

Issue Brief

October 2026
No: 556

**Fewer Rungs, Faster Falls:
How Cross-Domain Warfare Is
Reshaping the India–Pakistan
Escalation Ladder**

Brig Arun Sahgal (Retd), PhD
Dr. Sudesh Vasudeva



Fewer Rungs, Faster Falls

How Cross-Domain Warfare Is Reshaping the India–Pakistan Escalation Ladder

Abstract

The four-day India–Pakistan conflict of May 2025 was the first on the subcontinent to be fought across air, land, sea, cyber, space, the electromagnetic spectrum and the information domain all at once, and the first in which drones were used in an offensive manner. This paper reconstructs the cross-domain dynamics of ‘Operation Sindoor’ from open records, separating what independent evidence supports from what either government has only claimed. It then examines the operational role of emerging and disruptive technologies (EDTs) in the conflict, the calibrated support Pakistan drew from China and other partners, and the likely character of the next confrontation. The central argument is that cross-domain operations and EDTs compress decision time while multiplying ambiguity, and that this combination erodes the signalling conventions on which South Asian crisis stability has rested thus far. An illustrative scenario traces how a non-kinetic incident could pass through automated sensors and dual-use command systems to strategic alert within five hours. The article closes with an assessment of nuclear risks arising from conventional–nuclear entanglement and changing alert postures, and with measures to restore time and clarity to crisis decision-making.

Keywords: Counter-UAS, Cross-Domain Deterrence, Emerging and Disruptive Technologies, Entanglement, Escalation, India–Pakistan, Nuclear Command and Control, Operation Sindoor, Strategic Signalling

I. Introduction: Four Days That Rewrote the Ladder

On the night of 06–07 May 2025, a fortnight after gunmen killed 26 people at the Baisaran meadow near Pahalgam, India struck nine sites in Pakistan and Pakistan-occupied Kashmir. Over the next eighty-odd hours, the two states exchanged cruise missiles, loitering munitions, short-range ballistic missiles and salvos of small drones, fought one of the largest beyond-visual-range air engagements of the missile age, and reached a ceasefire on the afternoon of 10 May (Clary, C. 2025). Clary’s reconstruction counts the episode as only the second use of airpower by one nuclear-armed state on the territory of another, and the third instance of serious, deadly hostilities directly between nuclear states (Clary, C. 2025). What sets it apart, however, was its intensity more than its breadth. Combat spilled all at once into seven domains—air, land, sea, cyber, space, the electromagnetic spectrum and the information space—more importantly the effects produced in one domain were often felt, within minutes, in the others.

That breadth matters because South Asian deterrence has long assumed time. Mobilisation in 2001–02 took weeks; the Balakot exchange of 2019 unfolded over two days with room for third-party diplomacy. In 2025, sensors in orbit, standoff weapons and drone salvos shortened the interval between decision and effect to minutes, while disinformation clouded what actually happened (Clary, C. 2025) (Ganguly, S. and Warren S.A. 2025). Two expert readings have since emerged. One holds that both sides calibrated force, and that thresholds were tested but not crossed (Ladwig, W. 2025). The other holds that India learned to strike military targets early, that the next crisis will therefore open on a higher rung, and that fewer rungs now separate conventional fighting from nuclear threshold (Ganguly, S. and Warren S.A. 2025). The two readings are less opposed than they look: the first describes what happened in 2025; the second describes what the 2025 teaches.

This article works between them. Section II reconstructs the cross-domain dynamics of Operation Sindoor and Section III isolates the role of EDTs. Section IV examines external support to Pakistan, and Section V the probable shape of future operations. Sections VI–VIII trace how signalling, accidents and technology interact to open escalation pathways, including towards the nuclear threshold. A note on evidence is necessary. Both governments made claims during and after the fighting that independent sources have not confirmed. Where this article relies on such claims it attributes them; where commercial imagery, foreign governments or peer-reviewed work supports a finding, it says so.

II. Anatomy of a Cross-Domain Crisis

Air Power and Precision Fires

The defining military fact of the conflict is what did not happen: there is no evidence that a manned aircraft of either side crossed into the other's airspace on any day (Clary, C. 2025). Each Air Force respected the other's integrated air defence system (IADS), and the war became a contest of standoff weapons fired across the border (Stimson, Center, 2026). India's opening strikes on 07 May used SCALP-EG cruise missiles, HAMMER glide bombs, precision artillery and drone-delivered munitions, with debris indicating BrahMos use from the first night (Clary, C. 2025). On the night of 9–10 May, the Indian Air Force struck at least eleven sites, among them Nur Khan near Rawalpindi, Rafiqui, Rahim Yar Khan, Sukkur, Sargodha, Bholari, Jacobabad and the drone and command facility at Murid, primarily with air-launched BrahMos fired from Su-30MKI aircraft (Clary, C. 2025) (Ganguly, S. and Warren S.A. 2025). Commercial imagery from Maxar and Planet Labs confirmed damage at Bholari, Nur Khan,

Rahim Yar Khan and Sargodha, and Pakistan's own notice declaring the Rahim Yar Khan runway non-operational is the cleanest cross-belligerent corroboration in the record (Chang, A., Robles, P. and Mashal, M, 2025). It was the first time India had fired cruise missiles at Pakistan, and the first time Pakistan had used conventionally armed short-range ballistic missiles—the Fatah-I and Fatah-II—against India (Clary, C. 2025).

The air battle of 07 May was the costliest episode for India. Published estimates of the aircraft airborne at standoff ranges run from about 114 to at least 125 (Peri, D. 2025), however, neither figure carries a stated basis.

Unmanned Systems, Land Fires and Counter-UAS

The conflict was the first in the India–Pakistan rivalry in which both sides employed drones with the intent of causing damage on the other (Clary, C. 2025). India used Israeli-origin Harop and Harpy loitering munitions against Pakistani air defence radars, with British-origin Banshee target drones probably serving as decoys; Pakistan's military spokesman himself named the Harop in his briefing of 08 May (Clary, C. 2025) (Al Jazeera, 2025). Pakistan launched mass salvos of small drones—Indian officials put one wave at 300–400 drones against 36 locations and another at over 600 across the Western Front—to saturate and map Indian defences, with Turkish-origin Yiha-III kamikaze drones appearing on the final night (Clary, C. 2025). India's layered response joined the Akashteer air defence control and reporting network, itself linked to the Air Force's Integrated Air Command and Control System (IACCS), with surface-to-air missiles and, to considerable effect, legacy L-70 and ZU-23 guns (Peri, D. 2025). Independent assessments agree that Indian air and missile defence largely defeated the Pakistani drone waves (Clary, C. 2025) (Ganguly, S. and Warren S.A. 2025), although the absence of any published launch figure makes the interception rates claimed by either side impossible to check. On the ground, artillery and small-arms fire across the Line of Control (LoC) killed more than fifty people, plausibly most of all deaths (Clary, C. 2025) —a reminder that the oldest domain remained the deadliest.

Cyber Operations and the Information Domain

Cyber activity accompanied the campaign but produced limited physical effect. The documented record shows denial-of-service attacks, defacements and intrusion attempts against government, financial and utility networks, alongside a far more consequential contest in the information space (Pytlak, A. 2025). Clary describes “unprecedented levels of mis- and

disinformation” that continues to cloud understanding of what happened (Clary, C. 2025). The most damaging falsehood was strategic rather than tactical. Pakistan’s military spokesmen denied conducting drone and missile attacks on India until the final night, so India’s retaliatory strikes of 08 May reached Pakistani audiences as unprovoked aggression rather than as a response (Clary, C. 2025). Information operations thus shaped perceptions of proportionality—the very currency of escalation control.

Space, Electronic Warfare and ISR

Satellite imagery, airborne early warning and signals intelligence fed target tracks to strike packages on both sides, and electronic warfare (EW) was built into those packages to suppress radars and sever drone datalinks. Equally significant was the transparency created by commercial imagery and open-source analysis, which limited either side’s ability to hide deployments or inflate results (Chang, A., Robles, P. and Mashal, M, 2025). India, criticised in 2019 for overstating damage at Balakot, released imagery of nine of the eleven sites it claimed to have struck on 10 May (Clary, C. 2025). Battlefield transparency, once a by-product of superpower reconnaissance, has become a public good that constrains what governments can credibly assert.

Signalling and Rapid Termination

Both governments framed their strikes as measured. India described its first strikes as “focused, measured and non-escalatory”, aimed only at terrorist infrastructure (Clary, C. 2025). Overt nuclear signalling was lower than in earlier crises (Clary, C. 2025) (Peri, D. 2025); the only explicit gesture—a report on the morning of 10 May that Pakistan’s National Command Authority had been convened—was withdrawn by the Defence Minister within three hours (Clary, C. 2025). The ceasefire, reached over the military hotline amid alleged intense American telephone diplomacy, came before cross-domain pressure could yield a decisive result. The lesson visible in both capitals was that, multi-domain operations compress a crisis into hours and leave little room to correct a misreading. **Table 1** summarises the domain-by-domain picture.

Table 1: Cross-Domain Dynamics in Operation Sindoor (May 2025)

Domain	Capabilities Employed	Evidence Status	Strategic Effect
Air / Precision Fires	BrahMos, SCALP-EG, HAMMER; strikes on at least 11 air bases; BVR air battle	Damage at four bases confirmed by commercial imagery; aircraft-loss figures disputed	Deep-strike option established without territorial incursion
Unmanned Systems / C-UAS	Harop, Harpy, decoys; Pakistani mass drone salvos, Yiha-III; Akashteer, L-70, ZU-23	Drone types confirmed by debris; launch and interception counts unverified	Saturation tactics tested; legacy guns proved cost-effective
Land	Artillery, mortars and small arms across the LoC	More than 50 deaths near the LoC	Largest single category of fatalities
Cyber / Information	Denial-of-service, defacement, intrusion attempts; disinformation	Physical effects limited	Shaped perceptions of proportionality
Space / EW / ISR	Satellite tracking, airborne early warning, radar and datalink jamming	Inferred from strike outcomes; transparency via commercial imagery	Compressed sensor-to-shooter cycles
Nuclear Signalling	Reported NCA meeting, withdrawn within three hours	Documented	Lower overt signalling than in earlier crises

Source: Compiled by the Author(s) from Various Sources

III. Emerging and Disruptive Technologies Under Fire

Operation Sindoor moved EDTs from doctrine into use. Four clusters stand out. The **first** is unmanned systems employed at scale: cheap drones generated mass, overwhelmed or mapped air defences and suppressed radars at low cost and low risk to operators (Ganguly, S. and Warren S.A. 2025). The **second** is standoff precision. Supersonic cruise missiles and long-range air-to-air missiles—Meteor on the Indian side and the Chinese PL-15 on the Pakistani, the latter confirmed by debris recovered in India (Clary, C. 2025)—let both sides fight across the border at ranges beyond 100 km. The **third** is space-enabled ISR and multi-sensor fusion, which shortened the loop from detection to strike and gave Pakistan, through Chinese support, a degree of awareness its own sensors could not provide (Section IV). The **fourth** is the electromagnetic

spectrum, which emerged as a domain of first resort, with jamming integrated into offensive packages and air defence alike.

Two qualifications temper the enthusiasm that followed. The first is cost. The Stimson panel on South Asian air defence identified the asymmetry between cheap offensive drones and expensive interceptors as a lesson shared by both sides (Stimson, Center, 2026), and Indian success against small drones owed much to guns designed in the 1960s and 1970s (Peri, D. 2025). The second is that EDTs generated information faster than either side's institutions could verify it. Speed favoured the attacker in targeting, but it also favoured rumour—from an alleged strike on Kirana Hills to claims of a destroyed S-400—none of it supported by imagery (Clary, C. 2025). A technology that shortens the kill chain also shortens the time available to establish what the kill chain has done.

IV. The Collusive Front: External Support to Pakistan

Clary observes that 2025 was the first India–Pakistan conflict involving a military equipped with modern Chinese weapons—the J-10C fighter, the PL-15 missile and the HQ-9 air defence system (Clary, C. 2025). India's Deputy Chief of Army Staff, Lt Gen Rahul R. Singh, went further, stating that roughly 81 per cent of Pakistan's military hardware is of Chinese origin, that China supplied live inputs on Indian deployments during the fighting, and that Turkish drones and trained personnel were also involved (PTI, 2025). These are Indian official statements and have not been corroborated in detail by independent sources, but they describe a pattern consistent with the documented equipment picture.

In a future conflict, Beijing is unlikely to fight India on the Western Front. Its support is better understood as a calibrated, asymmetric force multiplier operating along five lines. In ISR and targeting, access to Chinese reconnaissance imagery and BeiDou positioning would support Pakistani long-range strikes and battle damage assessment (BDA), now supplemented by Pakistan's own electro-optical satellites EO-2 and EO-3, launched from China in February and April 2026 and offering persistent coverage of Jammu and Kashmir and adjoining areas (The News International, 2026) (MoFA, Pakistan, 2026). In technical sustainment, manufacturer teams could support software integration, radar tuning and electronic countermeasures on J-10C, JF-17 Block III, HQ-9 and naval platforms. In cyber and EW, Beijing could mount parallel intrusions against Indian logistics, power and telecommunications and supply jamming and signals-intelligence equipment. In resupply, China can replenish munitions, drones and air-to-air missiles, with China–Pakistan Economic Corridor (CPEC) infrastructure and the port of

Gwadar offering dual-use depth. Finally, through two-front pinning, elevated readiness along the Line of Actual Control (LAC) would hold Indian strike formations and air defence units in the north.

The external picture is not confined to China. Türkiye has supplied drones, and the Strategic Mutual Defence Agreement signed by Saudi Arabia and Pakistan in Riyadh on 17 September 2025, under which aggression against either is treated as aggression against both (Al Jazeera, 2025), opens the possibility of Gulf financial and material backing in a crisis. Indian planning must therefore account for a Pakistan whose staying power in a short, intense war is greater than its economy alone would suggest (**Table 2**).

Table 2: External Support to Pakistan: Mechanisms and Effects

Domain of Support	Primary Mechanism	Evidence Basis	Effect on the India–Pakistan Dynamic
ISR and Targeting	Chinese satellite imagery, BeiDou PNT; Pakistani EO-series satellites	Live inputs alleged by Indian Army; EO-2/EO-3 launched 2026	Precision long-range targeting and rapid BDA
Technical Sustainment	Manufacturer support for J-10C, JF-17, HQ-9 and naval platforms	Assessed	High readiness of Chinese-origin systems
Cyber and EW	Parallel intrusions; jamming and SIGINT equipment	Assessed	Strain on Indian C2 and critical infrastructure
Logistics and Resupply	Munitions, drones, PL-15-class missiles; CPEC and Gwadar	Assessed	Prevents early exhaustion of precision munitions
Northern Posture	Elevated readiness along the LAC	Assessed	Two-front fixation of Indian reserves
Gulf and Türkiye	Saudi–Pakistan defence pact; Turkish drones	Pact documented; drone use confirmed by debris	Financial and material depth

“Assessed” denotes the author(s)’ analytical judgement rather than a documented event

Source: Compiled by the Author(s) from Various Sources

V. The Next Contest: Cross-Domain Operations in Future Crises

The next confrontation is unlikely to resemble a border skirmish or a single-domain air exchange. It will more probably be marked by high-velocity operations across several domains, compressed decision cycles and an increasingly fused China–Pakistan military relationship. Four features can be anticipated.

- ***Grey Zone to Kinetic Saturation.*** Cyber intrusion, jamming and cognitive campaigns will begin days before the first missile is fired, with the aim of blinding sensors and slowing decisions. Once kinetic operations begin, loitering munitions, drone swarms and standoff missiles will be launched together across air, land and sea to saturate air defences, raising both intensity and lethality. Ganguly and Warren expect India to suppress Pakistani air defences at the outset (Ganguly, S. and Warren S.A. 2025); Pakistan can be expected to anticipate this and to strike first at Indian sensors.
- ***Sensor-to-Shooter Integration.*** Space-based ISR combined with AI-assisted target recognition will shrink the interval between detection and destruction to minutes. Strike aircraft, warships, rockets/missiles (S/MRBM) and artillery will increasingly fire on shared tracks generated by remote space and electromagnetic sensors rather than by their own radars.
- ***The Maritime Turn.*** The Arabian Sea is the most likely an arena of horizontal escalation. Submarine-launched cruise missiles, autonomous underwater vehicles and anti-ship missile salvos could be used to contest sea lines of communication and enforce anti-access zones. A maritime dimension would also lengthen the conflict from hours to days or weeks, because naval campaigns do not end with a call on the hotline.
- ***A Blurred Escalation Ladder.*** A cyberattack on a power grid or a military command network can produce disruption on a kinetic scale. As the line between non-kinetic aggression and conventional war fades, so the risk grows that a digital trigger will draw a heavy kinetic response (Pytlak, A. 2025).

Table 3 summarises how the technologies seen in 2025 are likely to evolve. Algorithm-paced warfare will push commanders towards reliance on automated recommendations; generative AI will manufacture deepfakes during the crisis itself; mesh-networked swarms will resist single-node jamming; and directed-energy weapons (DEWs) will begin to answer the cost

problem. India’s trial of a 30 kW laser system that disabled a fixed-wing drone and a drone swarm in April 2025 marks the start of that transition (DRDO, 2025). Quantum sensing, if it matures, would make the concealment of submarines and mobile launchers harder—a development with direct nuclear implications (Section VIII).

Table 3: EDT Evolution Matrix: From Operation Sindoor to Future Crises

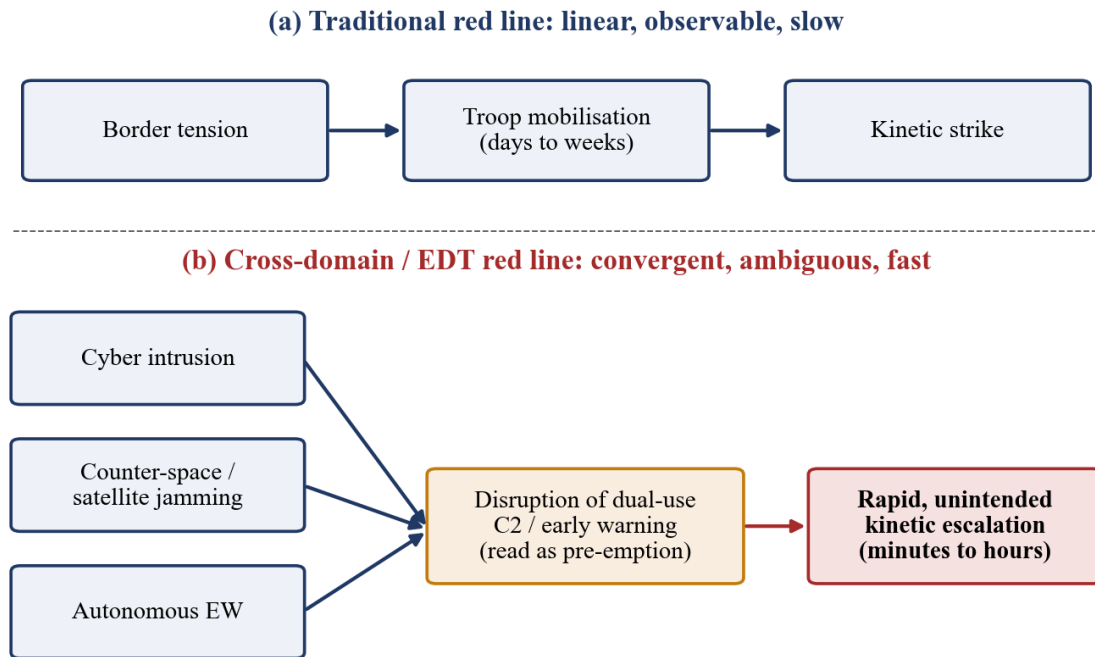
Technology Area	Role in Operation Sindoor (2025)	Trajectory in Future Crises
Unmanned Systems	Human-piloted loitering munitions, tactical UAVs, mass decoy salvos	Autonomous, mesh-networked swarms; unmanned ground and underwater vehicles
Air and Missile Defence	Layered SAMs, guns with modern ammunition, IACCS/Akashteer	Directed-energy weapons (laser, high-power microwave); AI-predictive interception
Space and ISR	Satellite tracking, commercial imagery, OSINT verification	Low-Earth-orbit constellations, persistent SAR, quantum sensing
Cyber and EW	Denial-of-service, datalink and GPS jamming, limited infrastructure targeting	AI-enabled intrusion, autonomous EW, attacks on dual-use C2 networks
Command and Decision	Human decisions under compressed timelines	AI decision support, with attendant risk of automation bias
Information	Disinformation and contested narratives	Real-time generative deepfakes aimed at leaders and publics

Source: Author’ Assessment

VI. Signals Lost in Translation: Red Lines in An Age of Ambiguity

Traditional signalling in South Asia relied on observable kinetic change: armoured formations moving towards the border, missile units dispersing, leave cancelled etc. Such signals were slow, legible and reversible. Cross-domain operations replace them with signals that are fast, ambiguous and often invisible to the publics whose pressure shapes leaders’ choices (**Figure 1**).

Figure 1: Traditional Linear Escalation Contrasted with Cross-Domain Convergent Escalation



Source: Author(s)

Three mechanisms drive the ambiguity. The first is the compression of reaction windows. When standoff weapons and AI-assisted sensor-to-shooter loops cut decision time to minutes, defensive moves—switching on jammers, manoeuvring satellites, dispersing air defence units—can be read as preparation for a disarming first strike (Jervis, R. 1976). The second is dual-use ambiguity. Command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) networks serve conventional and strategic forces alike. An attack on an air defence radar meant to open a corridor for a conventional strike may be read as an attack on nuclear early warning (Ganguly, S. and Warren S.A. 2025) (Acton, J.M. 2018). The Stimson panel noted the defensive corollary: adversaries can misinterpret defensive actions as offensive (Stimson, Center, 2026).

The third mechanism is the asymmetric interpretation of thresholds. Pakistan's doctrine of full-spectrum deterrence relies on nuclear weapons, including short-range systems, to offset conventional inferiority (Kidwai, K. 2015). India regards limited cross-domain actions—cyber operations, counter-drone strikes, strikes on terrorist infrastructure—as calibrated options below the conventional threshold, and Ladwig notes that cross-border force has moved in Indian

thinking “from exception to expectation” (Ladwig, W. 2025). Each side’s sub-threshold option therefore sits close to the other’s red line. In this structure, misreading is not an occasional failure; it is the default.

VII. Pathways to Inadvertent Escalation

Interactions between non-kinetic EDTs and conventional platforms create escalation routes that neither side intends (Posen, B.R. 1991). Two archetypes illustrate the mechanism. In the first, an offensive cyber or high-power microwave attack disables an early-warning radar network. Unsure whether the blackout is a temporary exploit or a prelude to an air campaign, the blinded state launches missiles against suspected launch sites, turning a non-kinetic disruption into a kinetic exchange. In the second, a surveillance swarm suffers spoofing or an algorithmic fault, strays from its sector and strikes an ammunition depot near a nuclear-capable air base; the victim reads a malfunction as a deliberate strike on its deterrent.

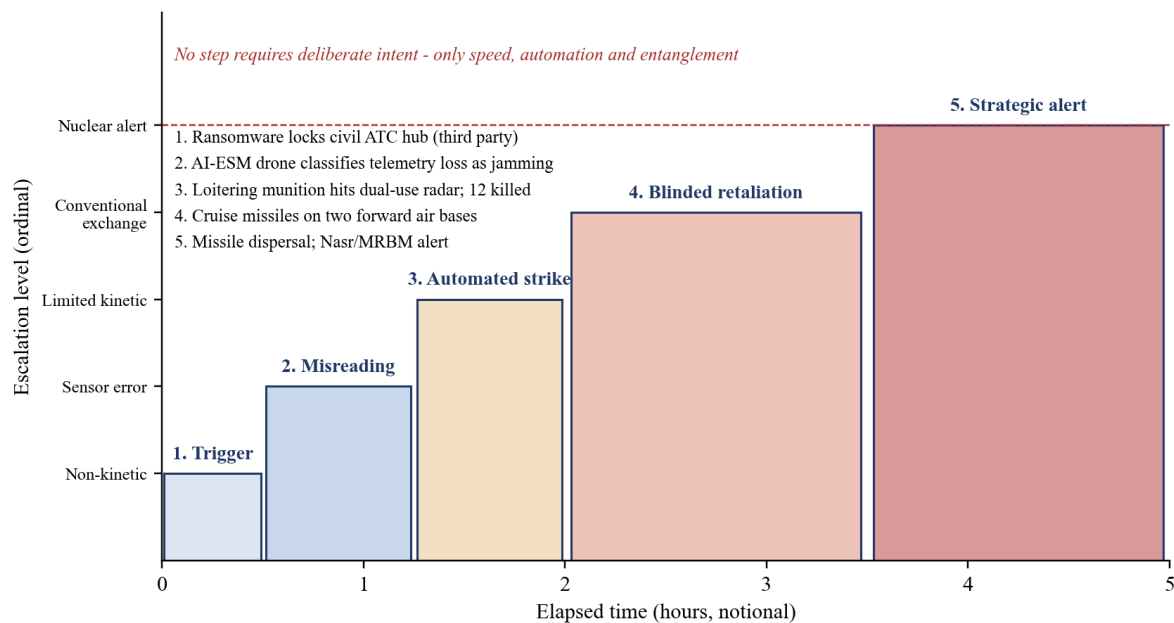
The scenario that follows, named “Dark Horizon”, combines these mechanisms. It is illustrative rather than predictive, and its timings are notional (**Figure 2**).

- **Phase 1, the trigger (00:00–00:30 h).** During a period of tension after a major terrorist attack, a criminal syndicate launches an automated ransomware attack on a civil air traffic control hub in northern Pakistan. At the same time, an Indian AI-enabled electronic support measures (ESM) drone is monitoring Pakistani radar activity along the LoC.
- **Phase 2, the misreading (00:30–01:15 h).** The drone’s onboard classifier, trained largely on pre-strike signatures, interprets the sudden loss of civil telemetry as deliberate high-power jamming intended to mask an incoming strike. Under rules of engagement written for compressed reaction windows, an accompanying loitering munition is released against the presumed source.
- **Phase 3, the cross-domain strike (01:15–02:00 h).** The munition hits a forward air defence radar, killing twelve personnel and blinding a node of Pakistan’s IADS that also feeds early warning to strategic command. Islamabad reads the event not as an isolated error but as the first phase of a counterforce strike.
- **Phase 4, blinded retaliation (02:00–03:30 h).** With radar coverage degraded and fearing that Indian cruise missiles are already inbound, Pakistani commanders

invoke pre-delegated authority and launch standoff cruise missiles at two Indian forward air bases. One of which houses dual-capable aircraft. Indian early-warning systems assess that nuclear-related infrastructure is under attack.

- **Phase 5, the strategic threshold (03:30–05:00 h).** India disperses land-mobile ballistic missiles from garrison and raises the readiness of its sea-based deterrent. Chinese reconnaissance satellites detect the dispersal and pass tracking data to Islamabad, which raises the readiness of its short-range Nasr systems and orders medium-range missiles to deploy. Both sides now face use-it-or-lose-it pressure.

Figure 2: The “Dark Horizon” Scenario: Escalation from a Third-Party Cyber Incident to Strategic Alert in Five Notional Hours



Source: Author(s)

Three lessons follow. Algorithmic cascades allow a glitch in a civilian network to be misread by an automated sensor in another domain and answered with force. Compressed loops deny operators the time to verify context, use the hotline or confirm damage. attacks on dual-use command assets oblige the adversary to assume the worst. None of these steps requires malice; each requires only speed, automation and entanglement—features that both militaries are now acquiring.

VIII. The Nuclear Shadow: Entanglement, Alert Postures and Second-Strike Confidence

South Asia’s geography and doctrines make the nuclear consequences of cross-domain warfare unusually acute. Missile flight times between the two countries are measured in

minutes. India's doctrine of no first use backed by massive retaliation (MEA, 2003) faces Pakistan's full-spectrum deterrence (Kidwai, K. 2015). Both arsenals are growing: SIPRI estimated 190 Indian and 170 Pakistani warheads in June 2026, and noted that India's canisterised missiles may allow warheads to be carried mated in peacetime (SIPRI, 2026). SIPRI's South Asian contributors warned in 2020 that machine learning and autonomy could become the focus of an arms race among the region's nuclear-armed states (Topychkanov, 2020). The events of 2025 bring that warning closer. Four effects can be distinguished.

Strain on Nuclear Command, Control and Communications

Cyber intrusions paired with high-power EW can target space-based and terrestrial links between national command authorities and nuclear forces. A partial blackout during a conventional crisis may be read as an attempt at decapitation and induce panic. AI-assisted decision support, adopted to cope with hypersonic or swarm threats, compresses deliberation from minutes to seconds and introduces failure modes—data poisoning, algorithmic bias, false positives—that humans may not detect in time (Topychkanov, 2020).

Changes in Alert Posture

South Asian deterrence has historically rested on de-mated warheads stored apart from their delivery systems—an arrangement that built in hours of delay. Canisterised missiles such as the Agni-P improve survivability remove that buffer (SIPRI, 2026). If drones or cyberattacks threaten storage sites, early-warning radars or the perimeters of strategic bases, leaders may feel compelled to mate warheads early in a conventional crisis to avoid decapitation.

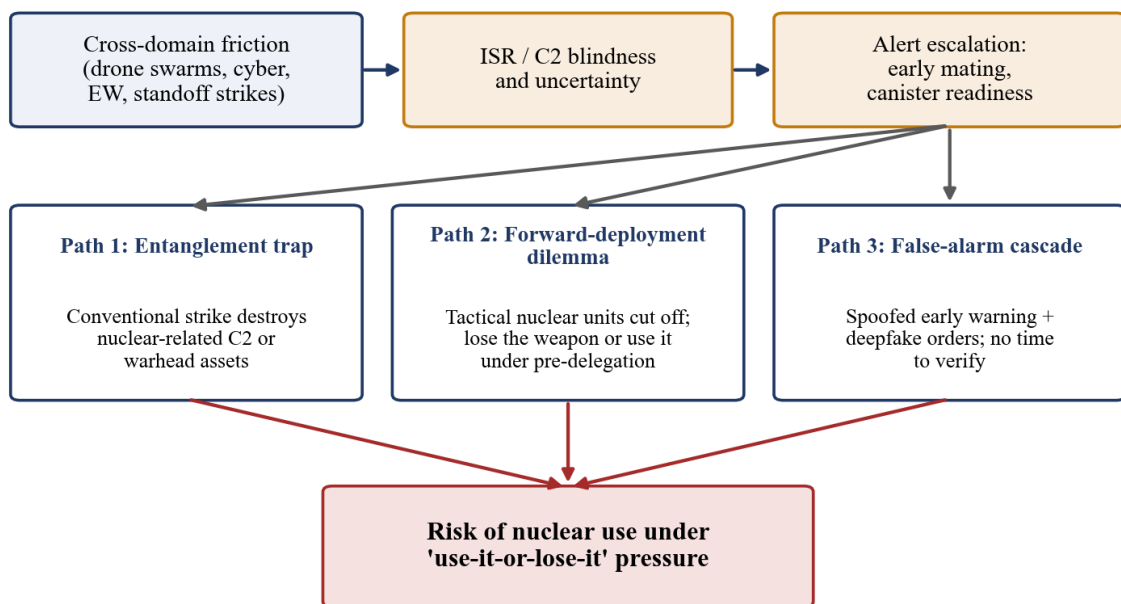
Vulnerability of Fixed and Mobile Assets

Persistent synthetic aperture radar constellations, AI-driven image analysis and drone surveillance make silos, storage sites and launcher columns easier to track. Clary and Narang have shown how improving Indian sensing and precision could create counterforce temptations (Clary, C. and Narang, V. 2019); the same tools, available to Pakistan through Chinese support, work in the other direction. Quantum magnetometry and gravimetry, should they mature, would threaten the concealment on which sea-based second-strike rests. Fear for the survival of second-strike forces is the classic driver of pre-emption (Talmadge, C. 2017).

Pathways to Nuclear Use

Three pathways stand out (**Figure 3 and Table 4**). In the entanglement trap, an attack on an air base or missile facility, believed to be purely conventional, destroys nuclear-related command or warhead assets, and the victim concludes that a disarming strike is under way (Acton, J.M. 2018) (Talmadge, C. 2017). In the forward-deployment dilemma, tactical nuclear units such as Nasr batteries, cut off from central command by loitering munitions or special forces, must choose between losing the weapon to destruction or seizure and firing it under pre-delegated authority. In the false-alarm cascade, cyber interference with early-warning radars, combined with deepfake audio or video of senior commanders, produces indications of an incoming strike that compressed timelines leave no time to verify.

Figure 3: Pathways from Cross-Domain Friction to the Risk of Nuclear Use



Source: Author(s)

Table 4: Nuclear Risk Drivers and Mitigating Measures

Risk Driver	Mechanism	South Asian Aggravator	Possible Mitigation
Entanglement	Dual-use radars, C2 and air bases hit in conventional strikes	Shared conventional and nuclear infrastructure; short flight times	Identify and avoid strategic nodes in targeting; restraint toward early-warning assets
Disarming Fear	ISR, precision and quantum sensing threaten second-strike forces	Small arsenals; mobile launchers in compact terrain	Survivable basing; mutual no-attack understandings on nuclear facilities
Alert-Posture Change	Canisterisation and early mating remove time buffers	Canisterised Agni-P; forward tactical systems	Peacetime de-mating norms; notification of alert changes
Automation	AI decision support and autonomous ESM/strike systems	Compressed timelines; models trained on limited data	Human authority over kinetic release; joint statement on AI in nuclear command
Information Manipulation	Deepfakes; spoofed early-warning data	High public pressure; low trust	Authenticated hotlines and verified crisis communication

Source: Author(s)Assessment

The convergent point is that none of these pathways depends on either leadership wanting nuclear war. India’s caution is deep-rooted, and Ganguly and Warren judge India unlikely to be the first state to break the nuclear taboo (Ganguly, S. and Warren S.A. 2025) . Pakistan’s doctrine, however, explicitly contemplates nuclear use to halt threatening conventional operations (Ganguly, S. and Warren S.A. 2025) (Kidwai, K. 2015). Entanglement means that what one side intends as a conventional move can register on the other side’s instruments as a strategic one (Acton, J.M. 2018) (Sahgal, A. and Vasudeva, S. 2026). This is exacerbated by recent changes in Pakistani nuclear command control, where authority has decidedly shifted from Civilian to Military control, more specifically the Army Chief.

IX. Conclusions and Policy Implications

Operation Sindoor showed that two nuclear-armed states can fight a short, intense, multi-domain conflict and stop. It did not show that they can do so again. The capabilities that kept 2025 limited—standoff weapons, drones, space-enabled ISR, control of the information narrative—are the same capabilities that will compress the next crisis, raise its starting point and multiply the opportunities for misreading, resulting in inadvertent or unintended escalation. Cross-domain warfare does not merely add domains; it couples them, so that an event in cyberspace or the spectrum can produce a consequence on the runway, in the missile garrison and, at worst, in the nuclear command chain.

Five measures follow for Indian policy makers; most would serve both states. First, protect decision time: keep human authority over kinetic release by autonomous systems, and test rules of engagement against false positives as rigorously as against threats. Second, map and reduce entanglement by identifying which radars, command nodes and bases perform strategic functions, and by avoiding targeting plans that strike them early. Third, broaden crisis channels beyond the DGMO hotline and the NSA link (Ladwig, W.C. 2025), and add authenticated communication to counter deepfakes. Fourth, invest in cost-effective defences—directed energy, guns and EW—so that drone saturation cannot force escalation by attrition. Fifth, plan for a collusive front: treat Chinese ISR, sustainment and northern pinning, Gulf financial depth and Turkish technology as baseline conditions rather than contingencies (PTI, 2025) (Al Jazeera, 2025). The aim is not to make conflict impossible, which lies beyond any doctrine, but to ensure that the next crisis can still be halted by people who understand both what is happening and its consequences.

Works Cited

- Acton, J.M. (2018). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war. *International Security*, vol. 43, no. 1. <https://www.belfercenter.org/publication/escalation-through-entanglement-how-vulnerability-command-and-control-systems-raises>.
- Air defense in South Asia (2026, March 20). *Stimson Center*. <https://www.stimson.org/2026/air-defense-in-south-asia/>.

- Armaments, Disarmament and International Security (2026). *SIPRI Yearbook 2026*.
https://www.sipri.org/sites/default/files/2026-06/yb26_summary_en_0.pdf.
- Cabinet Committee on Security reviews progress in operationalizing India's nuclear doctrine (2003, January 4). *MEA*. https://www.mea.gov.in/press-releases?dtl/20131/The_Cabinet_Committee_on_Security_Reviews_perationalization_of_Indias_Nuclear_Doctrine+Report+of+National+Security+Advisory+Board+on+Indian+Nuclear+Doctr ine.
- Chang, A., Robles, P. and Mashal, M. (2025, May 14). India and Pakistan talked big, but satellite imagery shows limited damage. *The New York Times*. <https://www.nytimes.com/interactive/2025/05/14/world/asia/india-pakistan-attack-damage-satellite-images.html>.
- Clary, C. and Narang, V. (2019). India's counterforce temptations: Strategic dilemmas, doctrine, and capabilities. *International Security*, vol. 43, no. 3.
<https://www.belfercenter.org/publication/indias-counterforce-temptations-strategic-dilemmas-doctrine-and-capabilities>.
- Clary, C. (2025, May 28). Four days in May: The India–Pakistan crisis of 2025. *Stimson Center Working Paper*. <https://www.stimson.org/2025/four-days-in-may-the-india-pakistan-crisis-of-2025/>.
- DRDO conducts successful field demonstration of Mk-II(A) laser-directed energy weapon system (2025).
DRDO. https://www.drdo.gov.in/drdo/sites/default/files/drdo_news/NPC12to15Apr2025.pdf.
- Have India and Pakistan started a drone war? (2025, May 8). *Al Jazeera*.
<https://www.aljazeera.com/news/2025/5/8/have-india-and-pakistan-started-a-drone-war>.
- Ganguly, S. and Warren, S.A. (2025). Escalation risks rising? Airpower in Kargil and Pahalgam. *The Washington Quarterly*, vol. 48, no. 3. doi: 10.1080/0163660X.2025.2558282.
- Jervis, R. (1976). *Perception and Misperception in International Politics*. Princeton, NJ, USA: Princeton Univ. Press.
- Kidwai, K. (2015, March 23). A conversation with Gen. Khalid Kidwai. *Carnegie International Nuclear Policy Conference*. <https://carnegieendowment.org/files/03-230315carnegieKIDWAI.pdf>.
- Ladwig, W.C. (2025, May 21). Calibrated force: Operation Sindoor and the future of Indian deterrence. *RUSI Commentary*. <https://www.rusi.org/explore-our-research/publications/commentary/calibrated-force-operation-sindoor-and-future-indian-deterrence>.

- Pakistan's second homegrown EO-2 satellite launched from China (2026, February 12). . *The News International*. <https://www.thenews.pk/story/1398730-pakistan-s-second-homegrown-eo-2-satellite-launched-from-china>.
- Pakistan launches indigenous EO-3 satellite marking major space milestone (2026). *MoFA, Pakistan Press Release*. <https://mofa.gov.pk/press-releases/pakistan-launches-indigenous-eo-3-satellite-marking-major-space-milestone>.
- Peri, D. (2025, October 6). Military lessons from Operation Sindoor. *Carnegie India*. <https://carnegieendowment.org/india/research/2025/10/military-lessons-from-operation-sindoor>.
- Posen, B.R. (1991). *Inadvertent Escalation: Conventional War and Nuclear Risks*. Ithaca, NY, USA: Cornell Univ. Press, 1991.
- PTI (2025, July 4). China used India-Pak conflict as 'live lab', used strategy of killing by 'borrowed knife'. *The Week*. <https://www.theweek.in/wire-updates/national/2025/07/04/del46-def-army-ld-sindoor-china.html>.
- Pytlak, A. (2025). Cyber quicksand? Uncharted risks and escalatory dynamics in a future India–Pakistan crisis. *Stimson Center*. <https://www.stimson.org/2025/cyber-risks-and-escalatory-dynamics-future-india-pakistan-crisis/>.
- Sahgal, A. and Vasudeva, S. (2026). Escalation by accident: Structural drivers of the next India–Pakistan conflict in a post-ceasefire strategic order. *Strategic Assessment—An Indian Perspective*.
- Talmadge, C. (2017). Would China go nuclear? Assessing the risk of Chinese nuclear escalation in a conventional war with the United States. *International Security*, vol. 41, no. 4. <https://www.belfercenter.org/publication/would-china-go-nuclear-assessing-risk-chinese-nuclear-escalation-conventional-war>.
- Topychkanov, P. (Ed.) {2020}. The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. *SIPRI*. https://www.sipri.org/sites/default/files/2020-04/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov_1.pdf.
- 'Watershed': How Saudi–Pakistan defence pact reshapes region's geopolitics (2025, September 18). *Al Jazeera*. <https://www.aljazeera.com/news/2025/9/18/watershed-how-saudi-pakistan-defence-pact-reshapes-regions-geopolitics>.

About the Author

Brigadier Arun Sahgal (Retd), PhD is the Executive Director of the Forum for Strategic Initiative, a policy think tank focusing on national security, diplomacy and Track II Dialogues.

Dr. S K Vasudeva is PSA fellow at the office of Principal Scientific Adviser to Govt. of India.



All Rights Reserved 2026, Centre for Land Warfare Studies (CLAWS)

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from CLAWS. The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.