chemical processing capabilities, reliable fabrication infrastructure, and indigenous refining ecosystems in order to achieve semiconductor sovereignty (Australian Government Department of Industry, Science and Resources, 2024).

Conclusion

With significant ramifications for India's military autonomy and cyber sovereignty, the introduction of Project Glasswing and the wider trajectory of AI-enabled cyber warfare indicate a major shift in the strategic context of international security. This research has shown that AI is becoming a key tool for military decision-making, geopolitical influence, and strategic dominance rather than just a supporting technology. India faces an increasingly unstable security environment where defensive technological advancements by one state unintentionally create strategic insecurity for others, as China pursues "intelligentised warfare" and AI militarisation heightens the rivalry between India and Pakistan in South Asia. This dynamic is aptly captured by the Security Dilemma theory in international relations. The dual-use paradox is best illustrated by Project Glasswing, which is marketed as a defensive cybersecurity initiative that can find over 10,000 vulnerabilities in major operating systems and browsers. However, its underlying capabilities could be weaponised for aggressive cyber operations, undermining cyber deterrence and dangerously reducing crisis response times. Since advanced military large language models (LLMs) and AI-driven defence systems depend critically on secure semiconductor ecosystems, high-performance computing infrastructure, trusted data networks, and domestic chip fabrication definitively establishes that AI sovereignty is fundamentally inseparable from semiconductor sovereignty and compute sovereignty.

This paper defines "material zero-day vulnerabilities" as simultaneous flaws in software, hardware, firmware, and semiconductor supply chains that compromise long-term defence autonomy and decision sovereignty. Although the discovery of lithium in Jammu and Kashmir, rare earth sands in Odisha and Kerala, and significant quartz reserves in Andhra Pradesh and Rajasthan represent encouraging first steps towards upstream resources, they cannot achieve semiconductor sovereignty without the development of indigenous AI accelerators, wafer fabrication facilities, downstream processing capabilities, and semiconductor-grade chemical refinements. Constructivist viewpoints show how "sovereign AI" must become a normative identity for India's strategic autonomy doctrine, while realist IR theory argues that India's reliance on semiconductors Reliance on semiconductors represents a structural vulnerability in anarchic international systems, where technological superiority determines power distribution. Because AI-enabled systems could weaken nuclear deterrence by reducing strategic ambiguity, shortening decision-making deadlines, increasing automation pressure, and raising the risk of computational errors or unintentional escalation—particularly acute concerns given South Asia's history of rapid crisis escalation, as demonstrated during the Pulwama crisis, the implications for nuclear stability and strategic stability in South Asia are especially concerning. Although ethical principles emphasising human supervision and accountability are proposed by international governance frameworks under the UN Convention on Certain Conventional Weapons (CCW) and the IEEE Standards Association, these structures are still disjointed and insufficient to control rapidly developing military AI technologies.

This paper proposes a sovereignty-centred framework that integrates four interconnected pillars to support India's strategic autonomy in the emerging AI-driven security order: rapid expansion of domestic semiconductor manufacturing through the India Semiconductor Mission, with a focus on defence-grade chip fabrication and RISC-V open-source architectures; creation of sovereign compute infrastructure, including a national defence AI cloud independent of foreign-controlled platforms; and comprehensive cyber-defence modernisation with AI-driven vulnerability patching, zero-trust architecture for military networks, and systematic AI red-teaming of Indian military LLMs. India can only guarantee strategic autonomy, cyber resilience, and secure military AI deployment in future multidomain conflict scenarios while retaining significant human control over nuclear and conventional military assets through an all-encompassing, sovereignty-centered approach.

Reference

Anthropic. (2026, April 7). *Project Glasswing: Securing critical software for the AI era*. Anthropic.https://www.anthropic.com/glasswin

No Time. (2026, April 8). *What is Project Glasswing and what did it already find?* Medium. https://medium.com/no-time/what-is-project-glasswing-and-what-did-it-already-find-22fe48410b93

Anthropic. (2026, May 22). *Project Glasswing: An initial update*. Anthropic. https://www.anthropic.com/research/glasswing-initial-update

Priyanshu, A., Maurya, Y., & Hong, Z. (2024). AI governance and accountability: An analysis of Anthropic's Claude(arXiv:2407.01557). arXiv. https://arxiv.org/abs/2407.01557

Fan, H., Zhou, H., Huang, G., Raman, P., Fu, X., Gupta, G., Ram, D., Wang, Y., & Huan, J. (2024). HLAT: High-quality large language model pre-trained on AWS Trainium (arXiv:2404.10630). arXiv. https://arxiv.org/abs/

Economic Times. (2026, May 24). *Anthropic AI model finds over 10000 critical bugs across open-source software projects*. https://m.economictimes.com/tech/artificial-intelligence/anthropic-ai-model-finds-over-10000-critical-bugs-across-open-source-software-projects/articleshow/131292086.cms

Husain, A. (2021, November 18). *AI is shaping the future of war*. *PRISM, 9*(3). National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2846375/ai-is-shaping-the-future-of-war/

Collins, B. (2026, May 11). 'This is the tip of the iceberg': Google experts say they have seen hackers using AI to discover and weaponize a zero-day for the first time. TechRadar Pro. https://www.techradar.com/pro/security/this-is-the-tip-of-the-iceberg-google-experts-say-they-have-seen-hackers-using-ai-to-discover-and-weaponize-a-zero-day-for-the-first-time

RT News. (2017, September 1). *"Whoever leads in AI will rule the world": Putin to Russian children on Knowledge Day*. RT. https://www.rt.com/news/401731-ai-rule-world-putin/

Lee, K.-F. (2018). AI superpowers: China, Silicon Valley, and the new world order. Houghton Mifflin Harcourt.
https://books.google.com/books/about/AI_Superpowers.html?id=Xb9wDwAAQBAJ

Precedence Research. (2026, February 2). *Compound semiconductor market size, share and trends 2026 to 2035*. https://www.precedenceresearch.com/compound-semiconductor-market

Watling, J., & Roper, D. (2016, February). *ISR in 2035 and beyond: The role of information, surveillance and reconnaissance in future operations*. Royal United Services Institute.https://static.rusi.org/201602_op_isr_in_2035_and_beyond.pdf

King, A. (2024). *Digital targeting: Artificial intelligence, data, and military intelligence*. *Journal of Global Security Studies, 9*(2), ogae009. https://doi.org/10.1093/jogss/ogae009

Ranjan, O. (2022, December 2). *The PLA and intelligentized warfare – Analysis*. Eurasia Review. https://www.eurasiareview.com/02122022-the-pla-and-intelligentized-warfare-analysis/

Saeed, A. (2023, April 7). *Artificial intelligence and modern warfare: Comparative analysis of India and Pakistan*. Modern Diplomacy. https://moderndiplomacy.eu/2023/04/07/artificial-intelligence-and-modern-warfare-comparative-analysis-of-india-and-pakistan/

Amir, T. (2024, February 28). *Artificial intelligence at the helm: Revolutionizing India-Pakistan defense sectors – Analysis*. Eurasia Review. https://www.eurasiareview.com/28022024-artificial-intelligence-at-the-helm-revolutionizing-india-pakistan-defense-sectors-analysis/

Mansoor, S. (2024, June 24). *India's AI militarization: Security repercussions for Pakistan*. Russian International Affairs Council. https://russiancouncil.ru/en/analytics-and-comments/columns/military-and-security/india-s-ai-militarization-security-repercussions-for-pakistan/

Khurshid, T., & Zaman, H. (2024). *AI integration in Indian military: Appraisal of security apprehensions for South Asia*. *NDU Journal, 38*(1).

https://ndujournal.ndu.edu.pk/site/article/view/179

Fadilpašić, S. (2026, May 18). *Anthropic to present exposed Mythos flaws to global watchdog: Claims critical vulnerabilities found in every major operating system and web browser*. TechRadar.

https://www.techradar.com/pro/security/anthropic-to-present-exposed-mythos-flaws-to-global-watchdog-claims-critical-vulnerabilities-found-in-every-major-operating-system-and-web-browser

Rickli, J.-M. (2019). The destabilizing prospects of artificial intelligence for nuclear strategy, deterrence and stability. In V. Boulanin (Ed.), *The impact of artificial intelligence on strategic stability and nuclear risk: Volume I—Euro-Atlantic perspectives* (pp. 91–98). Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf

Topychkanov, P. (2020, April). *The impact of artificial intelligence on strategic stability and nuclear risk*. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2020-04/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov_1.pdf

Lu, M. (2025, January 6). *The value of the global semiconductor industry, in one giant chart*. Visual Capitalist. https://www.visualcapitalist.com/the-value-of-the-global-semiconductor-industry-in-one-giant-chart/

Visual Capitalist. (2023, November 16). *Semiconductor companies by industry revenue share 2023*. https://www.visualcapitalist.com/semiconductor-companies-by-industry-revenue-share-2023/

Berg, R. C., Ziemer, H., & Polo Anaya, E. (2024, May 15). *Mineral demands for resilient semiconductor supply chains: The role of the Western Hemisphere*. Center for Strategic and International Studies. https://www.csis.org/analysis/mineral-demands-resilient-semiconductor-supply-chains

TechRadar. (2026, April 8). *Anthropic to present exposed Mythos flaws to global watchdog: Claims critical vulnerabilities found in every major operating system and web browser*. https://www.techradar.com/pro/security/anthropic-to-present-exposed-mythos-flaws-to-global-watchdog-claims-critical-vulnerabilities-found-in-every-major-operating-system-and-web-browser

Kachwala, Z. (2026, May 28). *Anthropic to roll out Claude Mythos in coming weeks, launches Opus 4.8*. Reuters. https://www.reuters.com/business/anthropic-roll-out-claude-mythos-coming-weeks-launches-opus-48-2026-05-28/

Smith, R. (2026, February 22). *India joins America-led Pax Silica supply chain effort to build semiconductor talent and reduce reliance on China—agreement spans from rare earths to chipmaking tools*. Tom's Hardware. https://www.tomshardware.com/tech-industry/india-joins-america-led-pax-silica-supply-chain-effort-to-build-semiconductor-talent-and-reduce-reliance-on-china-agreement-spans-from-rare-earths-to-chipmaking-tools

Cruzes, S. (2026). *AI infrastructure sovereignty*. https://arxiv.org/abs/2602.10900

Wei, P., & Shu, W. (2026). *Preserving decision sovereignty in military AI: A trade-secret-safe architectural framework for model replaceability, human authority, and state control* (arXiv:2604.20867).

Tucker, P. (2019, March 20). *The newest AI-enabled weapon: "Deep-faking" photos of the Earth*. *Defense One*. https://www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/

Vincent Boulanin (Ed.). (2019). *The impact of artificial intelligence on strategic stability and nuclear risk: Volume I: Euro-Atlantic perspectives*. Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf

Moeed W. Yusuf. (2019, May). *The Pulwama crisis: Flirting with war in a nuclear environment*. *Arms Control Today*. https://www.armscontrol.org/act/2019-05/features/pulwama-crisis-flirting-war-nuclear-environme

Liang, X., & Klare, M. T. (2024, November 12). *Beyond a human "in the loop": Strategic stability and artificial intelligence*. Arms Control Association. https://www.armscontrol.org/issue-briefs/2024-011/beyond-the-loop

United Nations Office for Disarmament Affairs. (2025). *Lethal autonomous weapon systems*. United Nations.

https://www.unoda.org/en/our-work/emerging-challenges/lethal-autonomous-weapon-systems

IEEE Standards Association. (n.d.). *Autonomous and intelligent systems*. Retrieved July 2025.https://standards.ieee.org/initiatives/autonomous-intelligence-systems/

Ministry of Mines. (2023, February 9). *Geological Survey of India discovers lithium inferred resources in Jammu & Kashmir*. Government of India. https://mines.gov.in

IREL (India) Limited. (2025). *About IREL and rare earth mineral resources*. https://www.irel.co.in/

IBM Research. (2024, September 9). *A blueprint to accelerate India's semiconductor ambitions*. IBM.https://in.newsroom.ibm.com/blueprint-to-accelerate-India-semiconductor-ambitions

NITI Aayog. (2024, July 18). *Electronics: Powering India's participation in global value chains*. Government of India. https://www.niti.gov.in/node/1360

Commonwealth Scientific and Industrial Research Organisation (CSIRO). (2024, August 15). *International partnerships in the mineral world work to achieve real-world solutions*.https://www.csiro.au/en/news/All/Articles/2024/August/Australia-India-Partnerships-update

Ishika Mandal functioned as Research Intern at the Centre for Land Warfare Studies (CLAWS). She is currently pursuing a Master's degree in International Studies at Christ University (Central Campus), Bengaluru. Her academic interests focus on international relations, strategic affairs, and contemporary global security issues.