ShodhSamajik: Journal of Social Studies
January-June 2026 3(1)
https://shodhsamajik.com/

Original Article

ENTANGLED DETERRENCE: DUAL-USE TECHNOLOGIES AND STRATEGIC STABILITY IN SOUTHERN ASIA

Shubham Rai [1*]
[1] PhD Scholar, Nelson Mandela Centre for Peace and Conflict, Resolution, Jamia Millia Islamia, Delhi, India

ABSTRACT

This paper develops a hybridised theoretical framework, termed "Entangled Deterrence," to examine how dual-use emerging technologies are systematically undermining strategic stability across the Southern Asian security complex. Focusing on India's evolving posture within a tripolar nuclear environment involving China and Pakistan, the paper argues that artificial intelligence-enabled command and control, offensive cyber capabilities, and dual-use space-based sensing infrastructures interact to produce two structurally destabilising effects: decision compression, wherein the time available for deliberate crisis management shrinks to algorithmically determined windows; and C3I entanglement, wherein conventional and nuclear command architectures become indistinguishable to an adversary.

Drawing on official doctrinal documents, secondary strategic literature, and a structured case study of the 2019 Balakot Crisis, the paper contends that dual-use technologies do not merely modify existing arms races but qualitatively transform their character, converting India's pursuit of credible minimum deterrence from a condition of managed vulnerability into a volatile, multi-domain instability spiral. The paper concludes with targeted confidence-building measure (CBM) proposals calibrated to the technological realities of the Indo-Pacific security environment.

Keywords: Dual-Use Technologies, Deterrence Stability, Decision Compression, C3I Entanglement, India, Southern Asia, Arms Race, Artificial Intelligence, Counterforce, Credible Minimum Deterrence

INTRODUCTION

The architecture of nuclear deterrence rests on a deceptively simple logic: mutual vulnerability deters first use. When each side can credibly threaten unacceptable retaliatory punishment, regardless of who strikes first, rational actors are incentivised to preserve the peace Brodie (1959), Schelling (1966). This logic sustained the Cold War's long, if tension-filled, stability between the superpowers. Yet the contemporary strategic landscape in Southern Asia reveals how profoundly that logic has been disrupted by the advent of what strategic analysts now cluster under the label of "dual-use emerging technologies": artificial intelligence (AI), cyberwarfare tools, autonomous weapons platforms, and dual-use space-based sensing systems. Each of these technologies was developed predominantly for civilian or conventional military purposes; each has been, or is rapidly being, absorbed into the strategic architectures of nuclear-armed states, and each carries within it a structural propensity to blur the boundary between conventional and nuclear conflict.

*Corresponding Author:
Email address: Shubham Rai (shubham.rai317@gmail.com)

Received: 16 March 2026; **Accepted:** 20 April 2026; **Published** 26 May 2026
DOI: 10.29121/ShodhSamajik.v3.i1.2026.102
Page Number: 189-199
Journal Title: ShodhSamajik: Journal of Social Studies
Journal Abbreviation: ShodhSamajik J. Soc. Stud.
Online ISSN: 3049-2319, **Print ISSN:** 3108-2009
Publisher: Granthaalayah Publications and Printers, India
Conflict of Interests: The authors declare that they have no competing interests.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Authors' Contributions: Each author made an equal contribution to the conception and design of the study. All authors have reviewed and approved the final version of the manuscript for publication.
Transparency: The authors affirm that this manuscript presents an honest, accurate, and transparent account of the study. All essential aspects have been included, and any deviations from the original study plan have been clearly explained. The writing process strictly adhered to established ethical standards.

Southern Asia presents this problem in an especially acute and analytically distinctive form. Unlike the bilateral Soviet-American framework, Southern Asia hosts a tripolar nuclear arrangement involving India, Pakistan, and China, in which deterrence relationships are not dyadic but triangularly interdependent Narang (2014). A technological development that alters the credibility of India's second-strike posture against China simultaneously sends signals—intended or otherwise—to Pakistan. Arms race dynamics do not proceed in isolated bilateral tracks; they cascade and amplify through the triangle. Into this already complex structure, the diffusion of dual-use technologies introduces what this paper argues is a qualitatively new form of strategic

instability, one that cannot be adequately captured by either classical deterrence theory or standard arms-race models.

The central research question animating this inquiry is as follows: In what ways do dual-use technologies accelerate decision compression and C3I entanglement, and how does this alter India's arms race stability? The thesis advanced is that while dual-use technologies provide genuine tactical conventional advantages to states like India, their inherent ambiguity and progressive integration into strategic architectures structurally degrade crisis stability and incentivise asymmetric, qualitative arms racing. To demonstrate this thesis, the paper proceeds as follows. Section Two describes the methodology and surveys the relevant scholarly literature, identifying the key analytical gap this work addresses. Section Three develops the paper's original theoretical contribution—the "Entangled Deterrence" framework—synthesising neo-realist security dilemma theory with modern critical security studies. Sections Four and Five examine the two primary technological domains driving instability: AI and cyber systems, and the aerospace and space sensor environment. Section Six analyses the doctrinal strains these developments impose on established Indian and regional strategic postures, with particular attention to the No First Use (NFU) commitment and credible minimum deterrence (CMD). Section Seven presents a structured case study of the February 2019 Balakot crisis as an empirical illustration of dual-use instability dynamics. Section Eight offers conclusions and policy recommendations.

A note on scope and limitations is necessary. This paper's empirical analysis is bounded by developments up to October 2024. It does not claim to offer a comprehensive history of India's nuclear programme; its focus is strictly on the interaction between dual-use emerging technologies and strategic stability. Furthermore, while the tripolar structure is acknowledged throughout, the primary analytical lens remains India's strategic posture, with China and Pakistan treated as the principal external referents.

METHODOLOGY AND LITERATURE REVIEW

METHODOLOGICAL APPROACH

This paper employs qualitative policy analysis as its primary methodological mode. The evidentiary base consists of official doctrinal documents and defence policy statements from India, China, and Pakistan; publicly available defence procurement records and capability assessments; strategic and security studies literature drawn from peer-reviewed journals, think-tank publications, and official policy reports; and the structured case study of the 2019 Balakot crisis. The paper does not rely on classified materials. When quantitative claims about capabilities are cited, they draw on open-source assessments from recognised authorities such as the Stockholm International Peace Research Institute (SIPRI), the Federation of American Scientists (FAS), and the Carnegie Endowment for International Peace.

The methodological logic is interpretivist: the paper seeks to trace causal mechanisms and identify structural conditions rather than generate statistically generalisable findings. The "process tracing" approach, common in security studies George and Bennett (2005), guides the case study analysis, enabling the identification of specific pathways through which dual-use technologies generated instability dynamics during a real crisis episode.

LITERATURE REVIEW

The foundational scholarship on deterrence stability originates in the classical nuclear age. Brodie (1959) seminal argument that nuclear weapons make war irrational provided the conceptual bedrock, while Schelling (1966) analysis of the "manipulation of risk" introduced the crucial insight that stability is not a condition but a dynamic, subject to deliberate and inadvertent perturbation. Jervis (1978) foundational articulation of the security dilemma—the paradox by which defensive preparations are read as offensive threats—provides the structural logic underlying much subsequent analysis. Lieber and Press (2006) controversially argued that the United States was approaching a genuine counterforce capability against both Russia and China, reigniting debates about the survivability of assured destruction that bears directly on the Indian predicament.

On arms race dynamics, the foundational contributions are Richelson (1990) and Buzan and Herring (1998). These frameworks distinguish between quantitative arms races—more of the same—and qualitative ones, in which the character of weaponry fundamentally changes. It is in the latter category that dual-use technologies predominantly drive competition, as this paper argues. The scholarship on the revolution in military affairs (RMA), associated with Krepinevich (1994) and Murray (1997), anticipated how technological transformation could alter the very grammar of warfare; what was not fully theorised was how civilian-origin technologies, diffused widely across the economy, could enter strategic calculations in ways that elude traditional arms control verification architectures.

The more specific literature on emerging technologies and nuclear stability is a relatively recent growth area. Klare (2019) provides a careful assessment of the dangers posed to nuclear stability by precision-guided munitions, AI, and hypersonic weapons, arguing that the cumulative effect of these technologies is to heighten the risk of inadvertent nuclear war. The Carnegie Endowment's Acton (2018) introduced the concept of "entanglement"—the co-mingling of conventional and nuclear capabilities in shared command-and-control infrastructure—which has become a foundational concept for subsequent analysis and which this paper adopts and extends. Scharre (2018) treatment of autonomous weapons provides an important analysis of how removing human deliberation from lethal decision-making accelerates escalation dynamics, a concern directly relevant to AI-assisted early-warning systems.

In Southern Asia specifically, Narang (2014) comparative analysis of regional nuclear postures is indispensable. Narang distinguishes between India's "assured retaliation" posture and Pakistan's "asymmetric escalation" posture—a distinction that becomes critical when dual-use technologies threaten the viability of assured retaliation. Rajagopalan (2023) work on space and cyber dimensions of Indian security policy provides important empirical grounding. Pant (2011) analysis of India's strategic culture and its tensions with operational nuclear requirements illuminates the doctrinal fault lines through which technological pressures pass. Aurangzeb (2023) explicitly addresses the interplay between emerging technologies and the security dilemma in Southern Asia, noting how dual-use tools such as cyber capabilities and autonomous platforms accelerate competitive dynamics in ways that classical deterrence theory was not designed to manage.

The analytical gap this paper addresses is as follows: most existing literature either focuses on the US-China or US-Russia dyad Acton (2018), Lieber and Press (2006) or treats Southern Asian instability without sufficiently theorising the specific causal mechanisms through which dual-use technologies produce new forms of instability Narang (2014). This paper bridges that gap by developing an original theoretical framework—entangled deterrence—that maps those mechanisms precisely and applies them to the tripolar Southern Asian context.

THEORETICAL FRAMEWORK: ENTANGLED DETERRENCE

The "Entangled Deterrence" framework proposed here synthesises three intersecting theoretical logics to capture the novel instability dynamics produced by dual-use technologies in Southern Asia. The framework is not a refutation of classical deterrence theory but an extension of it, designed to account for conditions that classical theory did not foresee.

THE NEO-REALIST SECURITY DILEMMA AND TECHNOLOGICAL DETERMINISM

Classical neo-realism posits that states in an anarchic international system must seek to maintain or improve their relative power position Waltz (1979). Technological capabilities constitute a primary source of power, and their acquisition by one state—regardless of intent—compels adversaries to respond in kind or through compensatory strategies. Dual-use technologies accelerate this dynamic through what might be termed "technological determinism" at the strategic level: the mere existence and diffusion of advanced capabilities change the strategic environment, irrespective of the original purpose for which those capabilities were developed Khalid (2023).

AI systems developed for commercial logistics can be repurposed for military logistics optimisation. Satellite constellations launched for telecommunications provide persistent overhead surveillance. Cyber tools designed for network security testing serve as weapons. Because these technologies are developed, deployed, and proliferated primarily through civilian markets, states cannot easily restrict an adversary's access to them, nor can they credibly signal defensive intent. The result is a security dilemma operating at a pace and across a domain width that classical theory—formulated in an era of discrete military hardware—was not designed to handle. As Jervis (1978) observed, the security dilemma is most acute when offensive and defensive technologies are indistinguishable; dual-use technologies represent the apotheosis of this condition.

DECISION COMPRESSION AND ALGORITHMIC VULNERABILITY

Traditional deterrence theory assumes that rational decision-makers, upon receiving a warning of an incoming attack, have sufficient time to deliberate, verify, and respond proportionately Schelling (1966). This assumption of deliberative time is not merely incidental; it is structurally essential. Deterrence works because the prospective cost of nuclear retaliation—delivered by a surviving second-strike force—outweighs the prospective gain from a first strike. But this calculus requires that the retaliating state's decision-makers can actually authorise retaliation. If the decision-making process itself is compressed to the point where meaningful human deliberation is impossible—or where it is supplanted by algorithmic systems operating at machine speed—the foundations of deterrence stability are eroded. Fortunato (2023) terms this phenomenon "decision compression": the AI-driven reduction of warning-to-impact timelines to windows measured in minutes, within which human decision loops cannot plausibly operate. The integration of AI into early-warning sensor fusion systems, ballistic missile defence (BMD) targeting, and command authority verification chains is precisely the mechanism through which this compression operates.

Crucially, the vulnerability is not merely temporal; it is epistemic. AI systems trained on historical data patterns are susceptible to adversarial manipulation, data poisoning of sensor inputs, and algorithmic opacity—the inability of human operators to understand why an AI system has produced a particular threat assessment—all of which increase the risk that decision-makers will act on false or manipulated information during a crisis Scharre (2018); Fortunato (2023).

C3I ENTANGLEMENT AND COUNTERFORCE INCENTIVES

The third pillar of the framework addresses the structural entanglement of conventional and nuclear Command, Control, Communications, and Intelligence (C3I) architectures. Acton (2018) demonstrated that when conventional and nuclear forces share the same command networks, communication satellites, or early-warning sensors, a conventional attack—even one with no nuclear intent—can appear, from the adversary's perspective, as the opening salvo of a counterforce nuclear strike. The adversary faces an impossible epistemic choice: wait for confirmation of the attack's nature and risk losing retaliatory capability, or respond immediately and risk escalating a conventional exchange to the nuclear level. Dual-use technologies intensify this dilemma. Space-based commercial imagery satellites that provide persistent monitoring of missile garrisons—indistinguishable to the possessor from dedicated intelligence-gathering—can, in the hands of an adversary, enable real-time tracking of mobile ballistic missile launchers. Precision conventional strike systems, guided by these sensors, theoretically allow a state to destroy an adversary's nuclear delivery systems without crossing the nuclear threshold. This counterforce potential, whether or not a state intends to exploit it, fundamentally changes the calculus of the adversary that possesses the mobile second-strike capability. For India, whose assured-retaliation posture depends on the survivability of road-mobile Agni-series missiles, this is not an abstract concern.

The interaction of these three pillars—accelerated security dilemma, decision compression, and C3I entanglement—produces what this paper terms "entangled deterrence": a condition in which the actors remain formally committed to deterrence-based restraint but are structurally prevented from realising the crisis stability that deterrence is supposed to deliver. The entanglement is not merely technical; it is political and psychological, shaping the threat perceptions and crisis behaviour of decision-makers in ways that increase the probability of miscalculated escalation.

THE AI AND CYBER NEXUS: CRISIS INSTABILITY AND DECISION COMPRESSION

ALGORITHMIC WARFARE AND INDIA'S INTEGRATION OF AI

India's embrace of artificial intelligence for defence applications has accelerated substantially since the publication of its national AI strategy in 2018 and the establishment of the Defence AI Council (DAIC) and Defence AI Project Agency (DAIPA) in 2019 Ministry of Defence, India (2019). These institutional developments reflect a broader recognition that battlefield superiority in future conflicts will be increasingly contingent on the speed and accuracy of information processing. AI applications under active development or integration within India's defence establishment include automated radar signal processing for air defence, AI-assisted satellite imagery analysis for intelligence preparation of the battlefield, machine learning-based logistics and maintenance optimisation, and—most consequentially for this analysis—sensor fusion platforms designed to aggregate data from multiple surveillance streams into a coherent threat picture.

This last application is directly relevant to decision compression. India's integrated theatre commands, under development as part of the ongoing military restructuring process initiated following the 2017 Doklam standoff, are designed to enable rapid, cross-domain responses to threats across air, land, sea, space, and cyber domains simultaneously Pant and Sood (2021). AI-assisted command-and-control systems accelerate the speed at which information is processed, courses of action are generated, and authorisation is sought. In a conventional conflict scenario, this acceleration is operationally advantageous.

In a crisis with nuclear dimensions, however, it is a source of structural danger. The core problem is the compression of what strategists call the "OODA loop"—the observe, orient, decide, and act cycle Boyd (1986). As Fortunato (2023) demonstrates, the introduction of AI into early-warning and threat assessment compresses the decision cycle to a point where the senior decision-maker—who in India's command structure is the Prime Minister, advised by the Nuclear Command Authority (NCA)—receives an algorithmically generated threat assessment rather than a deliberatively assembled human judgement. The difference matters enormously. Human analysts can exercise contextual judgement, flag anomalies in the data, and inject political sensitivity into technical assessments. Algorithms optimise against specified objectives and are opaque about their reasoning. In a crisis in which the difference between a genuine nuclear attack and a spoofed sensor reading could determine whether India launches a retaliatory strike, the epistemological quality of the warning system is not a technical detail—it is a matter of civilisational consequence.

CYBER VULNERABILITIES AND NUCLEAR INFRASTRUCTURE

The cyber domain intersects with nuclear stability through two principal pathways. The first is the direct targeting of nuclear infrastructure: command networks, early-warning radars, and the communication links between the NCA and delivery systems. The 2010 Stuxnet operation against Iran's Natanz enrichment facility—widely attributed to the United States and Israel—demonstrated that cyber weapons could produce physical effects on hardened, air-gapped systems previously considered impervious to remote

attack Lindsay (2013). While Stuxnet targeted enrichment centrifuges rather than weapons systems, its implications for nuclear command infrastructure were widely noted. If a precision cyber weapon could degrade the operational continuity of a nuclear programme through the introduction of corrupted software in industrial control systems, analogous attacks on the computational substrates of nuclear command-and-control are at least technically conceivable.

India's nuclear command infrastructure, including the Strategic Forces Command (SFC) communication networks, is presumed to be hardened against conventional cyber intrusion. However, as Aurangzeb (2023) notes, the increasing connectivity of dual-use platforms—many of which rely on commercially sourced software components with known vulnerabilities—expands the attack surface available to a sophisticated adversary. The supply chain compromise vector, illustrated by the SolarWinds incident of 2020 and analogous attacks on defence contractors in multiple countries, suggests that adversaries need not directly penetrate hardened military networks if they can compromise the civilian infrastructure on which those networks depend for logistics, maintenance, or communications.

The second pathway is epistemic rather than infrastructural: the use of cyber tools to manipulate the information environment during a crisis in ways that generate false positives in early-warning systems or degrade the decision-maker's confidence in the accuracy of available intelligence. A sophisticated cyber intrusion that introduced false radar returns—simulating an incoming ballistic missile trajectory—during a period of heightened tension could, in a system with compressed decision cycles and AI-assisted threat processing, trigger responses that a purely human analytical chain would be more likely to question. This is the scenario that Fortunato (2023) models as the archetypal "inadvertent escalation" pathway in an AI-integrated nuclear command environment.

MAPPING ESCALATION PATHWAYS

Synthesising these dynamics, it is possible to map a plausible escalation pathway in a Southern Asian context. Consider a scenario in which India and Pakistan are engaged in a conventional military exchange following a major terrorist attack attributed to Pakistani state-linked actors. India conducts precision airstrikes on military targets in Pakistani territory. Pakistan, whose nuclear doctrine explicitly incorporates lower thresholds for nuclear use than India—as Narang (2014) documents under the "asymmetric escalation" posture—interprets the precision strikes as potential counterforce preparation: the targeting of its nuclear delivery systems under the cover of a conventional operation.

Pakistan's nuclear command system, potentially also AI-assisted and therefore operating on compressed decision timelines, generates an assessment that a disarming first strike is imminent. The time available for human deliberation in Rawalpindi narrows to minutes. This is not a hypothetical constructed for rhetorical effect; it is a structural consequence of the integration of dual-use AI into command architectures on both sides of the Line of Control. Aurangzeb (2023) identifies this configuration precisely as one of the most dangerous emerging features of the South Asian security environment.

AEROSPACE, SENSORS, AND THE DEFEAT OF AMBIGUITY

SPACE MILITARISATION AND DUAL-USE SATELLITE CONSTELLATIONS

The space domain has undergone a fundamental transformation in the past decade, driven primarily by commercial actors. The proliferation of small satellite constellations—including imaging satellites operated by companies like Planet Labs and Maxar—has democratised access to persistent, high-resolution overhead imagery that was previously the exclusive preserve of superpower intelligence agencies. The strategic implication is profound: any state with sufficient financial resources can now purchase near-continuous monitoring of an adversary's military installations, including missile garrisons and submarine bases. This commercial availability of what was previously a classified state capability constitutes one of the defining features of dual-use technology in the space domain.

For India, the development of indigenous space capabilities has been a strategic priority since the establishment of the Defence Space Agency (DSA) in 2019, which consolidated the management of military space assets previously dispersed across service branches Rajagopalan (2023). India's indigenous RISAT (Radar Imaging Satellite) constellation provides all-weather, day-night surveillance capability relevant to both conventional military operations and strategic monitoring. More significantly, India's March 2019 demonstration of a kinetic anti-satellite (ASAT) capability through Mission Shakti—in which a Prithvi Defence Vehicle missile intercepted an Indian satellite at approximately 300 kilometres altitude—announced India's membership in the exclusive club of demonstrated ASAT powers, alongside the United States, Russia, and China Rajagopalan (2023), Khalid (2023).

Mission Shakti created a new dimension of strategic ambiguity. China, whose own strategic communications and early-warning infrastructure rely substantially on satellite systems, must now factor into its planning the possibility that India could, in a crisis, blind Chinese space-based assets. Pakistan, which depends significantly on Chinese satellite systems for both commercial and military purposes, faces an analogous concern by proxy. From a deterrence theory perspective, an adversary's knowledge that its surveillance and communications satellites are targetable does not straightforwardly enhance stability; it incentivises that adversary to preemptively protect or reconstitute space-based capabilities, generating further competitive dynamics. The space domain thus becomes a theatre of qualitative arms racing even in the absence of a formal arms race declaration.

MISSILE DEFENCE, HYPERSONICS, AND THE OFFENCE-DEFENCE SPIRAL

India's pursuit of ballistic missile defence further illustrates the destabilising potential of dual-use technological acquisition. The Indo-Israeli Arrow system cooperation and the domestic Phase-I BMD development—comprising the Prithvi Air Defence (PAD) for high-altitude interception and the Advanced Air Defence (AAD) for lower-altitude engagement—are framed by Indian officials as purely defensive capabilities designed to enhance deterrence credibility Ministry of Defence, India (2023). This framing is internally consistent with India's assured-retaliation doctrine: if India can intercept an adversary's retaliatory strike, it may maintain the ability to respond even after absorbing an initial attack.

However, from the perspective of an adversary—particularly Pakistan—Indian BMD looks qualitatively different. If India can intercept Pakistani retaliatory missiles, then India's NFU commitment loses its strategic value for Pakistan: India could theoretically strike first and then intercept Pakistan's retaliation. This incentivises Pakistan to expand its arsenal quantitatively and qualitatively to saturate Indian BMD systems and to consider lower-altitude delivery platforms (cruise missiles) and countermeasures (MIRVed warheads and manoeuvring re-entry vehicles) that degrade interception probability. The result is a classic offence-defence spiral in which a capability acquired for ostensibly defensive purposes drives a qualitative arms competition Fortunato (2023), Glaser and Kaufmann (1998). India's development of the Agni-P medium-range ballistic missile—reportedly incorporating manoeuvrability features that complicate interception—and Pakistan's continued development of short-range tactical nuclear delivery systems like the Nasr (Hatf-IX) reflect precisely this dynamic.

On the Chinese side, the development of hypersonic glide vehicles—including the DF-17, which entered operational service by 2019—introduces a delivery modality that current Indian BMD systems cannot reliably intercept Stockholm International Peace Research Institute (2023). China's hypersonic programme, driven by its own concerns about US BMD, has the secondary effect of rendering India's BMD investments partially obsolete against the Chinese threat vector, while simultaneously incentivising India to invest in counter-hypersonic technologies. This is the qualitative arms race dynamic in operation: each technological advance drives compensating developments across the triangle without any party achieving a durable strategic advantage, but with all parties bearing escalating development costs and heightened crisis instability.

THE COUNTERFORCE THREAT TO MOBILE NUCLEAR PLATFORMS

The convergence of persistent space-based surveillance, AI-assisted image analysis, and precision conventional strike capability creates what strategists term a "counterforce temptation": the theoretical ability to locate and destroy an adversary's nuclear delivery systems before they can be launched, potentially enabling a disarming first strike. For India's assured-retaliation posture, the survivability of its road-mobile Agni-IV and Agni-V missiles and its sea-based leg—in the form of the Arihant-class nuclear-powered submarines (SSBNs)—is essential. If an adversary can persistently monitor the operating areas of these systems with sufficient fidelity to enable real-time targeting, the assured retaliation calculus collapses.

Commercial satellite imagery, now available at resolutions below one metre with revisit times measured in hours from commercial operators, provides a foundation for such monitoring. When supplemented by AI-powered change-detection algorithms—which can automatically identify the movement of large vehicles, the opening of missile garage doors, or the departure of submarines from port—the intelligence challenge of tracking mobile nuclear platforms becomes substantially more tractable Acton (2018). Neither China nor Pakistan currently fields a mature AI-satellite fusion capability of this character, but the trajectory of development in both countries suggests this gap will narrow. India, cognisant of this trajectory, has responded by investing in the hardening of its command architecture and expanding the sea-based component of its deterrent—a rational response that simultaneously accelerates the arms competition.

DOCTRINAL SHIFTS AND ARMS RACE STABILITY IN SOUTHERN ASIA

DOCTRINAL STRAIN: NFU AND CREDIBLE MINIMUM DETERRENCE UNDER PRESSURE

India's official nuclear doctrine, last formally articulated in 2003, rests on two foundational commitments: No First Use (NFU) and Credible Minimum Deterrence (CMD). The NFU pledges that India will not initiate the use of nuclear weapons; the CMD states that India will maintain the minimum nuclear force necessary to credibly threaten unacceptable retaliatory punishment without engaging in action-reaction quantitative arms racing Government of India (2003). For over two decades, this doctrinal pairing has provided a degree of structural predictability to the regional deterrence environment, even amid considerable operational ambiguity about what "minimum" means in practice.

Both commitments are under increasing strain from dual-use technological developments. The NFU commitment is credible only if adversaries believe that India would not strike first even if its nuclear forces were at risk. As counterforce technology improves—particularly the AI-satellite-precision-strike triad—this belief becomes harder to sustain. Adversaries calculating India's incentive structure must ask: if India can locate mobile missiles and destroy them conventionally before they are launched, why would India choose strategic restraint? The technological capability does not automatically produce the doctrinal shift, but it degrades the

credibility of the commitment by demonstrating that restraint might, in a sufficiently acute crisis, be operationally irrational Narang (2014), Pant (2011).

Signals in India's political and strategic discourse have reinforced this concern. Notably, in 2019, then Defence Minister Rajnath Singh suggested that India's NFU posture was conditional and could evolve based on "circumstances" The Hindu (2019). While this statement was subsequently walked back by official spokespeople, it introduced a degree of ambiguity into what had previously been an unequivocal commitment. Whether or not the statement reflected genuine doctrinal evolution, its effect on adversary threat perceptions—particularly in Rawalpindi, where Pakistani military planners calibrate their doctrinal posture against Indian capabilities and intentions—was to reduce confidence in the reliability of NFU as a stabilising constraint.

CMD is similarly strained. As AI-assisted BMD capabilities require sophisticated and expensive countermeasures, as hypersonic glide vehicles require dedicated interception research programmes, and as the sea-based deterrent requires the construction of additional SSBNs and submarine-launched ballistic missiles (SLBMs), the threshold between "minimum" and "credible" becomes contestable. There is an endogenous logic to arms racing embedded in CMD: the more adversary capabilities improve, the larger the force required to remain credibly retaliatory. Dual-use technologies accelerate this logic by continuously and unpredictably shifting the capability frontier.

STRATEGIC SUBSTITUTION: ADVERSARY RESPONSES

Regional adversaries have not passively absorbed India's dual-use technological investments. Both China and Pakistan have pursued forms of "strategic substitution": acquiring technologies that compensate for India's emerging advantages and that, in turn, generate new Indian security concerns. This is the arms race dynamic in its most directly observable form. Pakistan's response to India's conventional superiority—particularly the "Cold Start" doctrine and the development of precision strike capabilities—has been a deliberate lowering of the nuclear threshold through the development of tactical nuclear weapons (TNWs). The Nasr (Hatf-IX) short-range ballistic missile, with a reported range of 60 kilometres and a nuclear warhead capacity, is explicitly designed to neutralise India's conventional ground-force advantage by threatening nuclear use at the battlefield level Narang (2014), Kristensen and Norris (2018). From Pakistan's perspective, this is a rational compensatory response. From India's perspective, it is a direct threat to the coherence of CMD because it creates escalation scenarios in which India might face nuclear use at a tactical level before its assured-retaliation doctrine—predicated on second-strike use against adversary cities and military installations—becomes relevant. Dual-use technologies have not caused this doctrinal divergence, but they have accelerated the speed at which it generates crisis risk.

China's response to India's growing conventional and space capabilities is more expansive. China's space programme—including the BeiDou navigation satellite system, the Yaogan series of reconnaissance satellites, and substantial investment in AI-enabled intelligence fusion—provides Beijing with a comprehensive dual-use space architecture that simultaneously serves commercial, military, conventional, and strategic nuclear purposes Khalid (2023), SIPRI, 2023). The opacity of this architecture—the inability of external observers to determine which capabilities are dedicated to conventional or nuclear missions—is itself a source of strategic instability, particularly for India, which must calibrate its responses to Chinese space capabilities without clear insight into their purpose.

THE QUALITATIVE ARMS RACE SPIRAL

The cumulative effect of these dynamics is a qualitative arms race that proceeds not through the visible deployment of additional warheads or delivery systems—the traditional metrics of nuclear arms competition—but through the progressive integration of dual-use technologies into strategic architectures in ways that are individually deniable but collectively destabilising. No single decision—India's development of AI sensor fusion, Pakistan's deployment of Nasr, or China's expansion of its BeiDou constellation—crosses an obvious threshold that would trigger a crisis response or an arms-control intervention. Yet the aggregate effect of these developments is to progressively narrow the space for crisis management, reduce the windows for human deliberation, and increase the counterforce incentives facing all three parties. This is the qualitative arms race that Buzan and Herring (1998) anticipated but whose specific character dual-use technologies have made substantially more opaque and, therefore, more dangerous.

CASE STUDY: THE 2019 BALAKOT CRISIS AND DUAL-USE TECHNOLOGY DYNAMICS

The February–March 2019 India-Pakistan crisis represents the most significant conventional military exchange between the two states since the 1999 Kargil War and the first Indian airstrikes into Pakistani territory since 1971. It provides a uniquely valuable empirical window into how dual-use technologies—specifically, satellite-guided precision strike, electronic warfare, AI-assisted radar systems, and the information environment of social media—interact with nuclear deterrence in a real crisis.

BACKGROUND AND PRECIPITATING EVENTS

On 14 February 2019, a suicide bombing in Pulwama, Kashmir, killed approximately 40 Central Reserve Police Force (CRPF) personnel. The Jaish-e-Mohammed (JeM), a Pakistan-based militant organisation, claimed responsibility. India's government attributed direct responsibility to Pakistan's intelligence services (ISI) and initiated what it described as a "non-military, pre-emptive" retaliatory strike Ministry of Defence, India. (2019)

Affairs, India, 2019). In the early morning of 26 February, Indian Air Force Mirage-2000 aircraft crossed the Line of Control and struck what India claimed was a major JeM training facility at Balakot, in Khyber Pakhtunkhwa province—the first Indian airstrike on undisputed Pakistani territory since 1971.

The dual-use technology dimensions of the crisis were immediately apparent. India's Mirage-2000 aircraft—a platform that serves both conventional and, in some configurations, nuclear roles in the IAF inventory—delivered precision-guided munitions against the target facility. The use of precision-guided munitions, whose guidance technology is inherently dual-use (the same GPS and inertial navigation systems that guide conventional bombs can guide nuclear delivery systems), illustrates the C3I entanglement problem at the operational level: Pakistan could not determine, from external observation, whether the strike package crossing the Line of Control was delivering conventional or nuclear warheads.

DECISION COMPRESSION IN REAL TIME

Pakistan's response was rapid. Within hours, Pakistani Air Force F-16s and JF-17 Thunder aircraft crossed into Indian airspace in what Pakistani officials described as a "demonstration of resolve" Inter-Services Public Relations (2019). In the aerial engagement that followed, the Indian Air Force lost a MiG-21 Bison, whose pilot, Wing Commander Abhinandan Varthaman, was captured after ejecting over Pakistani territory.

The speed of Pakistan's response—measured in hours from India's initial strike to a Pakistani aerial incursion—is illustrative of the decision compression dynamics identified in this paper's theoretical framework. Pakistan's military decision-making cycle, under intense political pressure and with significant national prestige at stake, generated a military response that moved faster than any diplomatic de-escalation process could track.

Critically, the crisis exposed the role of the information environment—a domain in which social media and open-source intelligence (OSINT) constitute a form of dual-use intelligence infrastructure—in shaping the threat assessments of both sides. Commercial satellite imagery, released by operators including Planet Labs and analysed by independent researchers at the Belfer Centre (Harvard) and CSIS, provided a real-time public assessment of the damage at Balakot that contradicted Indian government claims of significant casualties Belfer Center for Science and International Affairs (2019). This publicly available commercial intelligence—simultaneously accessible to both governments, their militaries, and their domestic publics—complicated crisis communication in ways that classical deterrence theory, which assumed governments controlled the information environment, could not anticipate. Pakistani decision-makers could access the same commercial satellite assessment as Indian decision-makers, reducing the asymmetric information advantage that India might otherwise have exploited for coercive leverage.

NUCLEAR SIGNALLING AND THE DUAL-USE THRESHOLD

The crisis reached its most acute phase on 27 February, when Pakistani Prime Minister Imran Khan's address to the nation contained what many analysts interpreted as veiled references to Pakistan's nuclear deterrent, warning that the situation should not be allowed to escalate beyond control Dawn (2019). Meanwhile, India placed its Integrated Rocket Force on alert and conducted a test launch of an Agni-II ballistic missile that India characterised as a routine "user trial" but which Pakistan read as a deliberate nuclear signal Pandi (2019). Whether intentional or not, the missile test—involving a delivery system that is inherently dual-use—crossed a signalling threshold that contributed to international alarm and to the intensive US-Saudi diplomatic intervention that ultimately produced Pakistan's return of Wing Commander Varthaman on 1 March 2019.

The Balakot crisis thus illustrates each of the Entangled Deterrence framework's three pillars in operation. The neo-realist security dilemma was visible in the speed with which each side's actions were interpreted as threats requiring immediate military response rather than diplomatic engagement. Decision compression was evident in the sub-24-hour timelines from India's strike to Pakistan's aerial response, in the nuclear signalling that followed within days, and in the internationally expressed alarm about the pace of escalation. C3I entanglement manifested in the dual-use character of the aircraft, munitions, and ballistic missile systems involved—each platform serving both conventional and potentially nuclear roles, making adversary intention reading structurally unreliable.

LESSONS FOR THE ENTANGLED DETERRENCE FRAMEWORK

Several analytical lessons emerge from the Balakot case that both validate and refine the framework. First, the crisis confirms that dual-use technology blurring operates even in a crisis where neither party intends nuclear escalation: the structural features of the environment generate nuclear signalling and alarm independently of decision-maker intent. This is consistent with the framework's emphasis on structural rather than intentional mechanisms of instability. Second, the role of commercial dual-use surveillance (satellite imagery) in shaping both governments' assessments and both publics' information environments represents a dimension of C3I entanglement not fully anticipated by earlier scholarship. Third, and most sobering, the speed of escalation—from a terrorist attack to a nuclear crisis requiring superpower mediation in under two weeks—demonstrates empirically how compressed the decision-making timelines in the Southern Asian nuclear environment have already become, even before the full integration of AI into command-and-control systems.

The Balakot crisis was, in retrospect, a controlled experiment in dual-use instability: a case in which the structural features of the technology environment pushed a conventional military exchange toward the nuclear threshold faster than diplomatic processes could respond, and in which the crisis was resolved not by the functioning of deterrence logic but by external intervention and the shared exhaustion of crisis participants.

The lesson for the Entangled Deterrence framework is that the instability mechanisms it identifies are not future risks; they are present realities, already operating in the current technological environment, and likely to intensify as AI, satellite sensing, and precision strike capabilities are further integrated into Indian, Pakistani, and Chinese strategic architectures.

CONCLUSION AND POLICY RECOMMENDATIONS

SYNTHESIS

This paper has argued that dual-use technologies are not merely adding new capabilities to an existing strategic environment in Southern Asia; they are qualitatively transforming the structure of that environment in ways that classical deterrence theory is inadequate to capture. The "Entangled Deterrence" framework, developed across the preceding sections, identifies three interacting mechanisms driving this transformation: the acceleration of the neo-realist security dilemma through technological determinism; the compression of deliberative decision-making timelines through AI integration into command-and-control architectures; and the entanglement of conventional and nuclear C3I networks in ways that generate pervasive counterforce incentives and escalation pathways.

The empirical analysis of India's specific strategic posture demonstrates that these mechanisms operate across multiple technological domains simultaneously. AI sensor fusion and cyber vulnerabilities erode the epistemological foundations of crisis management. Space-based sensing and dual-use satellite constellations threaten the survivability of mobile second-strike platforms. Missile defence development drives offence-defence spirals. Doctrinal commitments to NFU and CMD face mounting credibility challenges as technological asymmetries widen and deepen. And the 2019 Balakot crisis provides stark empirical evidence that these instability dynamics are already present in the real-world strategic environment, pushing crises toward nuclear thresholds at speeds that outpace the diplomatic and deliberative processes that deterrence stability requires.

The fundamental insight that emerges is this: dual-use technologies convert deterrence from a condition of managed mutual vulnerability—stable, if unpleasant—into a volatile state of entangled interdependence in which the distinction between conventional and nuclear conflict is structurally blurred, in which decision-making timelines are compressed beyond the threshold of meaningful human deliberation, and in which the pursuit of security by each actor generates insecurity for all. This is not a critique of Indian, Pakistani, or Chinese strategic planners; it is a structural analysis of the environment within which all parties must operate. The appropriate response is not technological restraint—which no state is likely to practise unilaterally—but the deliberate construction of institutional, doctrinal, and diplomatic architectures capable of managing the instability that these technologies generate.

POLICY RECOMMENDATIONS

1) Establish AI-Specific Crisis Communication Protocols

India, China, and Pakistan should explore the establishment of dedicated crisis communication channels specifically designed to address AI-generated false positives and sensor anomalies. The existing hotlines between New Delhi and Islamabad have been inconsistently maintained and were reportedly not used during the 2019 crisis Sood (2020). A new architecture, modelled on the Cold War US-Soviet "Direct Communications Link" but updated for the AI era, should include agreed-upon protocols for communicating the existence of potential sensor errors during a crisis—a form of "algorithmic transparency signalling" that reduces the risk of inadvertent escalation from AI-generated threat assessments Aurangzeb (2023), Klare (2019).

2) Pursue Verifiable C3I Separation Agreements

The most direct response to C3I entanglement is deliberate structural separation of conventional and nuclear command networks. While full separation may be operationally impractical given the dual-use nature of satellite communications and early-warning infrastructure, partial separation agreements—covering, for instance, dedicated electromagnetic spectrum allocations for nuclear command communications that are explicitly protected from cyber attack and counter-space targeting—could reduce the entanglement risk without requiring complete technological bifurcation. Such agreements would need to be verifiable, which in turn requires confidence-building transparency measures about the technical architecture of C3I systems—a significant but not unprecedented demand in arms control history Acton (2018).

3) Develop Multilateral Space and Cyber Codes of Conduct

India should actively promote the negotiation of a multilateral space code of conduct within the UN Committee on the Peaceful Uses of Outer Space (COPUOS) and parallel diplomatic forums, with specific provisions addressing the protection of dual-use satellite infrastructure during conventional military operations. An analogous process in the cyber domain—building on the work of the UN Group of Governmental Experts (GGE) on responsible state behaviour in cyberspace—should explicitly address the question of cyber attacks on nuclear command infrastructure, establishing a norm analogous to the existing, if fragile, taboo against targeting nuclear early-warning systems with kinetic weapons Rajagopalan (2023), Klare (2019).

4) Reinforce Doctrinal Clarity on NFU

India should resist the temptation to exploit the strategic ambiguity created by its growing dual-use capabilities by allowing NFU ambiguity to deepen. While some strategic analysts argue that doctrinal ambiguity serves deterrence by introducing uncertainty into adversary calculations, the evidence from the Balakot crisis suggests that ambiguity in the Southern Asian context generates panic rather than caution. India should issue an updated, comprehensive nuclear doctrine document—the last such document dates to 2003—that explicitly addresses how emerging technologies interact with NFU and CMD commitments, providing greater transparency to adversaries and reducing the risk of misperception-driven escalation. This is not a call for unilateral concession; it is a recognition that clarity, in an environment of technological fog, is itself a form of strategic stability management.

DIRECTIONS FOR FUTURE RESEARCH

Several questions that fall outside the scope of this paper warrant future investigation. The specific technical architecture of India's nuclear command authority (NCA) and its interaction with AI-assisted military decision-support systems is a domain in which public information is insufficient for rigorous academic analysis; as declassification processes mature, this will be a productive research area. The role of non-state actors and proxy forces in triggering dual-use instability—illustrated by Jaish-e-Mohammed's role as the proximate trigger of the 2019 crisis—deserves further theoretical development, as classical deterrence theory focuses on state-to-state interactions and is poorly equipped to address the cascading effects of sub-state violence in a dual-use technological environment. Finally, the prospects for and limits of formal arms control in a qualitative arms race context—where the relevant "armaments" are software systems, sensor architectures, and AI algorithms rather than countable warheads—represent a fundamental challenge for the arms control community that demands sustained scholarly attention.

The trajectory of dual-use technological development in Southern Asia is not a path that resolves favourably without deliberate and sustained policy intervention. The structural features of entangled deterrence, left unaddressed, point toward a future in which the probability of inadvertent nuclear use during a conventional crisis—not through decision-maker recklessness but through the structural compression of time, the entanglement of architectures, and the opacity of algorithms—increases with each passing year. Averting that future is among the most consequential strategic challenges of the early twenty-first century.

ACKNOWLEDGMENTS

None.

REFERENCES

Acton, J. M. (2018). Entanglement: Chinese and Russian Perspectives on Non-Nuclear Weapons and Nuclear Risks. Carnegie Endowment for International Peace.

Aurangzeb, M. (2023). Emerging Technologies and the Security Dilemma in South Asia. Journal of Development and Social Sciences, 4(3), 112–129.

Belfer Center for Science and International Affairs. (2019). Satellite Imagery of the Balakot Strike Site. Harvard Kennedy School. Retrieved February 12, 2023, from

Boyd, J. R. (1986). Patterns of Conflict [Unpublished Briefing Document]. United States Air Force.

Brodie, B. (1959). Strategy in the Missile Age. Princeton University Press. https://doi.org/10.1515/9781400875108

Buzan, B., and Herring, E. (1998). The Arms Dynamic in World Politics. Lynne Rienner Publishers. https://doi.org/10.1515/9781685854003
Carnegie Endowment for International Peace. (2023). Introduction: Emerging Technologies and the Future of Strategic Stability [Working Paper].
Dawn. (2019, February 27). PM Imran Khan's Address to the Nation. Dawn. Retrieved April 17, 2024, from
Fortunato, M. A. (2023). Artificial Intelligence, Missile Systems, and Missile Defense: Decision Compression, Vulnerability, and Escalation Dynamics in South Asia. Security Science Journal, 4(1), 45–74.
George, A. L., and Bennett, A. (2005). Case Studies and Theory Development in the Social Sciences. MIT Press.
Glaser, C. L., and Kaufmann, C. (1998). What is the Offense-Defense Balance, and Can we Measure it? International Security, 22(4), 44–82. https://doi.org/10.2307/2539240
Government of India. (2003, January 4). Cabinet Committee on Security reviews operationalisation of India's Nuclear Doctrine. Press Information Bureau. Retrieved August 9, 2023, from
Inter-Services Public Relations. (2019, February 27). ISPR Statement on Aerial Engagement. Pakistan Armed Forces. Retrieved September 14, 2024, from
Jervis, R. (1978). Cooperation Under the Security Dilemma. World Politics, 30(2), 167–214. https://doi.org/10.2307/2009958
Khalid, A. (2023). U.S.-China Militarisation and the Risks to Global Strategic Stability. Strategic Studies Quarterly, 17(2), 88–113.
Klare, M. T. (2023, February). Assessing the Dangers: Emerging Military Technologies and Nuclear (in)Stability. Arms Control Today. Retrieved January 29, 2024, from
Krepinevich, A. F. (1994). Cavalry to Computer: The Pattern of Military Revolutions. The National Interest, (37), 30–42.
Kristensen, H. M., and Norris, R. S. (2018). Pakistani Nuclear Forces, 2018. Bulletin of the Atomic Scientists, 74(5), 348–358. https://doi.org/10.1080/00963402.2018.1507796
Lieber, K. A., and Press, D. G. (2006). The Rise of U.S. Nuclear Primacy. Foreign Affairs, 85(2), 42–54. https://doi.org/10.2307/20031910
Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122
Ministry of Defence, India. (2019). Annual Report 2019–20. Government of India. Retrieved December 3, 2023, from
Ministry of Defence, India. (2023). Annual Report 2023–24. Government of India. Retrieved March 18, 2024, from
Ministry of External Affairs, India. (2019, February 26). Official Spokesperson's Statement on Preemptive Strike. Government of India. Retrieved August 2, 2024, from
Murray, W. (1997). Thinking About Revolutions in Military Affairs. Joint Force Quarterly, (16), 69–76. https://doi.org/10.21236/ADA354177
Narang, V. (2014). Nuclear Strategy in the Modern Era: Regional Powers and International Conflict. Princeton University Press. https://doi.org/10.23943/princeton/9780691159829.001.0001
Pandit, R. (2019, February 27). India Carries out Ballistic Missile Test Amid Standoff. The Times of India. Retrieved May 21, 2024, from
Pant, H. V. (2011). The U.S.-India Nuclear Pact: Policy, Process, and Great Power Politics. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198073963.001.0001
Pant, H. V., and Sood, V. (2021). An India that Can Say Yes: A Responsible Rising Power. Observer Research Foundation.
Rajagopalan, R. P. (2023). India's Space Cybersecurity Mesh: Criticality and Call of Purple Revolution. Observer Research Foundation. Retrieved July 7, 2024, from
Richelson, J. (1990). Defying the Arms Race: Verification and Verification Challenges. Arms Control, 11(2), 159–183.
Scharre, P. (2018). Army of None: Autonomous Weapons and the Future of War. W. W. Norton and Company.
Schelling, T. C. (1966). Arms and Influence. Yale University Press. https://doi.org/10.2307/j.ctt5vm52s
Sood, V. (2020). India's Wars: A Military History, 1947–1971 [With Supplementary Crisis Communication Analysis]. HarperCollins India.
Stockholm International Peace Research Institute. (2023). SIPRI yearbook 2023: Armaments, Disarmament and International Security. Retrieved February 28, 2024, from https://doi.org/10.1093/sipri/9780198890720.002.0008
The Hindu. (2019, August 16). India's no-First-Use Policy May Change, Says Rajnath Singh. The Hindu. Retrieved September 4, 2023, from
Waltz, K. N. (1979). Theory of International Politics. Addison-Wesley.