Journal of Strategic Security

Volume 19 | Number 2 Article 2

Escalation by Algorithm, Restraint by Architecture: Pakistan's Military AI Divergence

Sajjad Ahmed
University Malaysia Sarawak, sajjad.ah911@gmail.com

Ahmad Nizar Yaakub
University Malaysia Sarawak, nizar@unimas.my

Asma Javed
Islamabad Model College for Girls, asma.sajjad289@gmail.com

pp. 23-46

Recommended Citation
Ahmed, Sajjad; Yaakub, Ahmad Nizar; and Javed, Asma. "Escalation by Algorithm, Restraint by Architecture: Pakistan's Military AI Divergence." *Journal of Strategic Security* 19, no. 2 (2026) : 23-46.
DOI: https://doi.org/10.5038/1944-0472.19.2.2527
Available at: https://digitalcommons.usf.edu/jss/vol19/iss2/2

Escalation by Algorithm, Restraint by Architecture: Pakistan's Military AI Divergence

Abstract

Debates on military artificial intelligence (AI) remain skewed toward great power dynamics, oscillating between techno-optimist celebrations of speed and techno-pessimist warnings of collapse. This binary overlooks how middle powers, operating under nuclearized rivalry and asymmetric sanction risk, embed restraint into organizational and technical practice. This article develops Systems Restrained Realism (SRR), a framework that extends defensive realism into the machine age by theorizing restraint as a deliberate doctrinal posture rather than a symptom of incapacity. Using Pakistan as a critical case, the study draws on expert interviews, procurement manuals, and UN submissions to demonstrate how restraint is operationalized through latency as doctrine, embedded organizational oversight, and localized training regimes designed to mitigate classifier fragility. The findings reveal that while India's accelerationist AI trajectory projects capability and ambiguity, Pakistan engineers restraint into systems and decision loops, externalizing it through normative signaling at UN forums. This posture highlights a structural asymmetry: Great powers can afford AI misfires under the banner of innovation, while middle powers face punitive scrutiny for errors, incentivizing opacity over transparency. By foregrounding SRR, the study challenges dominant narratives that equate restraint with weakness and automation with stability. It argues that in an era of machine-speed conflict, survival may hinge not on what states automate but on what they refuse to.

Acknowledgements

The authors acknowledge partial funding by UNIMAS and worthy interviewees whose insights helps the study to standalone in the field.

Introduction

South Asia is among the most volatile nuclear dyads in the world, marked by recurring crises, small-scale wars, and enduring risks of inadvertent escalation.[1] Into this fragile balance enters artificial intelligence (AI), a technology lauded for enhancing efficiency yet feared for compressing decision cycles and eroding human judgment.[2] India has actively showcased AI integration, including drone swarm demonstrations on Republic Day, doctrinal reforms, and new procurement rules in the Defence Research and Development Organisation (DRDO) Procurement Manual 2025, while think tanks such as the Carnegie Endowment for International Peace frame AI as both an opportunity and a risk.[3] Pakistan, by contrast, highlights danger: its Ministry of Defence Production yearbooks policy analyses, and United Nations submissions consistently warn of nuclear–AI entanglement and machine-speed escalation.[4] The juxtaposition is striking. India accelerates, Pakistan restrains, yet this asymmetry remains poorly theorized in the wider literature on military AI.[5]

The existing scholarship provides useful but incomplete frameworks. Work on organizational accidents emphasizes how complexity and tight coupling can generate systemic failures.[6] Research on the diffusion of technology highlights that military adoption depends on state capacity and organizational culture.[7] Analyses of the security dilemma and stability-instability paradox illustrate how military innovations can simultaneously deter and provoke escalation.[8] Recent debates polarize between techno-optimism, which assumes automation enhances stability, and techno-pessimism, which sees autonomy as accelerating collapse in a complex, multipolar world.[9] Yet neither perspective fully captures why and how some states actively codify restraint into the design of military systems.

This article develops the concept of Systems Restrained Realism (SRR) to explain such practices. Rather than treating restraint as accidental weakness or inevitable collapse, SRR conceptualizes it as a deliberate security posture in which states embed latency, oversight, and human-in-the-loop safeguards into AI systems. By integrating insights from accident-risk theory, critiques of technological determinism, and extensions of defensive realism, SRR reframes restraint as strategic agency rather than incapacity. This position advances existing debates

on autonomous systems such as drones by scholars such as Scheuerman, Chamayou, and Bruun & Blanchard, demonstrating how doctrines of caution are translated into algorithms, procurement requirements, and operational rules.[10]

By placing South Asia at the center of analysis, the study also addresses a geographic blind spot: much of the AI and security literature focuses on US-China or NATO-Russia dynamics. At the same time, the Indo-Pakistani rivalry offers an equally consequential laboratory for observing how autonomy intersects with nuclear stability.[11] Empirically, the study triangulates across multiple forms of evidence: Pakistani experts' views on ground realities, doctrinal texts, procurement manuals, and UN submissions; Indian AI strategies, DRDO reforms, and independent analyses; and global assessments of military autonomy and governance across land, sea, and air. This approach allows us to evaluate whether restraint in Pakistan is merely structurally driven by economic and industrial constraints or a conscious effort to embed caution into system design.

The broader implication is that the India-Pakistan dyad serves as an early stress test for how AI technologies reshape nuclear rivalries and crisis dynamics. The findings carry significance not only for South Asian stability but also for global governance debates on the security dilemma posed by lethal autonomous weapons, meaningful human control (MHC), and the management of crises at machine speed. Through SRR, this study provides a sharper test of whether restraint emerges from structural weakness or from deliberate choice, redefining restraint as a survival strategy in fragile, asymmetric, and nuclearized security environments.

Strategic AI Militarization and Divergent Doctrinal Architectures

The global integration of AI into military doctrine, command and control, and warfighting capabilities constitutes a paradigm shift in twenty-first-century security architecture. Initial scholarship emphasized AI's potential to enhance precision, efficiency, and situational awareness in complex environments.[12] More recent work has examined the destabilizing potential of military AI for deterrence, escalation dynamics, and operational control.[13] This tension reflects a growing divide between techno-optimist arguments that automation improves stability through speed and accuracy and techno-pessimist

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

perspectives that warn of accident risk, classifier error, and compressed escalation timelines.[14]

National approaches reveal striking divergence. The United Kingdom and France have articulated comprehensive strategies that codify ethical principles, set autonomy thresholds, and establish frameworks for human oversight. The United States, despite its normative leadership, has revealed inconsistencies, particularly during the Global War on Terrorism, when drone warfare and pattern-of-life analytics in Pakistan, Afghanistan, and other regions generated widespread civilian harm, instability, and chaos.[15] India, in contrast, has prioritized accelerated battlefield deployment, defense-industry partnerships, and operational trials without clear doctrinal guardrails. Pakistan's state submissions and policy documents emphasize caution, highlighting risks of algorithmic opacity and the potential for AI-nuclear entanglement.

While emerging studies have begun to recognize the relevance of middle powers in AI militarization, analyses of South Asia's rivalry remain fragmented, descriptive, and largely detached from deeper theorization. These accounts often catalogue developments or highlight risks but stop short of systematically embedding them in frameworks such as the security dilemma or accident-risk theory. This article introduces SRR as a corrective framework: one that conceptualizes restraint not as weakness or developmental lag, but as a deliberate doctrinal choice embedded in technical systems, organizational routines, and procurement pathways. By integrating insights from accident-risk theory and critiques of technological determinism, SRR provides analytical tools to understand how asymmetric rivals such as India and Pakistan translate systemic risk into distinct doctrinal logics. This reframing enables a sharper theorization of why Pakistan adopts embedded restraint even under adversarial pressure, a phenomenon underexplored in the existing literature.

Reinterpreting the Security Dilemma in the Age of Machine Autonomy

The classical security dilemma, as articulated by Jervis (1978), emphasizes how defensive measures by one state often create insecurity for another, especially under conditions of opacity and ambiguity.[16] AI compounds these dynamics. Autonomous systems can act without human intervention, accelerate decision timelines, and misclassify

inputs in ways political leaders neither anticipate nor control. This transforms the security dilemma into a technologically mediated phenomenon, where escalation risks stem not only from political intentions but also from algorithmic unpredictability.

Emerging scholarship has flagged these risks. Studies highlight the erosion of escalation control due to machine speed, classifier error, and reduced decision latency.[17] Yet most analyses stop short of theorizing how states integrate these concerns into their doctrinal logic, particularly in volatile regional contexts such as South Asia. Here, ambiguity is not only political but also technical, with machine autonomy compressing decision windows, rendering deterrence signaling increasingly fragile.

This study advances defensive realism by grounding it in SRR, beyond the security dilemma and 5th-generation warfare. Unlike classical realism, which privileges material capabilities and adversarial intent, SRR foregrounds the systemic and technological fragilities that condition state behavior under conditions of asymmetry and uncertainty. It posits that in the age of autonomous military systems, escalation is not driven solely by political ambition or power imbalance, but also by embedded risks within technological architectures, organizational routines, and normative pressures. SRR draws on three intellectual traditions.

First, the accident-risk scholarship by Sagan (1993) and Perrow (2011) demonstrates that complex, tightly coupled systems are prone to failure not as anomalies but as systemic inevitabilities.[18] AI-enabled military platforms, subject to classifier drift, data degradation, or sensor misrecognition, carry the same inevitability of error, magnified by their speed and autonomy. Second, critiques of technological determinism challenge the assumption that technology is neutral, showing instead that machines reshape political choices, ethical boundaries, and even the thresholds for violence. Applied to military AI, these insights reveal that algorithms not only execute doctrine but also actively co-produce it by encoding bias, fragility, and escalation potential.[19] Third, SRR adapts elements of defensive realism by highlighting how survival in fragile regional systems depends less on aggressive balancing than on calibrated restraint, latency, and ethical positioning.

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

Within this framework, restraint is theorized not as incapacity but as strategic optimization. By deliberately embedding Human-in-the-Loop safeguards, localizing datasets, and imposing doctrinal latency, states such as Pakistan are not "lagging" but actively insulating themselves against the destabilizing volatility of machine-led escalation. SRR, therefore, reframes restraint as agency, treating ethical coding, doctrinal brakes, and organizational caution as instruments of survival in adversarial environments where small errors can cascade into nuclear consequences.

In doing so, SRR contributes a novel analytical lens to strategic studies: one that integrates accident-prone technological infrastructures, socially constructed algorithmic biases, and geopolitical asymmetry into a single explanatory model. This framework not only clarifies Pakistan's restrained posture in the face of India's rapid AI militarization but also offers comparative leverage for analyzing other middle powers, such as Taiwan, Iran, and Singapore, whose strategies are defined less by acceleration and more by carefully engineered restraint within global technological competition.

From National Doctrine to Embedded Organizational Restraint

Much of the literature treats the published national military doctrine as the benchmark of responsible military AI adoption. Yet restraint may also manifest without codified strategies, through institutionalized practices embedded at organizational levels. Technologically advanced militaries such as those of the United States, the United Kingdom, and France codify AI norms through centralized strategies.[20] At the same time, India emphasizes capability-building through defense-industry collaboration and rapid-deployment trials.

Pakistan, by contrast, signals a different trajectory. Publicly available documents ranging from UN submissions to procurement manuals and ministerial statements consistently stress autonomy ceilings, classifier control, and human oversight as non-negotiable safeguards. This posture suggests that restraint is not absent simply because no national doctrine exists; rather, it is embedded in dispersed institutional routines and operational practices. Strategic studies have yet to fully theorize this phenomenon. The dominant assumption that formal doctrine equals responsibility while its absence implies weakness overlooks the possibility that decentralized architectures can generate

coherent systems of caution. Recognizing this opens analytical space for frameworks such as SRR, which treat restraint as a deliberate design choice rather than a developmental lag.

Training Context as Strategic Risk: The Limits of Generalized Autonomy

Existing literature has paid limited attention to the strategic significance of training environments in shaping AI-related risks. Algorithmic performance is not determined solely by system architecture but by the contextual fidelity of its training data. Failures in this domain are well documented: US drone operations repeatedly misclassified civilian gatherings as militant activity, leading to catastrophic escalation and reputational damage.[21] Yet much of the strategic analysis continues to assume data neutrality, overlooking how training environments themselves constitute a critical site of risk production.

In regions such as South Asia, where ethnographic diversity, contested geographies, and fluid civilian-combatant behaviors complicate classification, the limits of generalized autonomy are particularly acute. Recognizing dataset fragility and contextual misrecognition as central variables extends accident-risk theory into the digital age and reframes debates on deterrence, escalation, and doctrinal restraint. Integrating these dimensions highlights how training data is not a neutral technical input but a strategic variable, one that can either exacerbate or mitigate the risks of machine-speed decision making in volatile security environments.

Research Gap and the Study's Contribution

Despite a growing body of scholarship, three critical gaps persist in the literature. First, analyses of AI militarization remain disproportionately concentrated on major-power contexts, particularly US-China and NATO-Russia, while asymmetric regional rivalries such as India-Pakistan receive limited theoretical attention despite their nuclearized volatility. Second, existing assessments tend to equate responsible adoption with the publication of national strategies, overlooking embedded organizational restraint expressed in procurement protocols, operational guidelines, and UN submissions, which may function as de facto doctrinal frameworks. Third, AI system risk continues to be

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

framed primarily through international norms and IHL compliance, with insufficient engagement with classifier fragility, training environments, and latency as strategic design choices.

This article addresses these gaps by advancing SRR as a new theoretical lens. By situating the India-Pakistan dyad within both the classical security dilemma and SRR, it demonstrates that restraint can be deliberately engineered through organizational practices, technical safeguards, and latency, rather than merely being a by-product of incapacity. In doing so, the study reframes restraint as a proactive strategic posture in the age of autonomous systems, as posture scholars often call 6th-generation Warfare, offering conceptual and empirical contributions to both AI security studies and debates on nuclear stability.

Methodology

This study employs a qualitative, theory-informed case study design to analyze Pakistan's evolving military AI posture.[22] Pakistan was selected as a critical case because, although not an AI superpower, it operates within a nuclearized dyad with India in which technological asymmetry, repeated crises, and prior exposure to algorithmic warfare during the Global War on Terrorism converge. Primary data were collected through fifteen semi-structured experts' interviews in two episodes from November 2023-February 2024 and May 2025 with respondents across strategic, technical, and academic communities, including senior officers from Intelligence, Surveillance, and Reconnaissance (ISR), cyber and C2 divisions to explore readiness of Pakistan military within aspects of land and air defense; engineers and program leads affiliated with the National Engineering and Scientific Commission (NESCOM) and the Artificial Intelligence Technology Centre (AITeC) director; academic researchers at the National University of Sciences & Technology (NUST) and Quaid-i-Azam University; and policy advisers engaged in AI defense integration. Interviews used open-ended questions, allowing respondents to elaborate freely, and lasted 40-70 minutes, depending on participants' responses and follow-up probes. Access in a securitized environment required a combination of chain-based referral and purposive sampling. Several invitees initially declined due to the sensitivity of the research matter, but participation was secured through trusted introductions. To avoid bias from insider-only perspectives, the sample

deliberately included non-uniformed experts whose portfolios involved extensive defense-linked AI projects alongside uniformed personnel and engineers. Thematic saturation, as defined by Braun and Clarke, was reached in the thirteenth interview, with the remaining two interviews confirming the stability of the coding frame.[23] To minimize the risk of scripted responses, substantively similar questions were asked in varied forms across different interviews, and responses were compared with contextual notes and available open-source data for corroboration.

The broader project from which this article derives employed open-ended inductive coding across the full interview set, allowing a wide range of categories to surface without prior imposition. For this work, however, themes were refined and selected deductively to align with the security dilemma theoretical lens, and SRR was proposed to address the thesis objectives. This dual process combined inductive openness with theoretical focus, enhancing methodological rigor while sharpening analytical contribution. Transcripts were coded line by line in NVivo 12, then clustered into the article's final thematic architecture: "Indian Battlefield AI as a Perceived Strategic Escalator," "Latency as Doctrine: Human-in-the-Loop for Escalation Control," "Embedded Organizational Restraint in the Absence of a National Doctrine," "Normative Signaling and Global Engagement," and "Strategic Risk and the Necessity of Contextualized AI Training." Triangulation was conducted through cross-checking against official documents and comparative doctrinal literature on India, Israel, and France, which were used as benchmarks rather than parallel cases. The author's institution granted ethical approval; interviews were anonymized to ensure confidentiality; bilingual [English and Urdu] transcription and cross-validation were applied where needed; and no classified information was requested or recorded. These safeguards collectively ensure that findings are credible, transferable, and consistent with the sensitivity of the research context.

Emerging themes highlight a posture that diverges from existing depictions of AI militarization as either capability-maximizing or normatively constrained. Instead, Pakistan illustrates a hybrid architecture in which restraint is institutionalized across technical, doctrinal, and organizational levels. Each theme, therefore, represents not only an empirical finding but also a theoretical intervention into debates on the security dilemma, SRR, and the role of middle powers in

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

AI militarization. What follows is an in-depth examination of these themes presented as the organizing framework of the analysis rather than as descriptive findings alone.

Indian Battlefield AI as a Perceived Strategic Escalator

Across Pakistan's strategic, technical, and academic communities, India's accelerated pursuit of AI-enabled battlefield systems is interpreted less as routine modernization and more as a doctrinal continuation of its long-standing offensive posture. From its first nuclear test to the articulation of the Cold Start doctrine, recurring calls for an "Akhand Bharat" have been described by Midha as US-India, UK-India, and India-Israel defense deals that strategically signal preemption, rapid mobilization, and regional dominance.[24] AI integration swarm demonstrations on national days, capability-first trials along the Line of Control, and procurement reforms in the DRDO manual are read as the latest iteration of this offensive trajectory.[25]

Within the SRR lens, the escalatory danger does not arise from technology in isolation, but from how India integrates emerging systems with doctrines historically tilted toward compellence rather than deterrence. A senior ISR commander described India's swarm trials as "escalation rehearsals [first use of killer drones], not deterrence signals," noting that rapid loops "erase the time [don't wait for authentication], we need to verify and de-conflict."[26] A defense R&D engineer observed: "Cold Start was designed to collapse our window; battlefield AI shortens it further."[27] A respondent from AITeC stressed that "India runs capability-first under uncertainty; doctrine trails the demonstration, so the burden of caution shifts to us [Pakistan]."[28] An academic expert added that "models [algorithms] tuned for parades or controlled trials don't translate to the fluidity of our borderlands [where a single small mistake leads to heavy loss], but India pushes ahead regardless."[29]

Historical experience deepens this perception. Pakistan's exposure to US drone misfires on women and children in Damadola (2006) in Uruzgan (2010) and the Salala incident (2011), where autonomous systems misidentified Pakistan military personnel and were killed, instilled the lesson that machine-speed targeting collapses buffers for verification and shifts escalation beyond political control.[30] A senior policy adviser concluded: "Great powers like the US or those [Israel]

backed by them [Superpowers] can survive mistakes. For us, one misfire risks sanctions or isolation [at the time of nuclear tests]. Restraint is survival as much as strategy."[31]

Triangulated with India's procurement and doctrinal documents, these insights reinforce a consistent reading: Battlefield AI is not destabilizing because technology itself is malign, but because India's offensive doctrines, layered with machine-speed systems, amplify escalation risks in a nuclearized rivalry.[32] From an SRR perspective, Pakistan perceives these moves as deliberate doctrinal escalators that require its own counter-architecture of restraint, latency, and Human-in-the-Loop (HITL) oversight.

Latency as Doctrine: Human-in-the-Loop for Escalation Control

In sharp contrast to India's accelerationist trajectory, Pakistan has institutionalized latency (delay) as a doctrinal principle of AI integration.[33] The delay is not conceived as inefficiency but deliberately engineered as decision friction to safeguard escalation control in a nuclearized rivalry. Within the SRR framework, this latency reflects embedded restraint: The intentional design of buffers, oversight, and pause mechanisms to counter systemic fragility and adversarial acceleration. This diverges from techno-optimist narratives that treat machine speed as a guarantor of advantage and from European strategies that codify latency mainly as an ethical safeguard in national AI doctrines. For Pakistan, latency is neither an abstract ethical concern nor a technological incapacity; it is an operationalized restraint strategy rooted in the structural risks of inadvertent escalation.

Interview data consistently reinforce this doctrinal orientation. A cyber-operations officer underscored that "commanders must preserve a decision space [during military operations] autonomy without friction, reduce our ability to pause escalation."[34] A respondent from AITeC explained that systems were built with "purposeful friction [intentional delay] [authentication], embedding [algorithmic] verification checkpoints, even at the cost of slower kill chains."[35] Two academic researchers with defense-linked portfolios emphasized that this approach is a deliberate counter to India's speed-first model: "India calls machine speed superiority; we call it fragility."[36] Based on

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

the four interviews, no new categories emerged, underscoring strong convergence across military, technical, and academic respondents on latency as doctrine.

Cross-national comparison underscores the distinctiveness of this posture. The United States has long struggled with contradictions: Official doctrine demands "meaningful human control," yet drone operations during the Global War on Terrorism often bypassed layered oversight, producing civilian casualties in Pakistan, Afghanistan, Yemen, and Libya.[37] Our understanding of France and the UK's codification of HITL safeguards at the national level projects predictability in their AI doctrines.[38] Yet, India, by contrast, situates autonomy within battlefield trials without clear guardrails, projecting doctrinal ambiguity both regionally and domestically.[39] However, Pakistan's latency posture introduces a third model in the security concepts: delay is not backwardness but a strategic adaptation consistent with SRR, embedding restraint into system design to stabilize deterrence against adversarial acceleration.

The field evidence illustrates how this philosophy is put into practice. Engineers described simulation environments in which classifiers were stress-tested under uncertainty and volatility, with thresholds calibrated to require human override before lethal authorization. A policy adviser summarized this philosophy as "buying time against our own machines [predominantly autonomous decision making] as much as against India."[40] Another respondent from ISR presents it differently: "Delay is our doctrine to keep command in human hands when machines turn the matter to political or military crises." This emphasis on time as insulation resonates with accident-risk theory, which, as Sagan and Perrow do, highlights the role of organizational buffers in mitigating failures in tightly coupled systems.[41] In Pakistan's case, latency emerges as both technical architecture within the systems and strategic doctrine SOPs, a deliberate dual-layer of restraint that, under SRR, reframes human oversight not as inefficiency but as a survival-oriented insulation against machine-led escalation.

Embedded Organizational Restraint in the Absence of a National Doctrine

Pakistan's military AI governance is often misread as a doctrinal vacuum because no single national AI doctrine has been published, unlike those of the US, NATO alliance states, and China.[42] Interviews and documents indicate the opposite: Restraint is embedded organizationally and codified. A senior ISR commander put it plainly: "We are not doctrinally blind; each command runs its own control logic [either to do or not to do] and no system moves [in the volatile environment] without a human signature."[43] An expert from AITeC described the engineering philosophy as "purposeful friction," latency, validation checks, and abort authority hard-wired into the algorithmic stack: "Our doctrine lives in the fail-safes, not on paper."[44] An academic partner with large defense-AI and policing portfolios reinforced the point: "Classifier thresholds and geofenced rulesets are tuned to the operating environment; the code [algorithms themselves] is our doctrine in practice."[45] By the seventh interview, saturation of this theme was reached; subsequent respondents confirmed convergence around HITL oversight, calibrated autonomy ceilings, and escalation latency as common denominators across units.

Operational evidence during the early 2025 confrontation of India and Pakistan further demonstrates this embedded logic. Multiple interviewees converged on the same sequence: India initiated an overt strike with Israeli-designed, next-generation drones; Pakistan withheld immediate retaliation while latency protocols gated the kill-chain; when thresholds were crossed, counter-systems engaged and downed more than seventy drones.[46] A policy adviser stressed: "Buying time [to clearly understand the operational pace] against our own machines as much as against [those of India]."[47] The lesson drawn from the field is not that paper doctrine is irrelevant, but that escalation brakes must exist where friction matters in the machine and at the edge. This approach aligns with Pakistan's UN submissions advocating MHC and with the MoD's reports, which emphasize ISR and C2 integration rather than automated strike delegation.[48]

Comparative cases show how Pakistan's embedded restraint diverges from other doctrinal models. The United States proclaims "responsible AI" but remains ambiguous across various theaters, bypassing layered oversight, demonstrating the fragility of declaratory doctrine. Furthermore, in Israel's context, backed by US and European patrons, which fields AI-enabled targeting systems such as Habsora in Gaza with minimal transparency, relying on political cover to absorb

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

reputational cost,[49] an option unavailable to Pakistan due to power distribution imbalances within the realism framework. China represents the opposite end: a centralized, top-down doctrine of "intelligentized warfare," demonstrating how great powers integrate AI as a state-led modernization project.[50]

Russia, though a major power, has operated closer to Pakistan's logic window, improvising AI integration under sanctions in Ukraine without a coherent doctrine, exposing the risks of fragmented practice. Ukraine itself offers another instructive parallel: Doctrine-free but adaptive, it deploys AI-enabled ISR and drones through decentralized, improvisational integration that achieves functional coherence without a unifying national strategy.[51] Finally, South Korea and Japan illustrate yet another pathway: Codified restraint embedded in alliance frameworks, where doctrines serve alliance credibility and ethical signaling rather than immediate escalation control, which, to our understanding, compromises national sovereignty by having states follow others without considering on-the-ground geopolitical realities.[52]

In a nutshell, Pakistan's "doctrine-in-code" is not an anomaly or weakness; it is a context-rational design that minimizes misclassification risk where it occurs, keeps costs aligned with means, and sustains operational stability in a nuclearized rivalry. Whereas great powers such as the US, China, and Russia often rely on declaratory doctrines to signal norms, and alliance states codify restraint for legitimacy, Pakistan internalizes restraint into machine architectures and unit practices because it lacks the margin of error that larger states enjoy. As an air-intelligence planner concluded: "A single, well-versed doctrine cannot manage border misreads; local control logic can."[53] The challenge ahead, flagged by several respondents, is scalability. If autonomy migrates into strategic-level systems, a thin national meta-doctrine may be needed to harmonize brakes without smothering local responsiveness. Until then, Pakistan's embedded organizational restraint, demonstrated in the most recent military confrontation on the Line of Control and other bordering areas, shows that responsible military AI integration can be engineered without written or published doctrines through a distributed architecture of friction, oversight, and adaptive thresholds.

Normative Signaling and Global Engagement

A recurring theme emerged from the analysis of interviews: Pakistan's AI restraint does not end at the level of engineering or organizational practice; it is projected outward as part of its international diplomatic posture. Unlike states that rely on centralized doctrines or accelerationist trajectories, Pakistan has sought to shape the global conversation on autonomous weapons through persistent engagement at multilateral forums. This outward signaling is not incidental. It stems from institutional memory of the Global War on Terrorism, when algorithmic misclassification in the tribal belt, where carrying a gun is a tradition and considered an honor, produced both civilian harm and reputational damage.[54] As one civilian adviser in AI governance observed, "We can't afford to be seen as the next state to outsource death to software. We've lived that on the receiving end."[55] An expert representing Pakistan on various debate platforms and who participated in UN consultations echoed this logic: "Restraint is not just a doctrine, it's reputational defense."[56]

Since 2018, Pakistan has used the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems to advocate for a binding prohibition on fully autonomous weapons, stressing their incompatibility with international humanitarian law and principles of humanity. This global advocacy is mirrored, though not codified, in practice.[57] As one of the national AI policy advisers explained, "Our AI is not lawless, it's designed to pass legal tests by default." A former diplomat sharpened the distinction: "We argue at international forums for IHL, but at home we do not write [standard operating procedures], and our scientists code restraint into the systems themselves: Delay, cross-checks, and commander approval before release."[58]

Comparative evidence underscores why this signaling matters. The United States advances principles of "responsible AI," yet has absorbed no systemic sanction costs for misclassifications in Afghanistan or Iraq. Likewise, historically, Israel, backed diplomatically by the US and European partners, can deploy autonomous targeting with limited international pushback.[59] By contrast, Pakistan's nuclearization in the 1990s immediately invited sanctions and diplomatic isolation.[60] When reminded of these sanctions, former Brigadier said, "If an American drone misclassifies, it's a tragedy. If ours [Pakistani] does, it's a scandal that invites punishment. That difference defines our pace." He further added, "India builds for offense [under impunity of Superpower]; we

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

argue for restraint, because our legitimacy demands it."[61] It demonstrates how middle powers incur disproportionate penalties for transgressing international norms.

From the perspective of the proposed theoretical framework, Pakistan's global signaling is a functional extension of its survival logic. In an environment where machine error can escalate as quickly as adversarial intent, restraint is internationalized to pre-empt punitive isolation and preserve legitimacy. Normative entrepreneurship thus becomes a strategic shield: by embedding the language of MHC and IHL into its diplomatic engagement, Pakistan not only differentiates itself from India but also turns structural vulnerability into normative leverage.

Strategic Risk and the Necessity of Contextualized AI Training

Pressing themes that emerged from interviewees' interpretations highlighted that Pakistan's concerns extend beyond India's military intentions to the inherent fragility of algorithms themselves. Participants repeatedly underscored that algorithmic lagging, model drift, classifier degradation, and data drift pose as much of a threat to escalation control as adversarial action. In a culturally and ethnically complex battlespace such as Pakistan's tribal belts or urban peripheries, even small deviations in classifier reliability can produce catastrophic consequences. As one systems scientist cautioned, "You don't just fight India's machines [drones, autonomous systems], you fight your own models when they start drifting [either model drifting or model degradation] from on-ground reality."[62] Another senior former planner emphasized, "Concept drift in our geography isn't hypothetical [pointed to incidents such as the Damadola and Salala check post]. Behavior here shifts daily, and any AI that isn't localized will mistake a ritual for a threat."[63] These insights frame Pakistan's doctrinal emphasis on training fidelity: restraint is not only geopolitical but technical, aimed at insulating its AI posture against machine fragility.

Institutional documents such as the Ministry of Defence Production's Year Book 2021–2022 highlight cautious, stepwise integration of AI into ISR and command systems, with explicit avoidance of rapid delegation to autonomous strike functions and an acknowledgement

that reliability thresholds remain unproven in Pakistan's operating environment.[64] However, India's DRDO Procurement Manual 2025 demonstrates rapid prototyping and fast-track induction cycles, reflecting New Delhi's preference for speed and visible battlefield deployments. Carnegie report on India's AI Strategy describes this model as privileging capability signaling over risk management.[65] Pakistani interviewees repeatedly contrasted the two approaches: India's intention to deter China and Pakistan, and Pakistan's approach of neutralizing threats rather than escalating.

This divergence reflects broader lessons from global experience. During the War on Terror, US drone operations in Pakistan and Afghanistan repeatedly misclassified civilian convoys and gatherings targeting women, children, and elderly tribal men, demonstrating how even advanced sensors can wrongly engage targets.[66] Today, the use of drones and autonomous systems has expanded significantly across global conflict zones, including Myanmar, the Asia-Pacific, US military operations in the Red Sea, the Australian Army, Ukraine's covert drone strikes deep inside Russia, Russia's extensive drone use in Ukraine, and Singapore's[67] deployment of automated rifles and robotic defense technologies, repeating the same risks during the simulations and battle ground. However, historical blunders in US cases inform Pakistan's conviction that contextual training is not a luxury but a strategic necessity. As one AI reliability engineer explained, "Our models are built to ask more questions before acting [tuned under worst case scenario] [culturally refined parameters]. That's not inefficiency, it's survival."[68] Classifier calibration in Pakistan now incorporates region-specific ISR mapping, dialectic and behavioral tagging, mobility pattern recognition, and adversarial spoofing simulations, embedding escalation control directly into the training pipeline.

Comparative cases reinforce this logic with serious concerns. Israel has used AI-enabled drone swarms in Gaza with limited oversight, prioritizing tactical gains while intensifying risks to civilians.[69] Yet international accountability has been lacking, diplomatically shielded by US and European backing for a long time. Russia's targeting systems in Ukraine have likewise struggled with urban complexity, often leading to indiscriminate strikes. NATO's attempts to pool multinational datasets for AI-enabled decision support in Ukraine illustrate the alternative problem: context mismatch across operational theaters.[70]

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

China, meanwhile, has invested heavily in ethnically tuned surveillance AI in Xinjiang, an authoritarian approach that prioritizes control but offers little applicability in contested, high-friction battlespaces.[71] Against this global backdrop, Pakistan's decision to slow down and localize its training regime represents a unique doctrinal path: an attempt to mitigate algorithmic error in an environment where even minor misfires could have strategic consequences over the long term.

From the perspective of SRR, contextualized training demonstrates how restraint operates as an intentional design principle within asymmetric nuclear rivalry. SRR argues that in high-stakes environments, escalation risk emerges not only from adversarial intent but from systemic fragility embedded in technical architectures. A misclassified civilian convoy, a cultural gathering mistaken for a militant assembly, or spoofed signals wrongly identified as hostile acts are not simply technical slips; they are strategic triggers with the potential to escalate crises at machine speed. By treating training datasets as strategic infrastructure, Pakistan reframes rules as doctrine, building bounded autonomy systems that require human verification before committing force, thereby aligning operational survival with strategic restraint.

Interview evidence reinforces this framework orientation. A defense data scientist explained, "…if we lack data, we create contexts for the model to learn resilience. Sit-ins [political and religious] and surveillance networks [smart city initiative] become our training grounds."[72] A systems integrator emphasized the permanent challenge of drift: "Even our best models [pointing toward generations of Shahpar and its predecessors] are learning in a moving battlefield. That means retraining is not optional; it is SOPs."[73]

In this sense, Pakistan's approach illustrates the essence of SRR: Restraint is not an accidental approach that pretends to be a state's weakness, but a deliberate act of engineering survival into technical and doctrinal architectures. Strategic latency here is not passive delay but engineered prudence: embedded in decision loops, architectures, and, most critically, the training pipeline itself, where localized multivariate data is treated as the foundation for escalation control. Here, context is not merely background to AI; it is doctrine, and restraint is survival.

Implications for Theory, Policy, and Global AI Governance

This study has implications that extend beyond the Pakistan case, reshaping theoretical debates, domestic policy design, and the global governance of AI in military domains.

Theoretical Implications

By advancing defensive realism with SRR, this study contributes to international relations theory by demonstrating that restraint is not only a product of weakness or incapacity but also an intentional strategic design. Unlike classical realism, which interprets instability through adversarial ambition and material competition, SRR shows that escalation risks are often embedded in misclassified systemic fragility, drift, and machine opacity, and that states can strategically embed restraint in response. Unlike technological determinism, which frames systems as neutral, SRR emphasizes that restraint itself can be engineered into the code, datasets, and oversight structures. Pakistan illustrates how restraint can be institutionalized without a single national doctrine, creating a coherent security posture through distributed organizational practices. Theoretically, this reframes restraint from a reactive stance to an active form of agency that middle powers can exercise in asymmetric rivalries.

Policy Implications

For Pakistan, three SRR-aligned policy pathways emerge. First, doctrinal cohesion requires thin but binding harmonization across service branches to ensure distributed brakes remain consistent under crisis conditions without eliminating local flexibility. Second, multivariate, localized datasets must be treated as strategic assets integral to classifier reliability in ethnically complex and politically volatile environments. Third, normative entrepreneurship should remain central, as Pakistan's advocacy for MHC- and IHL-aligned coding serves as a reputational defense. In a system where middle powers face sanctions for errors that great powers tolerate, restraint is both a survival strategy and a shield for legitimacy.

Regional Implications

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

For South Asia, SRR sharpens our reading of the Indo-Pakistani rivalry. India's AI posture, linked to Cold Start and rapid battlefield automation, signals escalation through capability-first deployment. Pakistan's SRR-based latency and restraint posture serves as a stabilizer, but risks being misinterpreted as weakness if not paired with clear signaling. The implication is that AI-related confidence-building measures (CBMs), such as transparency about testing environments, latency thresholds, and escalation brakes, are urgently needed, mirroring nuclear CBMs that once helped reduce misperceptions in the region. Without such measures, India's accelerationism and Pakistan's restraint will remain locked in a destabilizing perceptual asymmetry.

Global Implications

At the international level, the findings reveal a hierarchy of accountability in AI militarization. Great powers like the US absorb reputational shocks from AI error, while Israel's actions in Gaza illustrate how client states benefit from great-power cover. By contrast, middle powers such as Pakistan risk punitive sanctions or isolation for equivalent missteps, repeating the asymmetry of the nuclear era. Pakistan's advocacy at the UN GGE on LAWS reflects an attempt to externalize internal restraint into universal norms, demonstrating how SRR can function as a bridge between domestic prudence and international governance. The implication for global AI governance is clear: Restraint must be evaluated not only by published doctrines but also by embedded practices, training fidelity, latency architectures, and veto mechanisms that reflect real operational safeguards.

Implications for Future Research

This study suggests a broader research agenda. First, comparative work should test whether other middle powers (Turkey, South Korea, Iran, and Singapore) adopt restraint as system-level design rather than doctrinal codification. Second, SRR should be examined in different dyadic contexts (Turkey-Greece, Israel-Iran, China-Taiwan) to assess its explanatory reach. Third, future inquiry should foreground training environments as strategic infrastructures and an underexplored variable linking technical fragility to geopolitical escalation. In doing so, SRR offers not only a framework for South Asia but also a lens to theorize how states at the periphery of great-power competition manage survival in the machine age.

Conclusion

The debate over military AI is dominated by techno-optimism and great-power narratives. Yet, Pakistan's experience exposes a deeper fault line: The international system unevenly distributes the costs of machine error. Great powers can absorb or obscure misfires under the banner of innovation, while middle powers such as Pakistan operate under a punitive gaze where restraint is survival, not luxury. This asymmetry corrodes both deterrence and governance, producing a world in which the least reckless actors are the most vulnerable to sanction, while the most reckless enjoy insulation through patronage and power. SRR reveals that restraint here is not a by-product of incapacity, but a doctrinal choice rooted in defensive realist logic: survival in a nuclearized rivalry demands friction, delay, and localized control. Latency, bounded autonomy, and context-specific training are not inefficiencies but engineered safeguards against the compression of political oversight. In Pakistan's case, restraint is not external rhetoric imposed by humanitarian law; it is an internalized survival strategy encoded in systems, organizations, and decision loops.

The danger lies in misinterpretation. India's accelerationist trajectory, which valorizes machine speed and capability-first demonstrations, risks being read as an offense regardless of its intent, thereby compressing verification windows and rendering escalation nearly automatic. If restraint continues to be mistaken for weakness, while speed remains celebrated as strength, the dyad will not stabilize; it will deteriorate into a cycle in which transparency is penalized and opacity rewarded. Globally, the lesson is clear: AI governance cannot be confined to ethical principles or technical standards. It must confront the political economy of risk, who is held accountable for failure, who escapes sanction, and who bears the asymmetric burden of restraint. Unless governance frameworks correct these inequities, middle powers will face incentives to conceal rather than codify restraint, undermining both transparency and stability.

Finally, SRR exposes the paradox of the machine age: Survival may depend less on the pursuit of speed than on the refusal to automate. To ignore this is to repeat history's most dangerous misjudgment, mistaking restraint for weakness and equating acceleration with

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

security. That path, as both nuclear history and Pakistan's experience warn, leads not to stability but to catastrophe.

Endnotes

[1] Surinder Mohan, "Between the Horns of a Dilemma: India, Pakistan, and Conflict Dynamics in South Asia," *World Affairs* 188, no. 1 (January 2025), https://doi.org/10.1002/waf2.12065.; Mehmood Hussain and Syed Inam Ali Naqvi, "Indo-Pakistan Rivalry and Integrated Ring Balancing: Prospects and Challenges to Regional Stability in South Asia," *Asian Journal of Political Science* 33, no. 1 (2024): 1–18, https://doi.org/10.1080/02185377.2024.2386663.
[2] Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018).; Elsa B. Kania, "Artificial Intelligence in China's Revolution in Military Affairs," in *Routledge Handbook on China's Security* (London: Routledge, 2022), 65–92, https://doi.org/10.4324/9781003268215-4.; Jeffrey Ding, "Machine Failing: How Systems Acquisition and Software Development Flaws Contribute to Military Accidents," *Texas National Security Review* (Winter 2024/2025).
[3] Anirudh Suri, "The Missing Pieces in India's AI Puzzle: Talent, Data, and R&D," Carnegie Endowment for International Peace, 2025.
[4] Ministry of Defence Production (MoDP), "Ministry of Defence Production Government of Pakistan," February 24, 2024.; D. S. Hooda, "Implementing Artificial Intelligence in the Indian Military," Delhi Policy Group, February 2023.
[5] Zohaib Altaf and Nimrah Javed, "The Militarization of AI in South Asia," *South Asian Voices*, January 17, 2024.
[6] Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton: Princeton University Press, 2010).
[7] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214.
[8] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214.; Paul Kapur, "Stability-Instability Paradox," in *The SAGE Encyclopedia of Political Behavior* (Thousand Oaks: SAGE, 2017), https://doi.org/10.4135/9781483391144.n364.
[9] Eleri Lillemäe, Kairi Talves, and Wolfgang Wagner, "Public Perception of Military AI in the Context of Techno-Optimistic Society," *AI & Society* 40 (2023), https://doi.org/10.1007/s00146-023-01785-z.; LM Guedes Gonçalves Costa, "'We Have Ethical, Legal and Security Concerns': An Analysis of Pakistan's Foreign Policy on Lethal Autonomous Weapon Systems" (2024).
[10] William E. Scheuerman, "Realism and the Critique of Technology," *Cambridge Review of International Affairs* 22, no. 4 (December 2009): 563–84, https://doi.org/10.1080/09557570903325504.; Grégoire Chamayou, *A Theory of the Drone* (New York: New Press, 2015).; Laura Bruun and Alexander Blanchard, "SIPRI Background Paper: Bias in Military Artificial Intelligence" (Stockholm: SIPRI, 2024).
[11] Inderjit Panjrath, "Pakistan's Tactical Nuclear Weapons: Giving the Devil More than His Due?" (New Delhi: Vij Books, 2018).; United Nations, "UN Secretary General's Disarmament Agenda," UNIDIR, 2018, https://app.unidir.org/node/5663.
[12] Arslan Munir, Alexander Aved, and Erik Blasch, "Situational Awareness: Techniques, Challenges, and Prospects," *AI* 3, no. 1 (March 2022): 55–77, https://doi.org/10.3390/ai3010005.
[13] Tayyaba Khurshid, "The Impact of Artificial Intelligence Militarization on South Asian Deterrence Dynamics," *BTTN Journal* 2, no. 2 (December 2023): 130–44, https://doi.org/10.61732/bj.v2i2.76.; Sardor Boratov, "AI, Autonomy, and the New

Security Dilemma: Deterrence, Escalation, and Strategic Ambiguity in the Algorithmic Age" (University of Warsaw, 2025), https://doi.org/10.2139/ssrn.5452734.
[14] Lillemäe, Talves, and Wagner, "Public Perception of Military AI."; Michele Giovanardi, "AI for Peace: Mitigating the Risks and Enhancing Opportunities," *Data & Policy* 6 (2024), https://doi.org/10.1017/dap.2024.37.
[15] Human Rights Watch, "World Report 2019: Rights Trends in Afghanistan," January 17, 2019.
[16] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214.
[17] Boratov, "AI, Autonomy, and the New Security Dilemma."
[18] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton: Princeton University Press, 1984); Scott Douglas Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton: Princeton University Press, 1993).
[19] Ding, "Machine Failing."
[20] Daniel Mügge, "EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?" *Journal of European Public Policy* 31, no. 8 (2024): 1–26, https://doi.org/10.1080/13501763.2024.2318475; U.S. Department of Defense, "Responsible Artificial Intelligence Strategy and Implementation Pathway" (Washington, DC: DOD, 2022), https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF.
[21] Paul R. Williams and Ryan Jane Westlake, "A Taste of Armageddon: Legal Considerations for Lethal Autonomous Weapons Systems," *Case Western Reserve Journal of International Law* (2025).
[22] Mariangel Pacheco Troisi, Mónica García-Melón, and Fernando Jiménez-Sáez, "Anticipatory Evaluation: How to Incorporate an Anticipatory Technique into a Theory-Driven Evaluation Process," *Evaluation and Program Planning* 108 (February 2025): 102509, https://doi.org/10.1016/j.evalprogplan.2024.102509.
[23] Virginia Braun and Victoria Clarke, "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology* 3, no. 2 (2006): 77–101.
[24] Nachiket Midha, "'From Attock to Cuttack and from Kashmir to Kanyakumari:' Understanding Akhand Bharat in Terms of Ontological Security," *The Columbia Journal of Asia* 2, no. 1 (May 2023): 15–24, https://doi.org/10.52214/cja.v2i1.11113.; Najm Ullah, Muhammad Zohaib, Ziaul Islam, and Sikandar Bakht, "Geopolitical Implications of the US-India Strategic Partnership in the Indo-Pacific Region," *Social Science Review Archives* 2, no. 2 (November 2024): 814–8730, https://doi.org/10.70670/sra.v2i2.128.
[25] "Indian Army Demonstrates Swarm of Drones," Indian Defence Industries, 2021, https://indiandefenceindustries.in/indian-army-swarm-of-drones.; Rueben Dass and Abdul Basit, "Drone Warfare Is Redefining India-Pakistan Rivalry," *The Diplomat*, June 4, 2025, https://thediplomat.com/2025/06/drone-warfare-is-redefining-india-pakistan-rivalry/.
[26] Author interview with ISR commander, Islamabad, May 10, 2025.
[27] Author interview with serving Brigadier, Rawalpindi, May 10, 2025.
[28] Author interview with AITeC official, Islamabad, May 11, 2025.
[29] Author interview with academic official, January 11, 2024.
[30] Paul Butkus, "Questioning the U.S. CIA Drone Program as a Counter-Terrorism Strategy in FATA, Pakistan between 2004 and 2018" (PhD diss., January 2020), https://www.proquest.com/docview/2378903896.
[31] Author interview with former Brigadier, Islamabad, January 18, 2024.
[32] Hooda, "Implementing Artificial Intelligence in the Indian Military."

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

[33] DRDO, "DRDO Procurement Manual 2025" (New Delhi: Defense Research and Development Organization, June 25, 2025).
[34] Author interview with cybersecurity official, Islamabad, November 7, 2023.
[35] Author interview with AITeC official, Islamabad, May 11, 2025.
[36] Author interview with QAU academicians, Islamabad, November 7, 2023.
[37] Aqil Shah, "Do U.S. Drone Strikes Cause Blowback? Evidence from Pakistan and Beyond," *International Security* 42, no. 4 (May 2018): 47–84, https://doi.org/10.1162/isec_a_00312.
[38] Mügge, "EU AI Sovereignty."
[39] DRDO, "DRDO Procurement Manual 2025."
[40] Author interview with national AI policy board member, Islamabad, December 18, 2023.
[41] Perrow, *Normal Accidents*; Sagan, *The Limits of Safety*.
[42] Mügge, "EU AI Sovereignty," 31, no. 8; U.S. Department of Defense, "Responsible Artificial Intelligence Strategy and Implementation Pathway"; Yatsuzuka Masaaki, "PLA's Intelligentized Warfare: The Politics on China's Military Strategy," NIDS Security Reports (2022), https://www.nids.mod.go.jp/english/publication/security/pdf/2022/01/05.pdf.
[43] Author interview with ISR official, Islamabad, May 10, 2025.
[44] Author interview with AITeC official, Islamabad, May 11, 2025.
[45] Author interview with cybersecurity official, Islamabad, November 7, 2023.
[46] Arvind Kumar and Hari Ram, "Operation Sindoor and the Rise of Drone-Centric Warfare: A Strategic Analysis of India's Technological Shift in Modern Combat Doctrine," *Zenodo* (July 2025), https://doi.org/10.5281/zenodo.16223932; Usman Haider, "The First India-Pakistan Drone War," *The Diplomat*, May 30, 2025, https://thediplomat.com/2025/05/the-first-india-pakistan-drone-war/.; Abdullah Khan, "How Pakistan's Tactical Deception and Electronic Warfare Crippled India's Air Strikes," Strafasia, September 2025, https://strafasia.com/how-pakistans-tactical-deception-and-electronic-warfare-crippled-indias-air-strikes/.
[47] Author interview with national AI policy board member, Islamabad, May 10, 2025.
[48] UNODA, "Submission of Views by Pakistan in Accordance with UNGA Resolution 79/239"; Ministry of Defence Production (MoDP), "Ministry of Defence Production Government of Pakistan," February 24, 2024.
[49] Shah, "Do U.S. Drone Strikes Cause Blowback?" 47–84; Frida Berrigan, "Made in the U.S.A.: American Military Aid to Israel," *Journal of Palestine Studies* 38, no. 3 (2009): 6–21, https://doi.org/10.1525/jps.2009.xxxviii.3.6; Noah Sylvia, "Israel's Targeting AI: How Capable Is It?" RUSI, February 8, 2024, https://www.rusi.org/explore-our-research/publications/commentary/israels-targeting-ai-how-capable-it.
[50] Josh Baughman, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," *SSRN Electronic Journal* (2024), https://doi.org/10.2139/ssrn.4828107.
[51] Baurzhan Rakhmetov and Kamila Murzagulova, "Artificial Intelligence in Warfare: The Case of the Russia-Ukraine War," *Journal of Strategic Security* 18, no. 4 (January 2025): 64–77, https://doi.org/10.5038/1944-0472.18.4.2470.
[52] Sunha Bae and So Jeong Kim, "AI Security Strategy and South Korea's Challenges," CSIS, 2025, https://www.csis.org/analysis/ai-security-strategy-and-south-koreas-challenges; James Schoff, "Coordination: Balancing Technonationalism with a Globalized World" (Washington, DC: Carnegie Endowment for International Peace, 2020), https://carnegie-production-assets.s3.amazonaws.com/static/files/Schoff_US-Japan.pdf.
[53] Author interview with ISR commander, Islamabad, February 12, 2024.

[54] Farooq Yousaf, "U.S. Drone Campaign in Pakistan's Pashtun 'Tribal' Region: Beginning of the End under President Trump?" *Small Wars & Insurgencies* 31, no. 4 (2020): 751–72, https://doi.org/10.1080/09592318.2020.1743490.
[55] Author interview with chairman, national AI program, Islamabad, January 18, 2024.
[56] Author interview with Pakistan representative to UN, Lahore, February 19, 2024.
[57] Pakistan, "General Statement by Pakistan at the Meeting of Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS)," United Nations, Geneva.
[58] Author interview with AITeC official, Islamabad, May 11, 2025; author interview with Pakistan representative to UN, Lahore, February 19, 2024.
[59] Shah, "Do U.S. Drone Strikes Cause Blowback?" 47–84; Berrigan, "Made in the U.S.A.," 6–21.
[60] S. Krishnan, "US Sanctions on Pakistan and Their Failure as Strategic Deterrent," *World Affairs: The Journal of International Issues* 27, no. 3 (2023): 78–95, https://doi.org/10.2307/48761480.
[61] Author interview with former Brigadier, Islamabad, January 18, 2024.
[62] Author interview with academic system trainer, Islamabad, November 7, 2023.
[63] Author interview with former Brigadier, Islamabad, January 18, 2025.
[64] Ministry of Defence Production (MoDP), "Ministry of Defence Production Government of Pakistan," February 24, 2024.
[65] DRDO, "DRDO Procurement Manual 2025"; Suri, "The Missing Pieces in India's AI Puzzle."
[66] Chris Woods, "Leaked Pakistani Report Confirms High Civilian Death Toll in CIA Drone Strikes," *The Bureau of Investigative Journalism*, July 22, 2013, https://www.thebureauinvestigates.com/stories/2013-07-22/leaked-pakistani-report-confirms-high-civilian-death-toll-in-cia-drone-strikes.
[67] Janes, "Myanmar Military Adapts FLIR Systems for Expanding Drone War," February 24, 2025, https://www.janes.com/osint-insights/defence-and-national-security-analysis/myanmar-military-adapts-flir-systems-for-expanding-drone-war; Janes, "Shifting Geopolitics Impacts Asia-Pacific Defence Spending," April 22, 2025, https://www.janes.com/osint-insights/defence-and-national-security-analysis/feature-shifting-geopolitics-impacts-asia-pacific-defence-spending.; Janes, "US Carrier Strike Group Provided More than Presence and Posture in Red Sea Operations," July 2, 2024, https://www.janes.com/osint-insights/defence-and-national-security-analysis/feature-us-carrier-strike-group-provided-more-than-presence-and-posture-in-red-sea-operations.; Janes, "Australian Army Applies AI in Unmanned Systems Tests," June 19, 2024, https://www.janes.com/osint-insights/defence-and-national-security-analysis/special-report-australian-army-applies-ai-in-unmanned-systems-tests; Janes, "Operation Spiderweb: Ukraine Covert Drone Strike inside Russia," June 12, 2025, https://www.janes.com/osint-insights/defence-and-national-security-analysis/operation-spiderweb-ukraine-covert-drone-strike-inside-russia.; Janes, "Singapore Gets to Grips with New Automatic Rifle," August 16, 2024, https://www.janes.com/osint-insights/defence-and-national-security-analysis/singapore-gets-to-grips-with-new-automatic-rifle.
[68] Author interview with QAU academician, Islamabad, November 7, 2023.
[69] Nadia Hardman, "'Hopeless, Starving, and Besieged': Israel's Forced Displacement of Palestinians in Gaza," Human Rights Watch, November 14, 2024, https://www.hrw.org/report/2024/11/14/hopeless-starving-and-besieged/israels-forced-displacement-palestinians-gaza.
[70] Muhammad Alfian Maulana, "Comparative Analysis of Western Nations' Actions in Russia-Ukraine and Israel-Palestine Conflicts," *Nation State* 7, no. 1 (June 2024): 29–52, https://doi.org/10.24076/nsjis.v7i1.1558.

https://digitalcommons.usf.edu/jss/vol19/iss2/2
DOI: https://doi.org/10.5038/1944-0472.19.2.2527

[71] Human Rights Watch, "China's Algorithms of Repression: Reverse Engineering Xinjiang Police Mass Surveillance," May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.
[72] Author interview with AITeC official, Islamabad, May 11, 2025.
[73] Author interview with Air University academician, Islamabad, November 11, 2023.