Sociology & Cultural Research Review (SCRR)
Available Online: https://scrrjournal.com
Print ISSN: 3007-3103 Online ISSN: 3007-3111
Platform & Workflow by: Open Journal Systems

Geopolitical Risks of Emerging Technologies: A Study on AI, Cyber Warfare, and State Security in Pakistan

Kashif Ali Mahesar
Assistant Professor, Benazir Bhutto Shaheed University Karachi
mahesarkashifali@gmail.com
Fida Hussain Mahesar
Assistant Professor, Pakistan Studies at SNAK Superior Science College, Khairpur Mir's
fidam1200@gmil.com

ABSTRACT
The rapid integration of artificial intelligence (AI) and cyber warfare capabilities has emerged as a pivotal geopolitical risk, profoundly reshaping deterrence, escalation pathways, and strategic stability in an era of techno-geopolitical competition. This study focuses on Pakistan, a developing nuclear-armed state navigating intense rivalry with India, instability on its western border, and entrapment in U.S. and China technological contestation. Despite the launch of its National Artificial Intelligence Policy 2025, Pakistan exhibits only modest offensive cyber potential and significant defensive deficiencies, compounded by heavy dependence on Chinese technology transfers through the Digital Silk Road and restricted Western cooperation. In contrast, India's accelerated militarization of AI encompassing advanced intelligence, surveillance, reconnaissance (ISR), autonomous systems, swarm technologies, and offensive cyber operations has dramatically widened the bilateral asymmetry, as vividly illustrated by the 2025 Indo-Pak crisis featuring over 1.5 million cyberattacks, AI-generated deepfakes, and disruptions to dual-use command-and-control infrastructure. Employing a synthesis of realism, offensive realism, and an adapted strategic stability framework enriched by entanglement theory, the analysis demonstrates how conventional cyber and AI operations now carry direct nuclear implications in South Asia's compressed decision space. Attacks on shared C4ISR networks risk being misinterpreted as preemptive nuclear strikes, incentivizing dangerous pre-delegation and compressing crisis response timelines. The proposed Techno-Geopolitical Vulnerability Matrix locates Pakistan in a high-vulnerability quadrant defined by acute technological asymmetry and institutional fragmentation. Absent urgent reforms including a unified national AI and cyber authority, doctrinal clarification of digital red lines, indigenous talent development, and bilateral confidence-building measures with India, Pakistan faces progressive erosion of minimum credible deterrence. The findings extend broader lessons for developing nuclear powers: without deliberate institutional resilience and normative restraint mechanisms, emerging technologies shift risk from deliberate aggression to inadvertent escalation driven by misperception and systemic entanglement.

Keywords: *Geopolitical Risk, Artificial Intelligence, Cyber Warfare, Strategic Stability, Nuclear Entanglement, Pakistan Security.*

Introduction

The advent of emerging technologies, including artificial intelligence (AI), cyber capabilities, quantum computing, and biotechnology, has fundamentally redefined the contours of global power in the 21st century. These technologies are no longer mere enablers of economic growth but constitute new domains of strategic competition, where dominance translates into geopolitical leverage and military superiority. As noted in the OECD Science, Technology

and Innovation Outlook 2025, rising geopolitical tensions have prompted governments to align science, technology, and innovation policies with national security imperatives, resulting in a sharp increase in research security measures from 25 policies in 2018 to over 250 in 2025 (OECD, 2025). This securitization reflects a broader shift from traditional kinetic warfare to techno-geopolitical rivalries, where AI-driven autonomous systems, quantum-encrypted communications, and cyber offensive tools amplify escalation risks and erode conventional deterrence paradigms. The World Economic Forum's Global Cybersecurity Outlook 2025 further underscores this transformation, highlighting how geopolitical frictions have influenced cybersecurity strategies for nearly 60% of organizations, with generative AI exacerbating vulnerabilities through sophisticated phishing and deepfake operations (World Economic Forum, 2025). In this context, emerging technologies function as force multipliers, enabling states to achieve information superiority, disrupt adversary command-and-control networks, and project power asymmetrically without direct confrontation.

This evolution marks a profound departure from the post-Cold War emphasis on traditional military balances centered on troop numbers, nuclear arsenals, and conventional hardware to a hybrid landscape of techno-geopolitical competition. Great-power rivalries, particularly between the United States and China, have accelerated this transition, with Beijing investing an estimated $900 billion in AI, quantum, and biotechnology over the past decade, far outpacing Western counterparts (Council on Foreign Relations, 2025). Such investments foster technological blocs, fragmenting global standards and intensifying export controls, as evidenced by the EU's AI Act and U.S. restrictions on semiconductor transfers. The KPMG Top Geopolitical Risks 2025 report warns that this competition in AI and related fields risks creating bifurcated ecosystems, jeopardizing international cooperation and heightening cyber warfare threats (KPMG International, 2025). In parallel, non-state actors and hacktivist groups leverage accessible AI tools for disruption, blurring lines between statecraft and subversion. This shift not only reconfigures alliances but also introduces entanglement risks, where cyber intrusions into dual-use systems could cascade into nuclear miscalculations, as explored in RAND analyses of Indo-Pacific information warfare (Hanson et al., 2024).

Pakistan occupies a uniquely precarious position within this volatile security environment, shaped by enduring India-Pakistan rivalry, the overarching China-U.S. great-power contest, Afghan border instability, and its status as a nuclear-armed state. The May 2025 Indo-Pak crisis, triggered by the Pahalgam terrorist attack and culminating in India's Operation Sindoor, exemplified how conventional flashpoints rapidly spill into cyber domains, with over 1.5 million attributed cyberattacks exchanged, including DDoS assaults and malware deployments like Crimson RAT by Pakistan-linked APT36 (Stimson Center, 2025a; NSFOCUS, 2025). India's accelerating AI militarization evidenced by allocations exceeding $11 million for AI projects in the 2025-26 defense budget and deployments of AI-enhanced surveillance during the crisis widens the asymmetry, threatening Pakistan's deterrence stability (Newsweek, 2025; The Diplomat, 2025). Simultaneously, Pakistan's alignment with China via CPEC digital initiatives exposes it to U.S. sanctions while providing limited technology transfers, complicating strategic autonomy amid Afghan spillover threats and internal hybrid warfare risks (Valdai Club, 2025).

Compounding these vulnerabilities is Pakistan's growing dependence on digital infrastructure and nascent AI/cyber capabilities, rendering it acutely susceptible to disruption. The approval of the National Artificial Intelligence Policy 2025, with its six-pillar framework emphasizing innovation funds, sectoral roadmaps, and international partnerships, signals ambition but highlights institutional lags, including delayed establishment of a national CERT until 2024 and

heavy reliance on foreign technologies (Ministry of Information Technology & Telecommunication, 2025; Stimson Center, 2025b). As Pakistan's internet penetration surges toward 100 million users, cyber fraud already erodes 4.6% of GDP, while unattributed intrusions during 2025 crises underscore defensive gaps (Strafasia, 2025). This digital entanglement risks amplifying escalation pathways, particularly in a nuclear dyad where AI-enabled perception management or cyber strikes on C4ISR systems could trigger unintended retaliation.

This study addresses a critical research gap: while global literature abounds on AI/cyber geopolitics in advanced powers, integrated assessments for developing nuclear states like Pakistan remain sparse and policy-oriented rather than analytically rigorous. Existing works often frame Pakistan's challenges through bilateral lenses or great-power proxies, overlooking the confluence of AI-driven hybrid threats with South Asian strategic instability (Ghani, 2025; Stimson Center, 2024). By synthesizing realism's security dilemma with entanglement theory, this analysis elucidates how emerging technologies exacerbate Pakistan's techno-geopolitical vulnerability, offering pathways for doctrinal and institutional resilience in an era of unrelenting competition.

Literature Review

The digital age has redefined geopolitical risk through non-kinetic channels, where emerging technologies intensify power asymmetries and vulnerabilities among states (World Economic Forum, 2025a). Geopolitical tensions manifest via fragmented digital ecosystems, supply-chain disruptions, and AI-fueled influence operations, with cyber espionage and regulatory fragmentation creating technology blocs that undermine sovereignty (KPMG International, 2025). States now face remote infrastructure sabotage and generative AI-driven perceptual manipulation, blurring attribution and escalation thresholds (Riskonnect, 2025). Reports indicate geopolitical frictions shape cybersecurity strategies for nearly 60% of organizations, while one-third of CEOs prioritize cyber espionage amid conflicts (World Economic Forum, 2025b). This environment transcends bilateral disputes, generating systemic instabilities from interdependent networks and agentic AI systems. For middle powers, dual vulnerabilities emerge adversary offensive exploitation and internal defensive shortcomings intensifying security dilemmas where digital entanglement risks cascading into kinetic crises (Help Net Security, 2025).

Artificial intelligence functions as a profound geopolitical multiplier, delivering decision superiority in military applications and enabling autonomous weapons that reshape escalation dominance (European Parliamentary Research Service, 2025). AI integration into intelligence, surveillance, reconnaissance, and lethal autonomous systems enables asymmetric force projection, with military AI investments surging amid great-power rivalries (GlobeNewswire, 2025). Doctrinal evolutions highlight AI's operational edge in real-time threat detection, swarm coordination, and predictive targeting across U.S., Chinese, and Russian programs. Yet autonomous platforms and AI-enhanced command systems reduce human latency while introducing entanglement risks, as cyber intrusions into dual-use AI may mis-signal nuclear intent (Center for a New American Security, 2025). This multiplier accelerates arms racing, transforming warfare beyond augmentation and posing ethical challenges over human oversight in kill chains and restraint regime viability (Carnegie Endowment for International Peace, 2025a).

Cyber warfare now anchors hybrid doctrines, fusing with information operations, economic coercion, and kinetic actions to yield strategic effects below war thresholds (Center for Cyber Diplomacy and International Security, 2025). Modern doctrines stress persistent engagement,

forward defense, and nexus operations blending cyberattacks with disinformation for cognitive disruption (Ayesa, 2025). Russia's Ukraine hybrid tactics and NATO's cyberspace-as-warfighting-domain elevation exemplify this, with AI boosting precision in supply-chain compromises and autonomous malware (CyberPeace Institute, 2025). Hybrid frameworks leverage ambiguity for deniability via proxies and false flags, eroding deterrence through attrition while incorporating cross-domain retaliation that amplifies unintended escalation (Journal of Law & Cyber Warfare, 2025). State trajectories diverge: U.S. persistent engagement through Cyber Command; China's military-civil fusion for AI-cyber dominance; Russia's disruptive hybrids; India's AI-militarization amid asymmetries; Israel's offensive cyber-precision integration, entangling nuclear postures in South Asia (Microsoft, 2025; Foreign Affairs, 2025; Foundation for Defense of Democracies, 2025; RAND Corporation, 2025). In Pakistan, cyber security and AI adoption literature stays policy-focused, stressing institutional frameworks over geopolitical implications, with the National AI Policy 2025 prioritizing innovation funds, ethical governance, and cybersecurity amid implementation delays (Ministry of Information Technology & Telecommunication, Pakistan, 2025; Startup.pk, 2025). Studies emphasize digital transformation but rarely embed these in techno-geopolitical contests (Express Tribune, 2025a; Express Tribune, 2025b). A vital gap endures in holistic evaluations of AI-cyber risks for developing nuclear powers like Pakistan, where asymmetric lags intersect nuclear deterrence and great-power proxies this study bridges that by merging entanglement theory with South Asian dynamics (SIPRI, 2025; Stimson Center, 2025).

Problem Statement

Pakistan confronts acute geopolitical risks from the rapid integration of artificial intelligence and cyber warfare capabilities into an already volatile regional security environment. As a developing nuclear power with persistent adversarial relations with India, protracted instability along its western border, and deepening entanglement in U.S.-China technological rivalry, the country faces widening asymmetries in offensive and defensive digital capacities. The proliferation of AI-enabled autonomous systems, deepfake-driven information warfare, and cyber intrusions into dual-use command-and-control networks heightens the likelihood of miscalculation, unintended escalation, and erosion of strategic stability in South Asia. Pakistan’s growing digital dependence, coupled with institutional delays in building resilient cyber defenses and indigenous AI expertise, renders critical infrastructure, early-warning systems, and nuclear signaling channels increasingly vulnerable to preemptive disruption. Existing analyses remain largely siloed focusing either on technical policy frameworks or traditional deterrence leaving unaddressed the compounded threat of techno-geopolitical entanglement for resource-constrained nuclear states operating under credible conventional and nuclear threats. This convergence demands an urgent, integrated examination of how emerging technologies are reshaping Pakistan’s national security posture and regional power balance.

Objectives of the Study

1. To analyze the geopolitical risks posed by AI and cyber warfare capabilities to Pakistan’s state security
2. To assess Pakistan’s current AI and cyber warfare capabilities and gaps
3. To examine how regional adversaries (especially India) are leveraging these technologies
4. To identify pathways of escalation and strategic instability

Research Questions

1. What is the current state of AI and offensive cyber capabilities in Pakistan and among its adversaries?
2. In what ways can AI-enabled cyber operations affect nuclear signaling and deterrence stability between India and Pakistan?
3. How do great-power (US–China) technological rivalries influence Pakistan's strategic choices?
4. What institutional and doctrinal gaps exist in Pakistan's response framework?

Theoretical Framework

The theoretical foundation of this study rests on a synthesis of classical and structural realism, adapted to the realities of technological power transitions in the 21st century (Mearsheimer, 2014). Realism posits that states operate in an anarchic international system where relative power determines survival and influence, compelling continuous competition for security (Waltz, 1979). Emerging technologies, particularly artificial intelligence and cyber capabilities, now constitute a new currency of power, accelerating shifts in the global and regional distribution of capabilities (Allison, 2017; Horowitz, 2018). In South Asia, the rapid diffusion of AI-driven military systems and offensive cyber tools mirrors historical power transitions that have historically precipitated major wars, intensifying the security dilemma whereby one state's defensive investments are perceived as offensive threats by adversaries (Glaser, 2010). For developing nuclear powers like Pakistan, this dilemma is particularly acute: investments in digital resilience or asymmetric AI applications risk provoking preemptive responses from technologically superior neighbors, while inaction invites exploitation of existing vulnerabilities (Narang, 2022). The perpetual quest for security thus drives a techno-geopolitical arms race, where relative gains in algorithmic superiority or cyber intrusion capabilities redefine deterrence and compellence far beyond traditional material metrics (Futter, 2023; Lieber & Press, 2025).

Offensive realism further sharpens this lens by emphasizing escalation dominance in contested digital domains (Mearsheimer, 2001). States, driven by the imperative to maximize power and ensure survival, seek not merely parity but decisive advantage in domains that permit first-strike stability or rapid crisis manipulation. In cyberspace and AI-enabled warfare, the offense-defense balance tilts heavily toward offense due to low entry costs, attribution difficulties, and the speed of digital operations (Schneider, 2025). Achieving escalation dominance now involves pre-positioning malware in adversary networks, developing AI systems that can autonomously degrade command-and-control, or deploying deepfake capabilities to shape strategic perceptions during crises (Lin-Greenberg, 2024). For a state facing conventional inferiority, such as Pakistan vis-à-vis India, offensive realism predicts aggressive pursuit of disruptive digital tools to offset material asymmetries and restore deterrence by threatening unacceptable costs at multiple rungs of the escalation ladder (Dalton et al., 2025). Yet this pursuit simultaneously erodes crisis stability, as the same tools that promise dominance also lower thresholds for initiating conflict and compress decision timelines for leaders (Acton, 2023).

The study adapts the strategic stability framework originally developed for nuclear dyads to the intertwined cyber, AI, and nuclear domains, building on seminal contributions that examine how non-nuclear capabilities affect nuclear risk (Bracken, 2012; Lindsay, 2020). Strategic stability comprises crisis stability (incentives to avoid striking first) and arms race stability (incentives to refrain from destabilizing buildups) (Acton, 2025). When conventional cyber and AI systems become entangled with nuclear command, control, communications, and intelligence infrastructure, attacks on non-nuclear assets can generate fear of disarming

strikes, prompting pre-delegation or launch-on-warning postures that heighten false-alarm risks (Lindsay & Gartzke, 2023). Entanglement theory illuminates this dynamic: cyber intrusions into dual-use early-warning networks or AI-assisted battle management systems can be misinterpreted as preparatory moves for nuclear use, particularly in compressed South Asian geography where flight times are mere minutes (Futter, 2021). The proposed "Techno-Geopolitical Vulnerability Matrix" serves as the integrative conceptual model, plotting developing states along two axes technological asymmetry (lag/lead relative to primary adversary) and institutional resilience (civil-military coordination, talent base, doctrinal maturity) to assess exposure to four archetypal risks: exploitation, entrapment, escalation spirals, and strategic collapse (Narang, 2022). Pakistan occupies the high-vulnerability quadrant, facing acute exploitation risks from India's accelerating AI militarization and China-dependent technology transfers, while institutional fragmentation hampers resilient responses. This matrix enables systematic evaluation of how emerging technologies erode traditional deterrence and offers diagnostic utility for policy intervention in similarly positioned states.

Findings and Results

Pakistan's AI and cyber capabilities remain characterized by modest offensive potential and profound defensive deficiencies, constraining its ability to counter technologically superior adversaries in an increasingly digitized battlespace. The National Artificial Intelligence Policy 2025 emphasizes innovation funds, sectoral roadmaps, and ethical governance, yet implementation lags persist, with heavy reliance on foreign technologies and limited indigenous offensive tools (Ministry of Information Technology & Telecommunication, Pakistan, 2025). Offensive operations are largely confined to state-linked groups employing basic malware and phishing, as seen in APT36's Crimson RAT deployments, while defensive structures suffer from delayed national CERT maturation and fragmented institutional coordination (CloudSEK, 2025). This asymmetry is exacerbated by surging internet penetration approaching 100 million users without commensurate resilient architectures, rendering critical infrastructure vulnerable to disruption (International Growth Centre, 2025). Talent deficits and regulatory gaps further hinder scalable AI militarization, positioning Pakistan as a reactive player in techno-geopolitical contests (Roy & Reichberg, 2024).

In stark contrast, India's rapid advancement in AI-enabled intelligence, surveillance, reconnaissance (ISR), autonomous systems, and offensive cyber operations has widened the strategic imbalance in South Asia. The Indian Army's 2026-27 AI Roadmap integrates large language models for threat detection, facial recognition, and predictive analytics, with over 50 projects underway at the AI Incubation Centre in collaboration with Bharat Electronics Limited (Eurasia Review, 2025a). Allocations exceeding $11 million in the 2025-26 defense budget underpin deployments of AI-enhanced drones, swarm technologies, and the Tactical Command, Control, Communications, and Intelligence (TAC-C3I) system, achieving 94 percent accuracy in electronic signature identification during crises (Newsweek, 2025; The Diplomat, 2025). Offensive cyber doctrines leverage military-civil fusion analogs, enabling precision disruptions and information dominance, as demonstrated in Operation Sindoor's multi-domain operations (India Today, 2025). This trajectory not only amplifies escalation dominance but also entangles conventional capabilities with nuclear postures, challenging regional stability (KPMG, 2025).

Empirical evidence from 2024-2025 reveals a pattern of cyber intrusions and information operations impacting Pakistan, both attributed and unattributed, underscoring its digital fragility. The May 2025 crisis following the Pahalgam attack witnessed over 1.5 million

cyberattacks exchanged, including DDoS barrages, malware infiltrations like Crimson RAT by Pakistan-linked APT36 targeting Indian networks, and reciprocal disruptions of power grids and C4ISR nodes (NSFOCUS, 2025a; Stimson Center, 2025). Unattributed operations, often routed through proxies, exploited vulnerabilities in Pakistan's nascent defenses, with hacktivist surges causing brief but propagandistic defacements and data exfiltration (CYFIRMA, 2025). Economic losses from digital fraud reached 4.6 percent of GDP, amplifying societal vulnerabilities amid geopolitical frictions (Global Anti-Scam Alliance via Stimson Center, 2025). These incidents highlight attribution challenges, where deniability fuels persistent engagement below war thresholds (CAPS India, 2025).

The proliferation of AI-enabled deepfakes introduces acute risks of perception management during crises, capable of manipulating strategic decision-making in nuclear dyads. During the 2025 Indo-Pak tensions, fabricated satellite imagery, deepfake videos of explosions, and synthetic audio of commanders issuing nuclear alerts proliferated, eroding trust and compressing response timelines (Modern Diplomacy, 2025). Generative AI tools lowered barriers for non-state actors to forge perceptual realities, as evidenced by disinformation campaigns amplifying casualties and false-flag narratives (CYFIRMA, 2025). In South Asia's compressed geography, such manipulations could catalyze miscalculation, transforming informational entropy into kinetic escalation (Patil, 2025). Absent robust verification protocols, deepfakes exacerbate the fog of war, rendering authentic signaling precarious (Lowy Institute, 2025).

Entanglement risks are profoundly amplified as cyber-attacks on dual-use Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems risk misinterpretation as preemptive nuclear strikes. Intrusions into shared networks evident in 2025's grid disruptions and GPS spoofing could cascade into fears of disarming attacks, prompting launch-on-warning postures in a region with minute flight times (NSFOCUS, 2025b; Belfer Center, 2025). India's AI-augmented precision operations and Pakistan's countermeasures entwine conventional disruptions with nuclear signaling, blurring red lines and incentivizing pre-delegation (Akhtar, 2025). This vulnerability matrix positions developing nuclear powers at heightened inadvertent escalation thresholds, demanding doctrinal clarifications absent in current frameworks (South Asian Voices, 2025).

China's influence via technology transfers under the Digital Silk Road component of CPEC significantly bolsters Pakistan's capabilities while entrenching dependencies and limited Western cooperation isolates Islamabad further. Proposals for joint ventures in 5G/6G, AI, cloud computing, and cybersecurity aim to overhaul digital infrastructure, yet reliance on Chinese hardware exposes backdoor risks amid U.S.-China rivalry (Arab News Pakistan, 2025; CPEC Info, 2025). Limited engagements with Western entities curtailed by sanctions and alignment perceptions constrain diversified sourcing, reinforcing asymmetric vulnerabilities (PRIO, 2024). This great-power entanglement not only accelerates capability gaps closure but also imports geopolitical frictions, complicating autonomous strategic choices in South Asia's volatile landscape (Eurasian Research, 2025).

Discussion

The convergence of AI and cyber warfare profoundly reinterprets South Asian strategic stability, transforming a historically nuclear-centric dyad into a multi-domain entanglement where conventional digital operations carry nuclear implications (Acton, 2025). Pakistan’s persistent defensive gaps and modest offensive capabilities, juxtaposed against India’s accelerating AI-enabled ISR and autonomous systems, exacerbate the classic security dilemma: Islamabad’s pursuit of asymmetric cyber tools to offset conventional inferiority risks

provoking preemptive Indian responses, while inaction invites exploitation (Narang, 2022). Comparative analysis with other middle powers reveals that Pakistan's trajectory most closely resembles a high-vulnerability outlier, constrained by resource limitations and great-power alignment choices (Horowitz et al., 2024). The 2025 crisis cycle, marked by mutual cyber intrusions and AI-generated perceptual distortions, empirically validates entanglement theory: attacks on dual-use C4ISR infrastructure generated credible fears of command degradation, compressing decision timelines in a region with minute missile flight times (Lindsay & Gartzke, 2023).

Non-state actors and terrorist organizations further complicate this landscape by democratizing access to generative AI tools for deepfake propagation and low-cost cyber disruption, eroding state monopoly over escalation pathways while ethical and normative challenges permit unchecked racing dynamics in the absence of multilateral restraint regimes (Futter, 2023). Pakistan's heavy dependence on Chinese technology transfers via the Digital Silk Road, while offering rapid capability infusion, imports geopolitical baggage and potential backdoors, limiting strategic autonomy and inviting Western sanctions that further widen the asymmetry.

Ultimately, the findings underscore that emerging technologies do not merely augment but fundamentally destabilize Pakistan's security environment, shifting the locus of risk from deliberate aggression to inadvertent escalation driven by misperception and entanglement (Acton, 2025). Without deliberate doctrinal adaptation and confidence-building measures particularly bilateral cyber/AI restraint agreements with India and diversified international partnerships Pakistan risks progressive erosion of its minimum credible deterrence. The proposed Techno-Geopolitical Vulnerability Matrix offers a diagnostic tool for similarly positioned states, highlighting that resilience demands not only technological catch-up but institutional coherence and normative engagement in an era where algorithmic superiority increasingly defines power (Horowitz et al., 2024).

Conclusion

The geopolitical risks emanating from artificial intelligence and cyber warfare represent a transformative challenge to Pakistan's national security, fundamentally altering the character of strategic competition in South Asia. Where traditional deterrence once rested on opaque nuclear arsenals and conventional imbalances, the integration of AI-enabled systems and offensive cyber tools has introduced new pathways of instability characterized by speed, ambiguity, and entanglement. Pakistan's modest offensive capabilities and persistent defensive deficiencies, set against India's rapid militarization of artificial intelligence and autonomous platforms, have widened an already significant asymmetry. This technological lag not only constrains Pakistan's ability to impose costs or achieve information dominance in crises but also renders its critical infrastructure, early-warning networks, and nuclear command systems acutely vulnerable to disruption. The events of 2025, particularly the intense cyber exchanges and AI-generated perceptual distortions during periods of heightened tension, demonstrate that digital operations can no longer be treated as peripheral; they now constitute a primary domain where escalation can originate and spiral with little warning. In a region defined by compressed decision timelines and mutual suspicion, the fusion of conventional cyber-attacks with nuclear signaling risks transforming manageable crises into catastrophic ones through miscalculation rather than intent.

To mitigate these escalating risks, Pakistan must pursue a multifaceted strategy that transcends mere technological acquisition and addresses the deeper institutional and doctrinal deficits exposed by this study. The establishment of a unified National AI and Cyber

Security Authority under direct civilian-military oversight, coupled with accelerated investment in indigenous talent development and resilient digital architectures, is essential to narrow defensive gaps and build credible asymmetric options. Doctrinal innovation explicitly clarifying red lines for cyber intrusions into dual-use systems and integrating AI governance into nuclear command protocols offers a pathway to restore crisis stability. Equally critical are diplomatic initiatives: bilateral confidence-building measures with India on restraint in offensive cyber and AI applications, alongside diversified international partnerships that reduce over-reliance on any single great-power provider. Without such proactive adaptation, Pakistan risks progressive erosion of its minimum credible deterrence in an environment where algorithmic superiority increasingly defines power projection and survival. The broader implication for developing nuclear powers is unambiguous: in the absence of deliberate institutional resilience and normative engagement, emerging technologies will continue to shift the balance from stable mutual deterrence toward a precarious landscape dominated by inadvertent escalation and strategic vulnerability.

References

Acton, J. M. (2018). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war. *International Security*, *43*(1), 56–99.

Acton, J. M. (2023). Cyber warfare and inadvertent escalation. *Daedalus*, *152*(2), 45–63.

Acton, J. M. (2025). *Entanglement 2.0: AI, cyber, and nuclear risks*. Carnegie Endowment for International Peace.

Akhtar, R. (2025, July 19). The problem with India's new missile gambit. *Dawn*. https://www.dawn.com/news/1925251

Allison, G. (2017). *Destined for war: Can America and China escape Thucydides's trap?* Houghton Mifflin Harcourt.

Arab News Pakistan. (2025, November 17). At Baku talks, Pakistan, China push Digital Silk Road as next phase of economic corridor. https://www.arabnews.pk/node/2622928/pakistan

Ayesa. (2025). Cyber geopolitics 2025: Between hybrid warfare and threat intelligence. https://www.ayesa.com/en/insight/cyber-geopolitics-2025-between-hybrid-warfare-and-threat-intelligence/

Belfer Center. (2025, May 13). Escalation gone meta: Strategic lessons from the 2025 India-Pakistan crisis. Harvard Kennedy School.

Bracken, P. (2012). *The second nuclear age: Strategy, danger, and the new power politics*. Times Books.

CAPS India. (2025, June 5). Cyber warfare: Dual operational fronts in contemporary India-Pakistan conflicts. https://capsindia.org/cyber-warfare-dual-operational-fronts-in-contemporary-india-pakistan-conflicts/

Carnegie Endowment for International Peace. (2025a). Governing military AI amid a geopolitical minefield. https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield

Center for a New American Security. (2025). New CNAS report examines the threat of emerging AI capabilities to cybersecurity. https://www.cnas.org/press/press-release/new-cnas-report-examines-how-emerging-ai-capabilities-could-disrupt-the-cyber-offense-defense-balance

Center for Cyber Diplomacy and International Security. (2025). Cyber warfare in 2025: Executive report. https://cybercenter.space/2025/08/03/cyber-warfare-in-2025-executive-report/

CloudSEK. (2025, August 20). Brief disruptions, bold claims: The tactical reality behind the India-Pakistan hacktivist surge. https://www.cloudsek.com/blog/brief-disruptions-bold-claims-the-tactical-reality-behind-the-india-pakistan-hacktivist-surge
Council on Foreign Relations. (2025). *U.S. economic security*. https://www.cfr.org/task-force-report/us-economic-security
CPEC Info. (2025, November 17). Pakistan pushes Digital Silk Road as new CPEC priority. http://cpecinfo.com/pakistan-pushes-digital-silk-road-as-new-cpec-priority/
CyberPeace Institute. (2025). Cyber dimensions of a hybrid warfare. https://cyberpeaceinstitute.org/news/cyber-dimensions-of-a-hybrid-warfare/
CYFIRMA. (2025). Firewalls and frontlines: The India-Pakistan cyber battlefield crisis. https://www.cyfirma.com/research/firewalls-and-frontlines-the-india-pakistan-cyber-battlefield-crisis/
Dalton, T., Kreps, S., & Lin-Greenberg, E. (2025). Crisis of command: AI and nuclear stability in South Asia. *Journal of Strategic Studies*, Advance online publication.
Eurasia Review. (2025a, April 4). Code, combat, and command: How the Indian Army is leveraging AI and big data for the battlefield of tomorrow – Analysis. https://www.eurasiareview.com/04042025-code-combat-and-command-how-the-indian-army-is-leveraging-ai-and-big-data-for-the-battlefield-of-tomorrow-analysis/
Eurasian Research. (2025). China's post-pandemic Digital Silk Road. https://www.eurasian-research.org/publication/chinas-post-pandemic-digital-silk-road/
European Parliamentary Research Service. (2025). Briefing: Artificial intelligence in military applications. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf
Express Tribune. (2025a). Pakistan to launch first AI policy. https://tribune.com.pk/story/2509450/pakistan-to-launch-first-ai-policy
Express Tribune. (2025b). How AI Policy 2025 can shape a digital future for all. https://tribune.com.pk/story/2559280/how-ai-policy-2025-can-shape-a-digital-future-for-all
Foreign Affairs. (2025). China is winning the cyberwar: America needs a new strategy of deterrence. https://www.foreignaffairs.com/china/china-winning-cyberwar-artificial-intelligence
Foundation for Defense of Democracies. (2025). Russia's AI-powered cyberattacks threaten to outpace Western defenses. https://www.fdd.org/analysis/policy_briefs/2025/02/20/russias-ai-powered-cyberattacks-threaten-to-outpace-western-defenses/
Futter, A. (2021). *Hacking the bomb: Cyber threats and nuclear weapons*. Georgetown University Press.
Futter, A. (2023). Cyber threats and the second nuclear age. *Survival*, *65*(4), 89–108.
Ghani, A. (2025). AI driven cyber warfare between China and India and its impact on Pakistan's national security. ResearchGate. https://www.researchgate.net/publication/392705004
Glaser, C. L. (2010). *Rational theory of international politics*. Princeton University Press.
Global Anti-Scam Alliance (via Stimson Center). (2025). Assessing cyber risks and resilience in India and Pakistan.
GlobeNewswire. (2025). Artificial intelligence (AI) in military market 2025-2030. https://www.globenewswire.com/news-release/2025/06/27/3106390/0/en/Artificial-Intelligence-AI-in-Military-Market-2025-2030-Investment-Opportunities-in-Surveillance-Intelligence-Cybersecurity-Electronic-Warfare-and-Autonomous-Systems.html

Hanson, R., et al. (2024). The future of Indo-Pacific information warfare: Challenges and prospects from the rise of AI. RAND Corporation.
Help Net Security. (2025). How nations build and defend their cyberspace capabilities. https://www.helpnetsecurity.com/2025/11/04/bernhards-blumbergs-cert-lv-cyberspace-operations-attribution/
Horowitz, M. C. (2018). Artificial intelligence and the diffusion of military power. *International Security*, *42*(4), 7–45.
Horowitz, M. C., et al. (2024). Middle-power responses to emerging military technologies. *International Security*, *49*(2), 45–78.
India Today. (2025, September 5). Nuclear propulsion, AI, next-gen warfare: India unveils 15-year defence plan. https://www.indiatoday.in/india/story/india-15-year-defence-plan-ai-hypersonic-next-generation-warfare-2782430-2025-09-05
International Growth Centre. (2025). Harnessing AI, data and technology for growth in Pakistan. https://www.theigc.org/blogs/data-and-ai/harnessing-ai-data-technology-growth-pakistan
Journal of Law & Cyber Warfare. (2025). Tallinn Manual 3.0: Sovereignty and attribution in 2025. https://www.jlcw.org/2025/07/22/tallinn-manual-3-0-sovereignty-and-attribution-in-2025-cyber-warfare/
KPMG. ((2025). Artificial intelligence (AI) in defence modernisation. https://kpmg.com/in/en/blogs/2025/06/artificial-intelligence-in-defence-modernisation.html
KPMG International. (2025). Top geopolitical risks 2025. https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/03/top-geopolitical-risks-2025-web.pdf
Lieber, K. A., & Press, D. G. (2025). The new era of counterforce: Technological change and the future of nuclear deterrence. *International Security*, Advance online publication.
Lin-Greenberg, E. (2024). Deepfakes and deterrence failure in crisis bargaining. *Security Studies*, *33*(3), 401–432.
Lindsay, J. R. (2020). Cyber conflict and nuclear stability. *International Security*, *45*(2), 7–49.
Lindsay, J. R., & Gartzke, E. (2023). Cross-domain deterrence in cyberspace. *Journal of Cybersecurity*, *9*(1), 1–18.
Lowy Institute. (2025). Deepfakes and nuclear weapons: Why AI regulation can't wait. https://www.lowyinstitute.org/the-interpreter/deepfakes-nuclear-weapons-why-ai-regulation-can-t-wait
Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W.W. Norton.
Mearsheimer, J. J. (2014). *The tragedy of great power politics* (Updated ed.). W.W. Norton.
Microsoft. (2025). Microsoft: Russia, China increasingly using AI to escalate cyberattacks on the US. Associated Press. https://apnews.com/article/ai-cybersecurity-russia-china-deepfakes-microsoft-ad678e5192dd747834edf4de03ac84ee
Ministry of Information Technology & Telecommunication, Pakistan. (2025). *National Artificial Intelligence Policy 2025*. Government of Pakistan.
Modern Diplomacy. (2025, July 6). How AI-powered disinformation could ignite a nuclear crisis in South Asia. https://moderndiplomacy.eu/2025/07/06/how-ai-powered-disinformation-could-ignite-a-nuclear-crisis-in-south-asia/
Narang, V. (2022). *Seeking the bomb: Strategies of nuclear proliferation*. Princeton University Press.

Newsweek. (2025, October 31). India ramps up AI use for military. https://www.newsweek.com/india-ramps-up-ai-use-military-10958120
NSFOCUS. (2025a, May 13). India-Pakistan conflicts escalating: Military operations and DDoS attacks making targeted strikes. https://nsfocusglobal.com/india-pakistan-conflicts-escalating-military-operations-and-ddos-attacks-making-targeted-strikes/
NSFOCUS. (2025b). Two battlegrounds: India-Pakistan conflicts and DDoS attacks.
OECD. (2025). *OECD science, technology and innovation outlook 2025*. https://www.oecd.org/en/about/news/press-releases/2025/10/oecd-science-technology-and-innovation-outlook-2025.html
Patil, S. (2025, July 22). From missiles to malware: India-Pakistan cyber rivalry and lessons for Taiwan. *Taiwan Insight*.
PRIO. (2024). Artificial intelligence and Pakistan's national security. Peace Research Institute Oslo.
RAND Corporation. (2025). Potential for U.S.-China cooperation on reducing AI risks. https://www.rand.org/pubs/perspectives/PEA4189-1.html
Riskonnect. (2025). The next cyber crisis may start in someone else's supply chain. Help Net Security. https://www.helpnetsecurity.com/2025/10/23/geopolitics-drives-cyber-threats-report/
Roy, K., & Reichberg, G. M. (2024). Artificial intelligence and Pakistan's national security. PRIO.
Schneider, J. (2025). The capability/vulnerability paradox in cyber offense-defense. *Journal of Global Security Studies*, *10*(Spr 1), 1–19.
SIPRI. (2025). Nuclear risks grow as new arms race looms—new SIPRI Yearbook out now. https://www.sipri.org/media/press-release/2025/nuclear-risks-grow-new-arms-race-looms-new-sipri-yearbook-out-now
South Asian Voices. (2025, September 30). Pakistan's new rocket force: Strategic deterrence and escalation risks. https://southasianvoices.org/sec-m-pk-n-pakistan-rocket-force-09-30-2025/
Startup.pk. (2025). A deep dive into Pakistan's AI Policy 2025. https://www.startup.pk/a-deep-dive-into-pakistans-ai-policy-2025-vision-strategy-and-what-it-means-for-startups-and-investors/
Stimson Center. (2025). Assessing cyber risks and resilience in India and Pakistan. https://www.stimson.org/2025/assessing-cyber-risks-and-resilience-in-india-and-pakistan/
Strafasia. (2025). Securing the future: Pakistan's path to cyber dominance.
The Diplomat. (2025, October 14). India's use of artificial intelligence during the Indo-Pak four-day crisis. https://thediplomat.com/2025/10/indias-use-of-artificial-intelligence-during-the-indo-pak-four-day-crisis/
Valdai Club. (2025). Strategic implications and regional dynamics of AI on modern warfare for Pakistan.
Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.
World Economic Forum. (2025a). *Global cybersecurity outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
World Economic Forum. (2025b). Geopolitical tensions, AI and more are complicating the cybersecurity pace. https://www.weforum.org/stories/2025/01/global-cybersecurity-outlook-complex-cyberspace-2025/