

THE ALGORITHMIC KILL CHAIN

AI in Warfare and Pakistan's Preparedness



Authored by: Azhar Zeeshan

Edited by: SAT Research Desk

Published by South Asia Times | southasiatimes.org

Authored by: Azhar Zeeshan
Edited by: SAT Research Desk



ABOUT THE AUTHOR

Azhar Zeeshan is a researcher at the Centre for Aerospace and Security Studies (CASS), Lahore. His areas of interest are religious extremism and emerging technologies in warfare. He holds an MPhil in History from Quaid-i-Azam University and a BS (Hons) in International Relations from the University of Peshawar.

ABOUT SAT BRIEFS

SAT Briefs are the weekly original research of South Asia Times. Each brief examines a pressing question in regional and international affairs, advances an evidence-based argument and sets out policy options for decision-makers. The views expressed are those of the author.

Suggested citation: Azhar Zeeshan, *The Algorithmic Kill Chain: AI in Warfare and Pakistan's Preparedness*, SAT Brief No. 04 (Islamabad: South Asia Times, October 2026).

KEY ARGUMENT

Artificial intelligence (AI) has not changed the logic of targeting, but it has transformed its tempo. From the machine-learning analysis of Pakistani phone metadata in the drone era, through Israel's Lavender and Gospel systems in Gaza, to the 13,000 targets the United States struck in Iran in 38 days, algorithms now compress the journey from detection to destruction into minutes. The same speed multiplies error and diffuses responsibility: the strike on a girls' school in Minab showed how a stale database entry, moving through a process built for speed, can kill more than 150 people. South Asia has already fought its first sensor-network war, in May 2025, and machine-speed decision cycles between nuclear-armed rivals raise the risk of inadvertent escalation. Judged against Andrew Krepinevich's four dimensions of disruptive military innovation, Pakistan has laid credible foundations through the National Centre of Artificial Intelligence (NCAI), the Pakistan Air Force's (PAF) Centre of Artificial Intelligence and Computing (CENTAIC), the National Aerospace Science and Technology Park (NASTP) and the National AI Policy 2025. It is not yet ready. The gap lies not in algorithms or hardware but in doctrine, joint integration and an innovation ecosystem, and closing it will decide whether Pakistan masters this revolution or remains on its receiving end.

CONTENTS

EXECUTIVE SUMMARY..... 5

1. INTRODUCTION..... 6

2. THE ANALYTICAL LENS: DISRUPTIVE MILITARY INNOVATION..... 7

3. THE ANCHOR EVENT: MINAB AND THE 38-DAY KILL CHAIN..... 9

4. THE CONTEXT: AI AND THE CHARACTER OF WARFARE..... 11

5. CONNECTING THE DOTS..... 14

6. HISTORICAL ANCHOR: IGLOO WHITE..... 15

7. PAKISTAN’S AI LANDSCAPE AND READINESS..... 17

8. POLICY RECOMMENDATIONS FOR PAKISTAN..... 19

9. ASSESSMENT: WHAT WE KNOW AND WHAT TO WATCH..... 21

10. CONCLUSION..... 23

ENDNOTES..... 24

EXECUTIVE SUMMARY

- On 28 February 2026, in the opening hours of the United States (US)–Israeli war on Iran, a US cruise missile destroyed a girls' elementary school in Minab, killing between 156 and 175 people, most of them children.^[1,2] US targeting data still coded the building as military, although it had been walled off from an adjacent Revolutionary Guard base for roughly a decade.^[3]
- The war's defining feature was speed. The United States struck more than 13,000 targets in 38 days, about one every four minutes, with AI-enabled systems such as Palantir's Maven Smart System helping to nominate targets and pair weapons.^[4]
- This tempo has a lineage. Pakistan's tribal districts were among the first places where population-scale data was algorithmically mined to nominate people for lethal attention, through the US National Security Agency's (NSA) SKYNET programme.^[5] Israel's Lavender system later flagged as many as 37,000 Gazans as suspected militants, with human review reportedly lasting about 20 seconds.^[6]
- The common failure is institutional, not merely algorithmic: flawed or outdated data meeting a process in which human verification has been compressed to seconds. Speed does not cause the error, but it multiplies it.
- South Asia entered this regime in May 2025, when both India and Pakistan claimed data-fused kill chains and AI-assisted targeting.^[7,8] Between nuclear-armed rivals, that compression raises the risk of inadvertent escalation.
- Pakistan has built foundations: the National Centre of Artificial Intelligence, the PAF's CENTAIC, NASTP and the National AI Policy 2025.^[9,10] Measured against Krepinevich's framework, it remains at an early and uneven stage. It should harness commercial capital, create a procurement pathway for industry, build talent, choose niches, govern targeting data, and pursue human-control commitments with India.

1. INTRODUCTION

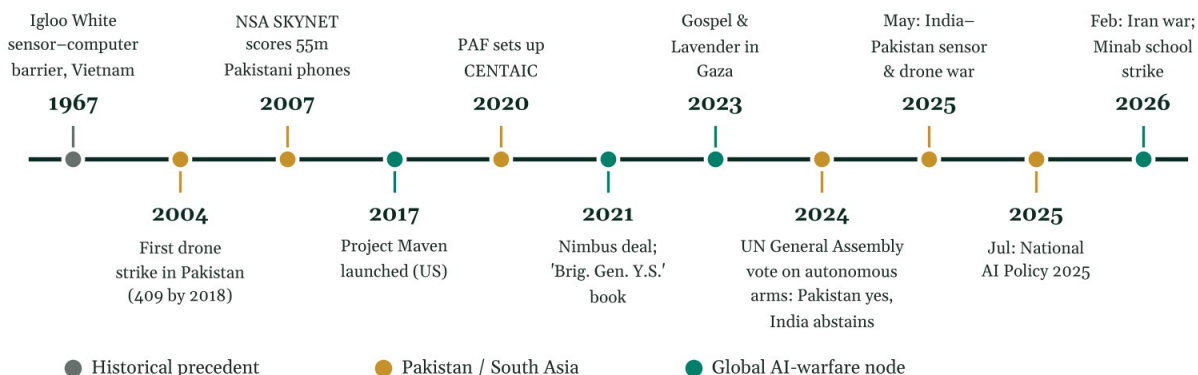
Long before artificial intelligence dominated headlines, it was already at work in Pakistan, particularly in the context of warfare. From 2004 onwards, surveillance drones hovered almost constantly over Waziristan and adjoining areas, and Pakistan's National Counter Terrorism Authority recorded 409 drone attacks on Pakistani territory by 2018.^[1] Behind them, intelligence agencies were already using machine learning to sift data and nominate targets. In this regard, Pakistan became a testing laboratory for the AI-enabled conflicts that followed. Those experiments have since matured into a new way of war. From Gaza to Iran, algorithms now sift surveillance data, nominate targets and compress the journey from detection to destruction into minutes, sometimes seconds.

The speed is dazzling, but so are the dangers. On the first day of the 2026 US–Israeli war on Iran, a US missile struck a girls' school in Minab whose conversion from military use a decade earlier had never been reflected in US targeting data.^[3] The incident is the anchor of this brief, because it shows in a single event both the power and the hazard of algorithmic warfare.

Pakistan once stood at the receiving end of this revolution. The question now is whether it can stand among those who master it. Drawing on Andrew Krepinevich's concept of disruptive military innovation, this brief argues that the answer depends less on who owns AI than on who can turn it into operational effectiveness. It examines how AI is changing warfare, connects the cases of Waziristan, Gaza, Iran and the India–Pakistan crisis of May 2025, identifies the hazards they reveal, and assesses how prepared Pakistan is for what lies ahead.

From Waziristan to Minab: Connecting the Dots

Milestones in AI-enabled targeting and Pakistan's response, 1967–2026



Sources: P. N. Edwards (1996); Dawn (2018); Ars Technica (2016); Quwa (2020); +972 Magazine (2024, 2025); UN General Assembly (2024); Observer Research Foundation (2025); The Express Tribune (2025); Arms Control Today (2026).

2. THE ANALYTICAL LENS: DISRUPTIVE MILITARY INNOVATION

This brief adopts Andrew F. Krepinevich's framework of disruptive military innovation, developed in *The Origins of Victory*, as its principal conceptual foundation. ^[12] The framework explains how emerging technologies reshape military power and why technological advancement alone does not translate into battlefield superiority. Its central proposition is that military advantage depends on a state's ability to recognise the strategic implications of emerging technologies, experiment with their applications, adapt organisational structures and operational doctrines, and integrate new capabilities into effective ways of warfare.

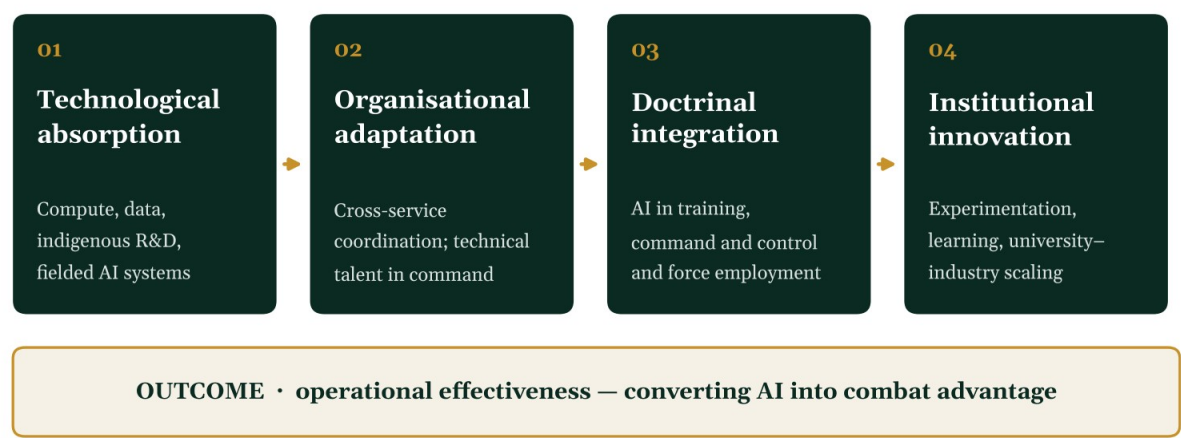
Applied to AI, the framework challenges the assumption that acquiring sophisticated algorithms, unmanned platforms or AI-enabled systems automatically generates a decisive advantage. AI is better understood as an enabling technology whose strategic value emerges through integration across intelligence, surveillance and reconnaissance (ISR), command and control, targeting, logistics, cyber operations and human-machine teaming. By compressing the intelligence-to-decision-to-action cycle, AI can improve the speed and quality of military responses. These advantages remain contingent, however, on reliable data, computing infrastructure, trained personnel, resilient communications and appropriate human oversight.

The decisive question is not who possesses AI, but who can convert its potential into operational effectiveness.

The framework is operationalised through four interrelated dimensions. **Technological absorption** concerns computing infrastructure, data, indigenous research and development, and AI-enabled military capabilities. **Organisational adaptation** examines whether institutions can overcome bureaucratic resistance, coordinate across services and bring technical expertise into operational decision-making. **Doctrinal integration** assesses whether AI is incorporated into training, command structures, force employment and multi-domain operations rather than treated as an isolated addition. **Institutional innovation** evaluates the capacity to experiment, learn from operational experience, collaborate with universities and industry, and scale successful applications. Pakistan's preparedness must therefore be measured not by the platforms it acquires, but by its ability to build an integrated military innovation ecosystem.

The Analytical Lens: Disruptive Military Innovation

Krepinevich's four dimensions, as operationalised in this brief



Source: SAT adaptation of A. F. Krepinevich, *The Origins of Victory* (Yale University Press, 2023).

3. THE ANCHOR EVENT: MINAB AND THE 38-DAY KILL CHAIN

Operation Epic Fury began on 28 February 2026. By 7 April, the White House reported that US forces had struck more than 13,000 targets in Iran in 38 days, including more than 2,000 command-and-control targets, 1,500 air-defence targets and 1,450 industrial-base targets.^[4] That is about 342 strikes a day. US officials said the Pentagon used the Maven Smart System, an AI-powered data-fusion and decision-support platform built by Palantir, to identify top-priority targets and to help choose weapons.^[4] The Pentagon had raised the ceiling of Palantir's Maven contract to nearly US\$1.3 billion through 2029, and by then the platform had more than 20,000 active users across the US military.^[3] Kill chain, in military usage, is the process by which forces move from detecting a target to striking it; systems like Maven are designed to make that chain shorter.

The same opening day produced the war's most consequential error. The Shajareh Tayyebbeh girls' school in Minab had once formed part of an Islamic Revolutionary Guard Corps (IRGC) naval compound. Between 2013 and 2016 it was physically separated from the base, with a fence, separate street entrances and civilian markings, and satellite imagery showed a school sports pitch by 2017.^[3,2] According to a legal analysis of the strike, outdated Defense Intelligence Agency target coding still listed the building as part of the military installation.^[3] Arms Control Today reported a preliminary Central Command finding that US intelligence maps did not show the conversion, and that the school had entered an AI-generated target list without adequate human supervision. The same report notes that *The New York Times*, citing officials, said the error was "unlikely to have been the result of new technology" and attributed it to "human error in wartime".^[4] In September 2026, the United Nations (UN) Independent International Fact-Finding Mission on Iran found reasonable grounds to believe the United States had "failed in its obligation to do everything feasible to verify" that the school was a military objective. The White House rejected the finding.^[1]

WHAT IS CONFIRMED — AND WHAT IS NOT

Confirmed: the date, the location, the US munition, the building's civilian conversion and the stale target coding.^[2,3] **Disputed:** whether algorithmic target nomination, rather than a human database failure, was decisive. **SAT's reading:** the distinction matters less than it appears. A stale database entry survived a process engineered for speed, and nobody in the loop had the time, or the incentive, to run the simple public check that would have caught it.

The Tempo Shift

Average interval between strikes in two US campaigns

5.4 days

US drone campaign in Pakistan, 2008–2012

336 attacks in five years (National Counter Terrorism Authority)

4.2 minutes

US campaign against Iran, 28 Feb – 7 Apr 2026

More than 13,000 targets struck in 38 days

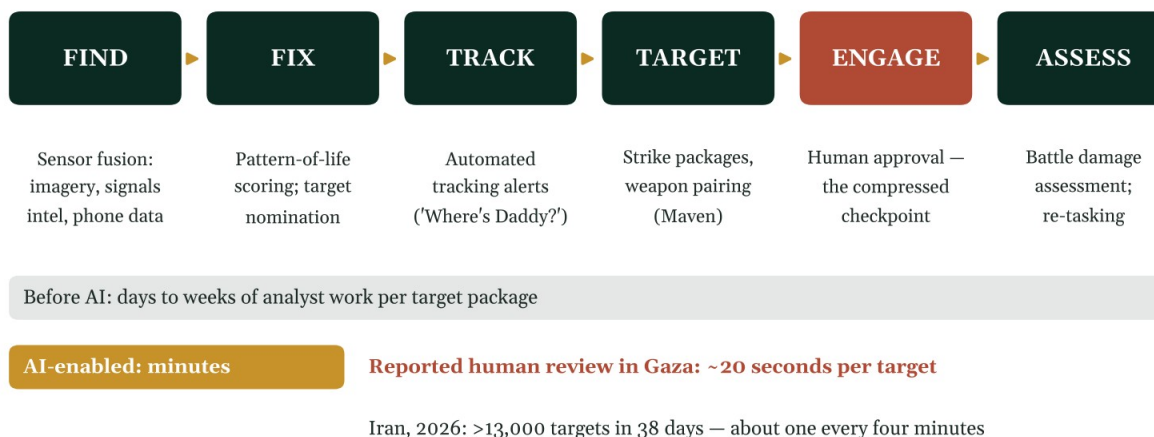
Sources: Dawn, 9 November 2018; Arms Control Today, May 2026. SAT calculation. The campaigns differ in aims, scale and legal basis; the comparison illustrates tempo, not equivalence.

4. THE CONTEXT: AI AND THE CHARACTER OF WARFARE

AI is transforming warfare from a contest decided mainly by firepower, manpower and industrial capacity into one increasingly shaped by data, computational speed and the ability to decide faster than an adversary. It is doing so along four axes: a faster kill chain; wider use of autonomous and semi-autonomous systems, including swarms of inexpensive platforms that can saturate sophisticated air defences; multi-domain sensor fusion across air, land, sea, space and cyberspace; and cheaper access to precision for smaller states, as the Russia–Ukraine war has shown. None of this abolishes the principles of war. It also creates new vulnerabilities: corrupted data, spoofed sensors, jamming and cyber intrusion against the networks on which AI depends. Three data points, drawn from intelligence history, the conduct of war and regional military practice, give this shift its strategic shape.

How AI Compresses the Kill Chain

The find–fix–track–target–engage–assess (F2T2EA) cycle and where algorithms now sit inside it



Sources: Y. Abraham, +972 Magazine (2024); M. T. Klare, Arms Control Today (2026). SAT schematic; durations illustrative, not to scale.

4.1 Waziristan as the first laboratory

Of the 409 drone attacks Pakistan's counter-terrorism authority recorded between 2004 and 2018, which killed 2,714 people, 336 took place between 2008 and 2012 alone.^[11] Around the same time, the US National Security Agency's SKYNET programme, revealed in Snowden documents published in 2015, applied machine-learning analysis to the mobile-phone metadata of roughly 55 million people in Pakistan to score individuals as likely militant couriers.^[5,14] The NSA claimed a false-positive rate as low as 0.008% in some tests; others reached 0.18%, which across 55 million people could mislabel about 99,000. The system reportedly flagged Al Jazeera's Islamabad bureau chief, Ahmad Zaidan, as a potential target.^[14]

No public evidence ties a specific drone strike to SKYNET output. The defensible claim is narrower but still significant: Pakistan's tribal districts were among the first places where population-scale data was algorithmically mined to nominate people for lethal attention.

4.2 Gaza and the industrialised target bank

Israel's campaign in Gaza since 7 October 2023 has been the most intensive use of AI-assisted targeting yet documented. Investigative reporting by +972 Magazine and Local Call, based on Israeli intelligence sources, described three systems. ^[6] **The Gospel** marks buildings and structures. **Lavender** marks people: at its peak it flagged as many as 37,000 Palestinians as suspected militants. **"Where's Daddy?"** tracks those individuals and alerts officers when they enter their family homes. Sources said human reviewers often spent about 20 seconds per target, mainly to confirm the target was male, acting as a "rubber stamp", and that the system was regarded as making errors in roughly 10% of cases. ^[6] The Israeli military disputes this characterisation and describes such systems as tools that assist human analysts.

The intellectual blueprint was public. In 2021, a book titled *The Human-Machine Team*, published under the pen name "Brigadier General Y.S.", argued for a machine that could rapidly generate thousands of potential targets in wartime. It described the problem such a machine would solve as:

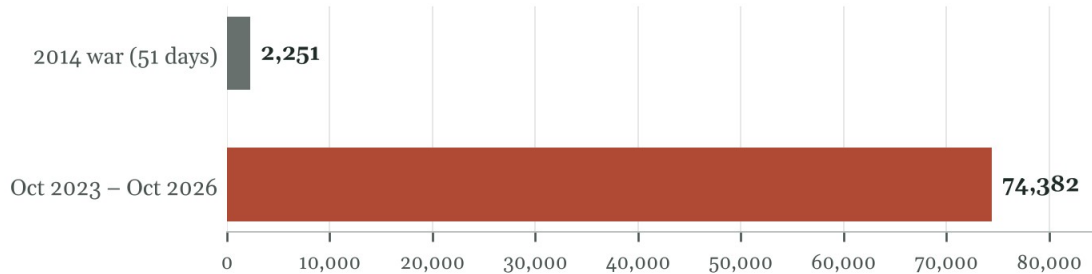
"...a human bottleneck for both locating the new targets and decision-making to approve the targets."^[6]

The Guardian later identified the author as Yossi Sarial, then commander of Israel's elite intelligence Unit 8200. ^[15]

The human toll gives this context its weight. Israel's 2014 Gaza war killed 2,251 Palestinians, according to the UN. ^[16] By 12 October 2026, Gaza's Ministry of Health reported 74,382 Palestinians killed since October 2023. ^[17] In September 2025, the UN Independent International Commission of Inquiry concluded that Israel has committed genocide in Gaza; Israel rejects the finding. ^[18] AI-enabled targeting cannot alone explain the difference between these figures: political intent, rules of engagement, permitted civilian harm and the duration of the war all matter. What the evidence supports is that automated target generation removed a constraint, the limited supply of vetted targets, that had previously capped the pace of bombardment.

The Scale of Killing in Gaza

Palestinians killed: the 2014 war versus the war since October 2023



Sources: UN OCHA, 23 June 2015 (2014 war); Gaza Ministry of Health, as reported by *The Express Tribune*, 12 October 2026. Durations differ greatly; AI-enabled targeting is one contributing factor among several and cannot alone explain the difference.

The supply chain is corporate. In 2021, Israel signed the US\$1.2 billion Project Nimbus cloud contract with Google and Amazon.^[19] In May 2025, Microsoft acknowledged providing AI and cloud services to the Israeli military, while saying it had found no evidence they were used to harm people in Gaza.^[20] In September 2025, after reporting that Unit 8200 stored intercepted Palestinian phone calls on its Azure cloud, Microsoft disabled certain subscriptions held by Israel's Ministry of Defence.^[21] Commercial technology firms are now part of the targeting infrastructure, and their terms of service have become a lever of wartime policy.

4.3 May 2025: South Asia's first sensor-network war

The India–Pakistan air battle of 7 May 2025 involved an estimated 110 aircraft. Reuters, citing US officials, reported that Pakistani J-10s downed at least one Indian Rafale. Four Pakistani officials told Reuters that Pakistan had linked air, land and space sensors into a "kill chain". A Pakistani-developed system, Data Link 17, connected Chinese-built fighters to a Swedish-made airborne surveillance aircraft, allowing J-10s to receive radar pictures while keeping their own radars off. Indian officials attributed the loss mainly to an intelligence error about the range of the Chinese PL-15 air-to-air missile. Greg Bagwell of the Royal United Services Institute (RUSI) observed that "the winner in this was the side that had the best situational awareness".^[7]

India, for its part, says it used AI during Operation Sindoor. Lt Gen Rajiv Sahni stated that the army processed 26 years of data through AI to predict where Pakistani guns and missile units would be located, with a reported accuracy above 94%.^[8] India alleged that Pakistan launched 300 to 400 drones against 36 locations on 8–9 May, and India used Israeli-made Harop loitering munitions against Pakistani air-defence sites.^[22] Most of these figures are claims by interested parties and remain unverified. The pattern is still clear: both sides now describe military success in the language of data fusion and algorithmic targeting.

5. CONNECTING THE DOTS

Viewed separately, these are a drone campaign, a war crimes controversy, a corporate ethics story and a dogfight. Viewed as a system, they reveal three things none of them shows alone.

First, the targeting logic is continuous; the tempo is not. SKYNET, Lavender and Maven apply the same idea: infer hostile identity or function from data patterns at population scale, then nominate targets for human approval. What changed between Waziristan and Minab is speed. The interval between strikes fell from about five days in Pakistan's peak drone years to about four minutes over Iran. Krepinevich would recognise the pattern: the technology matured over two decades, but the disruption came when organisations rebuilt their processes around it.

Second, the failure mode is shared, and it is human-institutional. SKYNET's false positives, Lavender's reported 10% error rate and Minab's stale database entry are not cases of rogue machines. They are cases of flawed or outdated data meeting a process in which human verification has been compressed to seconds. At low tempo, a bad data point costs one wrong strike that analysts may catch. At high tempo, it is replicated across hundreds of strikes before anyone looks back.

Speed does not cause the error, but it multiplies it.

Third, the edge goes to integration, not possession. Pakistan's best recent military performance, as described by its own officials and by Reuters, came not from frontier AI but from integrating imported Chinese and Swedish platforms through an indigenous data link.^[7] That is Krepinevich's argument in miniature. It also carries a warning. The same integration that rewards situational awareness compresses decision time between two nuclear-armed states, where an erroneous machine-generated assessment could accelerate a crisis before political leaders fully understand it. Meaningful human control over consequential decisions, reliable verification and clear accountability must therefore remain central to military AI governance.

RED TEAM: THE STRONGEST ALTERNATIVE READINGS

- **Gaza:** the scale of death reflects political decisions and permissive rules of engagement; AI was an accelerant, not a cause. *SAT accepts this; the brief claims enablement, not causation.*
- **Minab:** this may have been a conventional intelligence failure that would have happened without AI. *Plausible. But the stale record still survived a speed-optimised process with thin human review.*
- **May 2025:** the "kill chain" account comes largely from Pakistani officials, and the 94% figure from Indian officials; both have an interest in the narrative. *Treat both with caution until independently corroborated.*

6. HISTORICAL ANCHOR: IGLOO WHITE

The dream of an automated kill chain is older than machine learning. From 1967 to 1972, the US Operation Igloo White seeded the Ho Chi Minh Trail with acoustic and seismic sensors. Their signals were relayed by aircraft to an Infiltration Surveillance Center at Nakhon Phanom in Thailand, where International Business Machines (IBM) mainframes processed them and directed air strikes. The historian Paul Edwards describes it as the archetype of a "closed world" in which computers promised total battlefield visibility.^[23] The programme cost close to a billion dollars a year. Its reported truck kills were famously inflated, North Vietnamese forces learned to spoof the sensors with decoys and recorded noise, and traffic down the trail continued.^[23]

Dimension	Igloo White (1967–72)	AI-enabled targeting (2023–26)
Core promise	Sensors plus computers equals a transparent battlefield	Data fusion plus machine learning equals targets at machine speed
Human role	Analysts interpret sensor data; strikes cued by computer	Analysts approve machine nominations, sometimes in about 20 seconds
Builder	State-led, with defence contractors	Commercial cloud and AI firms are central (Nimbus, Maven)
Failure mode	Inflated metrics; sensors spoofed by the adversary	Stale data, false positives, automation bias; spoofing still possible
Lesson	Adversaries adapt to the sensor	Counter-AI (deception, data poisoning, electronic warfare) is the cheaper reply

Source: SAT comparison drawing on Edwards (1996), +972 Magazine (2024) and Arms Control Today (2026).

The parallel shows continuity and change. The continuity is the faith that more sensing and faster computing will dissolve the fog of war, and the adversary's ability to exploit that faith. What has changed is that today's systems *nominate* targets rather than merely relay signals, that private companies build and run much of the architecture, and that the tempo leaves far less room for doubt. For a state like Pakistan, Igloo White also points to an opportunity: deception, electronic warfare and data poisoning against an adversary's AI may be cheaper than matching that AI.

6.1 The grey zone mechanism

AI-enabled warfare is not itself grey-zone activity; Gaza and Iran are open wars. The grey-zone properties appear in how responsibility, infrastructure and norms are handled around it.

Mechanism	How it works	Evidence in this brief
Algorithmic deniability	Responsibility is split across vendor, database, analyst and commander, so each can point elsewhere	Minab: "AI-generated list" versus "human error in wartime" ^[4]

Mechanism	How it works	Evidence in this brief
Civil–military fusion via the cloud	Private firms become war infrastructure; terms of service become levers of policy	Project Nimbus; Microsoft's Azure cut-off to Israel's Ministry of Defence ^[19,21]
Population-scale surveillance	Ordinary communications data of whole societies feed lethal nomination	SKYNET (55 million phones); Unit 8200 call storage ^[14,21]
Normative positioning	States shape rules on autonomy while building the capability	UN General Assembly (UNGA) resolution 79/62: Pakistan voted yes, India abstained ^[24]
Escalation compression	Machine-speed tempo shortens the window for verification and political control	May 2025 India–Pakistan sensor war ^[7]

Source: SAT analysis. Bracketed numbers refer to endnotes.

7. PAKISTAN'S AI LANDSCAPE AND READINESS

Pakistan's AI ecosystem is gradually moving from policy ambition and academic research towards practical applications, including in defence. The Higher Education Commission set up the National Centre of Artificial Intelligence (NCAI) in 2018–19 through public development funding, giving university research an institutional base.^[25] On 30 July 2025, the federal cabinet approved the National AI Policy 2025. By 2030 it aims to train one million AI professionals, offer 3,000 scholarships a year, develop 1,000 local AI products and launch 50,000 AI-related projects, backed by an AI Innovation Fund and an AI Venture Fund intended to draw in private capital.^[9] Structural constraints remain: limited access to advanced computing, inadequate research funding, a shortage of specialised talent and little private-sector interest or investment in defence AI.

Publicly available information on AI adoption within Pakistan's armed forces is limited, which makes it difficult to judge the extent of operational integration. The available evidence suggests that the Pakistan Air Force is spearheading the effort. In August 2020 it announced the Centre of Artificial Intelligence and Computing (CENTAIC). The then Air Chief, Mujahid Anwar Khan, said it would help the PAF "incorporate artificial intelligence into its operational domain".^[10] CENTAIC was placed under the PAF's National Aerospace Science and Technology Park (NASTP) in July 2021. Its reported work includes computer vision for satellite imagery, natural language processing, high-performance computing for big data and reinforcement learning for autonomous aerial platforms, with a proposed joint AI laboratory with Türkiye.^[26] The data-fusion capability on display in May 2025 suggests that at least part of this work has reached operational use.^[7]

7.1 Readiness against the four dimensions

Dimension	Evidence	SAT assessment	Confidence
Technological absorption	CENTAIC, NASTP, NCAI; national AI funds; heavy reliance on imported Chinese and Turkish platforms; limited sovereign compute	Emerging	Moderate
Organisational adaptation	PAF-led; no public evidence of a tri-service AI command or joint data architecture	Uneven: PAF ahead, joint integration unclear	Low
Doctrinal integration	Multi-domain kill chain in May 2025, per Pakistani officials; no published military AI doctrine or rules on human control	Partial	Low to moderate
Institutional innovation	NASTP industry park; AI Policy funds; weak commercial pathway from prototype to procurement	Early	Moderate

Source: SAT assessment using Krepinevich (2023). Confidence reflects the quality of public evidence, not the state of the capability.

Measured against these criteria, Pakistan appears to be at an early and evolving stage of military AI integration, with considerable ground to cover before it can claim comprehensive readiness. CENTAIC

and NASTP are important institutional foundations, but they do not by themselves amount to preparedness. The decisive test is whether technical advances can be translated into doctrine, training, command-and-control arrangements, inter-service coordination and force-employment concepts.

7.2 Outside-in and inside-out

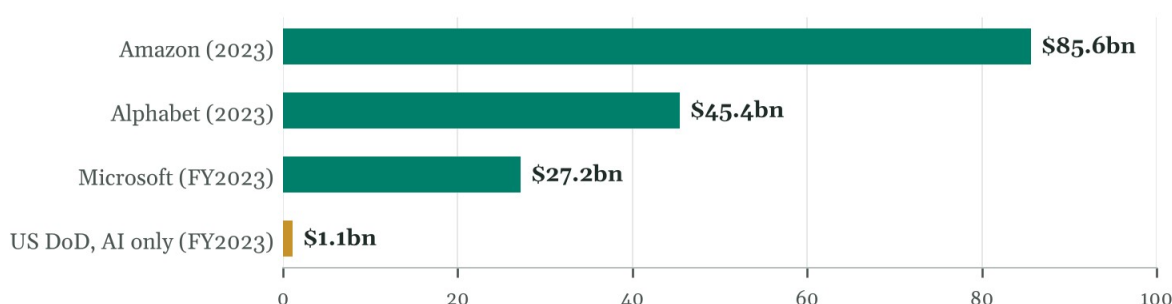
- **Outside-in:** India's public claims of AI-assisted targeting, and its access to Israeli and Western systems, create pressure for a reciprocal capability race. Pakistan's dependence on Chinese and Turkish platforms ties its AI trajectory to those partners' export and data policies.
- **Inside-out:** every Pakistani gain in sensor fusion also shortens Indian decision time. In a nuclear dyad, the stabilising measure, meaningful human control over consequential and nuclear-adjacent decisions, serves both sides.
- **Consistency:** Pakistan voted for the 2024 UN General Assembly resolution on lethal autonomous weapons while India abstained. ^[24] Pakistan's normative stance would carry more weight if it stated publicly how its own systems keep humans meaningfully in control. Opacity may aid deterrence, but it weakens credibility.

8. POLICY RECOMMENDATIONS FOR PAKISTAN

Pakistan cannot fund military AI through the state alone, and it does not need to. In fiscal year (FY) 2023, the US Department of Defense spent about US\$1.1 billion on AI. ^[27] In the same year Amazon, Alphabet and Microsoft reported total research and development budgets of US\$85.6 billion, US\$45.4 billion and US\$27.2 billion respectively, across all fields rather than AI alone. ^[28] The disparity makes the point: the frontier of this technology sits in private industry, and even the world's largest military draws on it. For a state with tight fiscal limits, the sensible course is to harness commercial expertise and capital rather than match the spending of major powers.

Where the Frontier Sits

Corporate research and development (R&D) budgets versus Pentagon AI spending, 2023 (US\$ billion)



Sources: company annual reports (Form 10-K), total R&D across all fields, not AI alone (Amazon reports 'technology and infrastructure'); Stars and Stripes, 5 March 2024, for DoD AI spending. Not like-for-like; shown to indicate order of magnitude.

- 1. Give industry a visible route to deployment.** Companies will not commit capital and scarce engineers to military AI if a working prototype has no clear route to trials, procurement and deployment. Transparent evaluation procedures, small pilot contracts and milestone-based, multi-year commitments would provide that assurance. Intellectual-property arrangements should leave firms a reason to innovate while guaranteeing the state the access and rights national security requires.
- 2. Build and keep the talent.** Joint programmes linking NCAI, university laboratories, CENTAIC and private firms could ease both the shortage of specialists and the weak commercialisation of academic research. Training alone will not keep graduates at home; competitive pay, credible career progression and modern research infrastructure will.
- 3. Be selective about what to build.** Reproducing the full AI stack of a major power is neither affordable nor necessary. Pakistan should aim for specialised, cost-effective capability in intelligence processing, autonomous surveillance, predictive maintenance, electronic-warfare support, sensor integration and counter-AI deception, with managed international partnerships where foundational research or computing costs are prohibitive.

4. **Learn from Minab: govern the data.** Audit and timestamp target and no-strike databases, require independent verification for sensitive site categories such as schools and hospitals, and set minimum human-review standards that cannot be compressed under operational pressure.
5. **Pursue crisis-stability measures with India.** A bilateral or multilateral commitment to human control over nuclear-adjacent decisions, and a channel for clarifying AI-related incidents, would serve Pakistan's interests as the conventionally weaker power.

The deeper lesson is that military AI capability is the product of an ecosystem, not of any single institution. Pakistan's task is to let the state set strategic priorities, industry supply technological dynamism, and universities sustain research and the talent pipeline. The goal is not to acquire AI for its own sake, but to build an adaptive innovation system that turns limited resources into lasting operational advantage.

9. ASSESSMENT: WHAT WE KNOW AND WHAT TO WATCH

9.1 What we know, and what we don't

Question	Evidence	Assessment	Confidence
Did AI accelerate US targeting in Iran?	White House strike totals; officials on Maven's role ^[4]	Yes, at unprecedented tempo	High
Was AI decisive in the Minab strike?	Central Command preliminary finding versus officials citing human error ^[4,3]	Stale data in a speed-optimised process; the precise AI role is disputed	Moderate
Did Lavender drive mass targeting in Gaza?	Multiple intelligence sources to +972; Israeli military denial ^[6]	Credible, detailed reporting; not officially confirmed	Moderate
Did Pakistan field a data-fused kill chain in May 2025?	Pakistani officials via Reuters; RUSI comment ^[7]	Likely, though detail comes from interested parties	Moderate
How far has AI spread beyond the PAF?	Little public information	Cannot determine	—
Does Pakistan have a military AI doctrine or human-control policy?	None published	Unknown	—

9.2 What to watch

Indicator	Why it matters	Horizon
Release of the full US investigation into Minab	Will show whether the failure lay in data, algorithm or process, and whether US rules on AI targeting change	Weeks to months
A Pakistani military AI doctrine or joint AI/data command	The clearest signal of organisational and doctrinal adaptation	Months
First defence-relevant contracts under the AI Innovation and Venture Funds	Tests whether the industry pathway is real	Months
Indian AI targeting or military large language model (LLM) deployments after Operation Sindoor	Sets the pace of any South Asian AI competition	Months
UN progress on a binding instrument on autonomous weapons, and Pakistan's position	Tests the consistency of Pakistan's normative stance	Months to years
Any India–Pakistan crisis featuring disputed AI-generated assessments	Would confirm the escalation-compression risk	Structural

10. CONCLUSION

The drones that once hovered over Waziristan were an early sign of a transformation that has since redrawn the character of war. AI now accelerates the kill chain, multiplies the reach of unmanned systems and rewards those who can fuse data faster than their adversaries. Yet the same speed that confers advantage also magnifies error and diffuses responsibility, as the strike on the school in Minab showed. Technology without verification, oversight and accountability is a liability.

For Pakistan, the evidence points to a country that has laid important foundations through NCAI, CENTAIC, NASTP and the National AI Policy 2025, and that showed in May 2025 what integration can achieve, but that has not yet built comprehensive readiness. Through Krepinevich's lens, the gap is not one of algorithms or hardware but of absorption, adaptation, doctrine and institutional innovation. Closing it requires an ecosystem in which the state sets priorities, industry supplies dynamism and universities sustain the talent pipeline, with human judgement kept firmly in command.

In the age of AI, victory will not go to the state with the most machines, but to the one with the institutions to use them wisely.

ENDNOTES

Sources are listed in order of first citation. Casualty figures from Gaza's Ministry of Health and from Iranian local officials are attributed as such.

1. Heba Habib, "United Nations says US may have committed war crimes in Iran: What it means," *Al Jazeera*, 18 September 2026, [aljazeera.com](https://www.aljazeera.com). Reports the findings of the UN Independent International Fact-Finding Mission on Iran; local officials reported 156 deaths.
2. Philip Wang and Richard Hall, "More Than 100 School Children Were Killed in Iran. Evidence Points to a U.S. Missile Strike," *TIME*, 11 March 2026, [time.com](https://www.time.com). TIME cites an Iranian teachers' union figure of some 175 dead.
3. Joseph N. Orenstein, "When Intelligence Fails: A Legal Targeting Analysis of the Minab School Strike," *Just Security*, 26 March 2026, [justsecurity.org](https://www.justsecurity.org).
4. Michael T. Klare, "AI Plays Major Role in the War on Iran," *Arms Control Today*, May 2026, [armscontrol.org](https://www.armscontrol.org). White House figures of 8 April 2026 cover the first 38 days of the war.
5. Christian Grothoff and J. M. Porup, "The NSA's SKYNET program may be killing thousands of innocent people," *Ars Technica*, 16 February 2016. The underlying Snowden documents were first published by The Intercept in 2015.
6. Yuval Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza," *+972 Magazine*, 3 April 2024, [972mag.com](https://www.972mag.com). Based on Israeli intelligence sources; the Israeli military disputes the characterisation.
7. Reuters, "How Pakistan shot down India's cutting-edge fighter using Chinese gear," *The Kathmandu Post*, 3 August 2025, [kathmandupost.com](https://www.kathmandupost.com). Draws on US, Pakistani and Indian officials.
8. Christine Casimiro, "AI Gives India 94% Precision Edge in Operation Sindoor: Report," *The Defense Post*, 7 October 2025, [thedefensepost.com](https://www.thedefensepost.com). The accuracy figure is an Indian Army claim.
9. "Cabinet approves national AI policy, targets 1m professionals by 2030," *The Express Tribune*, 30 July 2025, [tribune.com.pk](https://www.tribune.com.pk).
10. Bilal Khan, "Pakistan Air Force delves into artificial intelligence development," *Quwa*, 30 August 2020, [quwa.org](https://www.quwa.org).
11. Muhammad Azeem, "Thousands killed in drone strikes, terror attacks since 2004," *Dawn*, 9 November 2018, [dawn.com](https://www.dawn.com). Figures from Pakistan's National Counter Terrorism Authority (NACTA).
12. Andrew F. Krepinevich, *The Origins of Victory: How Disruptive Military Innovation Determines the Fates of Great Powers* (New Haven: Yale University Press, 2023), doi.org/10.12987/9780300271584.
13. Brandi Vincent, report on the Pentagon raising the Maven Smart System contract ceiling by \$795 million to nearly \$1.3 billion, *DefenseScoop*, 23 May 2025, [defensescoop.com](https://www.defensescoop.com).
14. Mike Murphy, "The potential flaw in the NSA's artificial intelligence system to identify terrorists in Pakistan," *Government Executive* (via Quartz), 17 February 2016, [govexec.com](https://www.govexec.com).
15. Harry Davies and Bethan McKernan, "Top Israeli spy chief exposes his true identity in online security lapse," *The Guardian*, 5 April 2024.
16. UN Office for the Coordination of Humanitarian Affairs, "Key figures on the 2014 hostilities," 23 June 2015, [ochaopt.org](https://www.ochaopt.org).

17. "Israeli army fire kills 5 more Palestinians in Gaza, death toll nears 74,400," *The Express Tribune*, 12 October 2026, tribune.com.pk. Figure from the Gaza Ministry of Health's daily report.
18. United Nations, "Israel has committed genocide in the Gaza Strip, UN Commission finds," 16 September 2025, un.org. Israel rejected the findings.
19. Yuval Abraham, "'No restrictions' and a secret 'wink': Inside Israel's deal with Google, Amazon," +972 Magazine, 29 October 2025, 972mag.com.
20. Associated Press, "Microsoft says it provided AI to Israeli military for war but denies use to harm people in Gaza," *Boston Globe*, 16 May 2025, bostonglobe.com.
21. Rebecca Szkutak, "Microsoft cuts cloud services to Israeli military unit over Palestinian surveillance," *TechCrunch*, 25 September 2025, techcrunch.com.
22. Amoha Basrur, "The use of drones marks a new phase in India–Pakistan hostilities," *Observer Research Foundation*, 13 May 2025, orfonline.org. Drone numbers are Indian government claims.
23. Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996).
24. UN General Assembly, Resolution A/RES/79/62, "Lethal autonomous weapons systems," adopted 2 December 2024 by 166 votes to 3, with 15 abstentions; recorded vote via un-project.org.
25. Higher Education Commission of Pakistan, "National Centres," established in FY2018–19 under the Public Sector Development Programme, hec.gov.pk.
26. "CENTAIC's Transformation Under PAF NASTP," *Second to None*, 10 May 2024, secondtonone.com.pk. A PAF-affiliated publication, treated here as an official-perspective source.
27. Briana Reilly, report on Pentagon AI spending (\$1.1 billion in FY2023; \$1.8 billion requested for FY2024), *Stars and Stripes* (CQ-Roll Call), 5 March 2024, stripes.com.
28. Amazon.com, Inc.; Alphabet Inc.; Microsoft Corporation, Annual Reports on Form 10-K for fiscal year 2023, filed with the US Securities and Exchange Commission. Figures are total R&D across all fields; Amazon reports "technology and infrastructure."



ABOUT SOUTH ASIA TIMES

South Asia Times (SAT) is an Islamabad-based platform for research, analysis and commentary on South Asia and its wider neighborhood. Its Research section publishes SAT Briefs, original policy research, and Backgrounders, explainers on the issues behind the headlines.

WRITE A SAT BRIEF

SAT commissions scholars, researchers and practitioners to author forthcoming briefs. Contributors are paid. Send a working title, a 300-word outline and a note on your expertise to [**submission@southasiatimes.org**](mailto:submission@southasiatimes.org).

ONLINE

southasiatimes.org · Research › SAT Briefs

© 2026 South Asia Times. The views expressed in SAT Briefs are those of their authors.