ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

NUCLEAR DETERRENCE AND ARTIFICIAL INTELLIGENCE: PRESERVING HUMAN CONTROL IN AN ERA OF STRATEGIC INSTABILITY

By
Ghazala Yasmin Jalil
Research Fellow
Arms Control & Disarmament Centre (ACDC), ISSI
Email: ghazala.jalil@issi.org.pk

Edited by
Malik Qasim Mustafa

August 21, 2026

(Views expressed in the brief are those of the author, and do not represent those of ISSI)

Artificial Intelligence (AI) is transforming all facets of life but especially revolutionizing warfare and defence. Major world powers have already begun the race to induct AI into modern warfare. AI-driven systems are increasingly transforming the nature of warfare and dominating modern battlefields.

There is also rapid integration of AI and machine learning into strategic weapons architecture and early-warning systems. While it affords many advantages, it also creates profound risks of accidental escalation and inadvertent warfare. At the same time, the rapid integration of AI in modern warfare and strategic weapons architecture remains largely unregulated. The nexus between nuclear deterrence and AI is very delicate. While there seems to be consensus that AI must not be given control over missile launches, there is an overall entanglement of AI within strategic weapons complexes. It is important to examine the role of AI in nuclear deterrence and future nuclear postures. The rapid AI revolution in modern warfare, defence, and weapons has meant that international law has not kept up with the pace of technology. Since AI introduces vulnerabilities to accidental escalation, global stability demands a binding international agreement that ensures meaningful human control over all nuclear launch decisions.

AI in Nuclear Deterrence

AI has potential use in several areas of nuclear deterrence architecture, including early warning; Intelligence, Reconnaissance and Surveillance (ISR); command and control; delivery systems; and the cyber domain in nuclear facilities.

© ISSI 2026 • All Rights Reserved

AI enhances ISR and early warning systems by rapidly fusing vast streams of data from satellites, sensors, and autonomous platforms such as UAVs and UUVs to detect nuclear threats, missile launches, and facility anomalies far faster than humans. By applying machine learning to cross-analyze intelligence, evaluate adversary capabilities, and simulate response scenarios, AI provides decision-makers with superior situational awareness and more accurate threat assessments. Crucially, these integrated technologies expand the remote-sensing footprint and give decision-makers extra time to deliberate and react during high-stakes crises.

There is a consensus among major powers that AI should not be integrated into nuclear command and control systems. AI does, however, play a role in augmenting cybersecurity measures against cyber-attacks on nuclear facilities and architecture. AI algorithms can help in rapidly identifying threats and responding to cyber breaches, helping minimize damage from cyber-attacks.

A significant degree of functional autonomy is already embedded across modern nuclear delivery platforms. Strategic assets like Intercontinental Ballistic Missiles (ICBMs), cruise missiles, and Submarine-Launched Ballistic Missiles (SLBMs) function automatically post-launch, relying on pre-programmed guidance systems to control their ascent and strike designated targets.[1] In fact, missile guidance, navigation, and control (GNC) systems were among the earliest military applications of automated closed-loop feedback systems. Within these delivery architectures, AI primarily acts as a qualitative force multiplier. Major nuclear powers are progressively integrating machine learning and semi-autonomous missile architectures into their next-generation capabilities.[2]

AI is also being integrated in non- nuclear domains that nevertheless affect strategic stability and escalation risk. These include the cyber domain, electronic and information warfare; air defences, the space domain, physical security of nuclear facilities and assets. The most significant integration of AI is in the ballistic missile defence systems that have a direct impact on nuclear deterrence and escalation risks. While missile defences have used AI-driven technology like automatic target recognition (ATR), which helps detect and target incoming missile threats, today tremendous advancements in AI can make missile defences more efficient, fast and precise in targeting threats. Ultimately, advances in AI have made offensive and defensive systems more efficient.

1 Erik Sand, "Strategy in the New Missile Age," *Security Studies* 35, 1 (2026): 1–38. doi:10.1080/09636412.2025.2604503.

2 Stefanovich, D. V. "Disruptive Technologies as a Source of Strategic Destabilization," *Russia in Global Affairs* 23, 1 (2025): 176–187, https://eng.globalaffairs.ru/articles/disruptive-tech-stefanovich/.

© ISSI 2026 • All Rights Reserved

AI and the Security Landscape

The advent of emerging technologies is changing the nature of warfare – from non-contact warfare; the increasing dominance of drones on the battlefield; to militarization of outer space; heightened risks from cyber-attacks, hypersonic missiles, and the incorporation of AI in weapon systems. The pursuit of hypersonic missiles by major powers like the US, Russia and China, as well as India in the South Asian region, is shrinking decision windows from hours to minutes. The incorporation of AI-driven systems is changing the battlefields. Increasing integration of AI in military systems – nuclear or non-nuclear – has the potential to affect nuclear deterrence and escalation dynamics.

Potential dangers of AI in the military domain include biased or poisoned data, compressed decision-making timelines, and perceptions. AI-driven military decision-support systems (DSSs) under compressed timelines may push decision-makers to make faster decisions, increasing the risk of miscalculation and errors leading to nuclear escalation.[3] Moreover, AI-driven operations - such as algorithmic cyberattacks or space strikes targeting dual-capable infrastructure - can cause adversaries to misinterpret non-nuclear threats as attempts to blind their nuclear deterrence ecosystem. In addition, vulnerabilities in AI systems, including algorithmic bias, brittleness, automation bias, and susceptibility to adversarial cyber exploits, can generate false alerts, distort situational awareness, and may trigger inadvertent nuclear responses.[4] Potentially exploiting vulnerabilities in data, bias, and deliberate data poisoning, opponents or malicious non-state actors could use AI-enabled cyber tactics to manipulate targeting data, sabotage early warning sensors and radars, or hack command, control, and communications networks. This could trigger unintended nuclear escalation.

In his research, James Johnson highlights how progress in AI could enable adversaries to target nuclear forces and Command, Control, and Communication (C3) networks using AI-enhanced cyber capabilities, and deploy drone swarms against strategic military targets. Furthermore, he warns that AI algorithms might misread enemy signals, introducing dangerous ambiguity during a high-stakes nuclear crisis.[5]

Nuclear crisis management is already constrained by severe time pressure. Integrating AI even in basic sensing and targeting roles threatens to further shorten timelines, compressing the decision window, increasing chances of miscalculation and further raising crisis instability. As Sahar Khan argues: “Even

[3] Vladislav Chernavskikh and Jules Palayer, “Impact of Military Artificial Intelligence on Nuclear Escalation Risk”, SIPRI Insights on Peace and Security, No. 2025/06, June 2025, https://www.sipri.org/sites/default/files/2025-06/2025_6_ai_and_nuclear_risk.pdf.

[4] Chernavskikh and Palayer, “Impact of Military Artificial Intelligence on Nuclear Escalation Risk.”

[5] James Johnson, *AI and the Bomb: Nuclear Strategy and Risk in the Digital Age* (Oxford University Press, 2023).

© ISSI 2026 • All Rights Reserved

if nuclear forces stay under strict human control, perceptions of vulnerability in conventional forces can influence nuclear decision-making…. AI doesn't need to be inside nuclear command and control to impact nuclear stability. It only has to change perceptions of survivability. The stability–instability paradox becomes more pronounced as battlefield transparency improves and reaction times decrease."[6]

Furthermore, leveraging AI in satellite surveillance and intelligence gathering compromises the stealth of strategic assets, including nuclear-armed submarines and mobile launching platforms. This heightened vulnerability could incentivize nations to deploy or launch their arsenals early in a crisis to prevent an enemy pre-emptive strike.[7] By enhancing an adversary's ability to track and neutralize these hidden retaliatory systems, AI directly undermines second-strike capabilities. This heightened vulnerability erodes overall strategic stability, creating a dangerous "use it or lose it" dynamic where states may feel compelled to deploy or launch their nuclear arsenals preemptively to avert an imminent disarming strike.[8]

AI-Nuclear Nexus in South Asian Context

The impact of AI integration in the military domain is more pronounced in South Asia. India is aggressively integrating AI across all three of its land, air, and naval warfare frameworks to enhance operational speed, surveillance, and precision targeting. India has established dedicated defense agencies such as the Defence AI Council (DAIC) and the Defence AI Project Agency (DAIPA/AI4AD) to systematically embed AI into military strategy and doctrine. DAIC intends to develop 25 defence-specific AI products in 2025 alone.[9] India also established the Centre for AI and Robotics (CAIR) to develop AI-based net-centric systems for C3 and drones, and has modernized the robotic maintenance system of the Indian Air Force. India's push for integration of AI in defence systems is reflected in dozens of ongoing projects and significant investment. The 2017 Joint Doctrine of Indian Armed Forces envisages leveraging disruptive technologies for military purposes. India's Land Warfare Doctrine also talks about integrating AI into operations. India is also combining indigenous research with external

6 Sahar Khan, "AI is Quietly Reshaping Nuclear Risk in South Asia," Asia-Pacific Leadership Network," March 27, 2026,

7 Ghazala Yasmin Jalil, "Artificial Intelligence and Nuclear Weapons: Way to the Future or Path to Disaster?" ISSI, December 11, 2023, https://issi.org.pk/issue-brief-on-artificial-intelligence-and-nuclear-weapons-way-to-the-future-or-path-to-disaster/

8 Chernavskikh and Palayer, "Impact of Military Artificial Intelligence on Nuclear Escalation Risk."

9 Yasir Hussain and Dalir Khan, "South Asia's AI Arms Race," January 30, 2025, https://ciss.org.pk/south-asias-ai-arms-race/

© ISSI 2026 • All Rights Reserved

technology partnerships with countries such as Israel and the US to deploy autonomous systems, predictive data analytics, and machine-learning tools across all three of its armed services.[10]

Pakistan has also tried to keep up with the development of AI technologies. In 2020, the Pakistan Air Force (PAF) formed the Centre for Artificial Intelligence and Computing (CENTAIC) for AI research that focuses on military and civilian applications. The Pakistan Army formed the Army Centre of Emerging Technologies within the Cyber Command in order to develop AI in cybersecurity. In addition, Pakistan has collaborated with China to develop AI in military systems like drones that are effective in targeting and reconnaissance roles. However, Pakistan's investment in AI-driven military systems remains minimal in comparison to India, which is massively investing in research and development of AI-driven military systems.

The integration of AI into South Asia's strategic dynamics seriously threatens the delicate balance of nuclear deterrence between India and Pakistan. Due to geographical proximity, missile flight times are as short as 3 to 5 minutes, leaving minimal room for detection, verification, and response. As India advances its AI capabilities in predictive analytics, unmanned systems, and ISR, its enhanced counterforce and precision-targeting capacity could erode mutual vulnerability. This technological advantage risks emboldening aggressive doctrinal shifts, such as Launch-on-Warning postures or preemptive decapitation strategies against Pakistan, thereby lowering the nuclear threshold in South Asia.[11]

Pakistan may face increasing pressure to integrate AI into its own military systems in order to reduce the AI-driven asymmetry with India and to maintain its Full Spectrum Deterrence. The integration of AI into decision-making ecosystems compresses timelines, resulting in increased crisis instability. Historical precedents from defining moments such as Soviet Lieutenant Colonel Stanislav Petrov's human intervention during a 1983 automated false alarm to the "accidental" firing of 2022 BrahMos missile by India highlight a critical vulnerability - how quickly a technical error can escalate without robust safeguards and human judgement.

Governance Challenges

There is no serious effort to negotiate legally binding limits on AI in nuclear weapons architectures. Existing frameworks, such as the US-led Political Declaration on Responsible Military Use of Artificial Intelligence (REAIM), establish non-binding, voluntary norms that may collapse under high-stress

[10] Summar Iqbal Babar1 and Malaika Sarwar, "AI-Militarization in South Asia: A Comparative Analysis," BTTN Journal, Vol 4, Issue 1, July, 2025.

[11] Babar and Sarwar, "AI-Militarization in South Asia: A Comparative Analysis."

© ISSI 2026 • All Rights Reserved

geopolitical crises. In recognition of AI's potential to fuel unintended escalation in decision processes, UNGA adopted a resolution in October 2025 which urged that "human control and oversight is maintained over command, control and communications systems of nuclear weapons, including those that integrate artificial intelligence technology."[12] It also urged countries to publish national policies and doctrines explicitly affirming this. Thus, at the international institutional level, debate is beginning to take shape. In July 2026, more than 200 Nobel laureates, scientists, and diplomats gathered in Rome, warning over the dangers of the AI-nuclear nexus and erosion of human control over existential decisions, and at the same time urged world leaders to stop dual arms races.[13] However, efforts to regulate AI in nuclear contexts are sporadic and inadequate.

Recommendations and Policy Options

The risks associated with the AI-nuclear nexus require effective measures at both the international and regional levels that may help reduce the risks of inadvertent escalation while allowing states to benefit from AI applications.

International Level

- **Institutionalise Human Control:** Nuclear-armed states should commit to maintaining meaningful human control over all decisions involving the use of nuclear weapons and prohibit fully autonomous nuclear decision-making. Such commitments should be incorporated into national policies and doctrines as well as codified in the form of legally binging treaty.

- **Develop an international framework for AI and nuclear risk reduction:** States should work through the UN and relevant disarmament forums towards common principles governing AI in nuclear command, control and communications, including safeguards, risk assessments and accountability mechanisms. Pakistan's Permanent Mission in Geneva and New York could take lead in this regard.

- **Promote transparency and confidence-building:** Nuclear-armed states should develop appropriate transparency measures and strategic communication mechanisms to reduce

12 UN General Assembly 16 October 2025https://docs.un.org/en/A/C.1/80/L.56

13 "Rome Declaration Calls for a New Global Ethic on Artificial Intelligence and Nuclear Weapons," *Pressenza*, July 16, 2026, https://www.pressenza.com/2026/07/rome-declaration-calls-for-a-new-global-ethic-on-artificial-intelligence-and-nuclear-weapons/

© ISSI 2026 • All Rights Reserved

misperceptions concerning the integration of AI into nuclear and nuclear-related systems, while protecting legitimate national-security requirements.

Regional Level

- **Establish AI-specific confidence-building measures:** India and Pakistan should explore bilateral arrangements to address the risks created by AI-enabled surveillance, early-warning, autonomous systems and decision-support technologies that could affect strategic stability.
- **Develop a bilateral code of conduct:** The two countries could initiate dialogue on a code of conduct for military AI, particularly concerning systems with potential implications for nuclear deterrence, crisis stability and decision-making timelines.
- **Create dedicated crisis-communication channels:** Existing communication mechanisms should be supplemented, where feasible, with channels for addressing AI-related incidents, misperceptions or technical failures during crises.
- **Promote Track 1.5 and Track 2 Dialogue:** Regular engagement among policymakers, military experts, scientists and strategic communities should be encouraged to build mutual understanding of emerging military AI capabilities and identify practical measures to prevent inadvertent escalation.

Conclusion

The integration of AI into military systems and deterrence architectures carries greater dangers in South Asia, where India and Pakistan are geographically contiguous and where missile flight times are 3-5 minutes. It has the potential to influence nuclear escalation even when the integration occurs in non-nuclear weapons systems such as UAVs, ISR, and early warning systems. Integration of AI in military systems may compress decision-making timelines, potentially increasing the risk of miscalculation during a crisis. In South Asia, AI-driven enhanced precision would heighten India's counterforce and preemptive strike capabilities. It can also undermine the integrity of second-strike capabilities and, thus, affect strategic stability.

While the integration of AI in military systems affords advantages, it is highly risky to incorporate it into nuclear deterrence architectures. Nuclear weapons states need to enact measures to ensure regulation of AI. At the international level, states need to create bilateral hotlines and adopt a multilateral framework to ban fully autonomous nuclear decision-making; advocate for mandatory "human-in-the-loop" protocols to ensure AI never gets into nuclear command and control systems;

© ISSI 2026 • All Rights Reserved

and develop transparency measures to build trust between nuclear-armed states. In South Asia, India and Pakistan need to talk about and implement bilateral confidence-building measures, as well as develop a code of conduct for AI in military systems, especially in nuclear deterrence ecosystems, promote 1.5 and Track 2 diplomacy dialogues, and establish communication channels for military AI-related matters.

© ISSI 2026 • All Rights Reserved