RESEARCH PAPERS

Asymmetric Shadows: Pakistan’s Cyberwarfare Posture in Theory and Practice

Author: Satyajit Lall • **Published:** April 02, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

In the shadows of nuclear deterrence, cyberspace has emerged as Pakistan’s most agile battlefield where ambiguity, influence, and deniability shape strategy more than firepower. This paper examines Pakistan’s evolving cyberwarfare posture, arguing that its approach is neither ad hoc nor underdeveloped, but instead a coherent extension of its long-standing asymmetric and hybrid warfare doctrine. Despite lacking a formal, publicly articulated cyber doctrine, Pakistan has cultivated a flexible, intelligence-driven model that prioritizes deniable, sub-threshold operations, narrative dominance, and escalation control. A central paradox defines Pakistan’s cyber strategy. Domestically, the country faces acute vulnerabilities including fragmented governance, limited technical capacity, weak cyber resilience, and an underdeveloped regulatory ecosystem. Critical infrastructure remains exposed, incident response is largely reactive, and human capital shortages further constrain defensive capabilities. Yet rather than inhibiting cyber ambition, these weaknesses have incentivized a greater reliance on offensive and influence-oriented cyber tools, which offer low-cost, high-impact alternatives to conventional military power. Externally, Pakistan’s cyber posture is shaped overwhelmingly by its rivalry with India. Perceived Indian technological superiority, coupled with persistent cyber espionage and information warfare threats, has reinforced Pakistan’s preference for ambiguity and deniability over overt deterrence. Cyberspace is thus treated as an extension of geopolitical competition, where operations are calibrated to impose psychological and strategic costs without crossing escalation thresholds. The May 2025 crisis, Operation Sindoor, serves as a critical case study. The conflict highlighted Pakistan’s emphasis on narrative warfare, with coordinated information campaigns targeting domestic, regional, and international audiences. Cyber operations during this period remained

limited and largely symbolic, focused on disruption, signaling, and perception management rather than sustained or destructive attacks. This restraint reflects a deliberate strategy aimed at avoiding escalation while maintaining strategic relevance. However, the crisis also exposed significant defensive shortcomings. Pakistan's cyber resilience appeared strained under pressure, with narrative control often substituting for technical robustness. This imbalance, external agility paired with internal fragility, underscores the structural limits of its cyber posture. Ultimately, Pakistan's cyberwarfare doctrine is best understood as an adaptive, asymmetric strategy rooted in its broader security culture. It privileges influence over disruption, ambiguity over declaration, and crisis-driven operations over sustained engagement. While effective in the short term, this approach carries long-term risks, particularly in a nuclearized region where miscalculation in the cyber domain could have far-reaching consequences.

Introduction

Cyberspace has become a prime gray-zone arena for nuclear-armed rivals to pursue coercion without triggering conventional or nuclear escalation. In South Asia, the India–Pakistan rivalry now extends decisively into this domain, with cyber operations, information warfare, and narrative manipulation increasingly complementing, or supplanting, traditional military tools. For Pakistan, the cyber space presents a stark paradox: deep vulnerabilities in governance and resilience expose it to attack, yet these same weaknesses have driven a growing embrace of offensive cyber capabilities as a cornerstone of asymmetric and hybrid strategies. The May 2025 conflict, Operation Sindoor, offers a vivid, real-time window into Pakistan's evolving cyberwarfare doctrine and its role in attempting to reshape deterrence between the two nuclear powers.

Unlike several emerging powers that have issued explicit cyber doctrines, Pakistan has avoided a formal, publicly declared framework for cyberwarfare. Its approach must instead be pieced together from policy statements, institutional structures, threat perceptions, and crucially empirical patterns of behavior during crises. Scholarship on Pakistan's security posture consistently highlights a strategic preference for deniable, sub threshold instruments of power, from proxy militancy to information manipulation, that advance objectives while minimizing escalation risks.[i] Cyber operations fit seamlessly within this tradition, delivering low cost means for signaling intent, imposing disruption, and contesting narratives. Far from indicating doctrinal incoherence, this deliberate opacity promotes flexibility, sustains strategic ambiguity, and favors intelligence-led adaptability in an asymmetric rivalry.

Pakistan's domestic cyber environment remains markedly fragile. Analyses of its threat landscape reveal persistent weaknesses: fragmented institutional coordination, constrained technical capacity, and pervasive vulnerabilities in civilian and critical information infrastructure.[ii] Official advisories and policy documents readily concede the magnitude of these cyber threats, yet chronic implementation shortfalls separate ambitious goals from actual operational readiness.[iii] This glaring asymmetry, ambitious offensive pursuits juxtaposed against defensive fragility, defines a core paradox in Pakistan's cyber posture, profoundly influencing the selective and calibrated use of cyber tools.

Operation Sindoor marked a significant escalation in India–Pakistan hostilities, encompassing kinetic strikes, drone activity, and an intense wave of cyber and information operations. Indian media and cybersecurity firms reported large-scale cyber intrusions, hacktivist campaigns, and coordinated misinformation efforts during the conflict, many of which were attributed to Pakistan-linked actors.[iv] While attribution in cyberspace remains inherently contested, the crisis nonetheless offers valuable insight into how cyber operations were synchronized with narrative warfare and diplomatic signaling. For Pakistan, the conflict functioned as a real-world stress test of both cyberwarfare practices and cyber resilience under pressure.

Internal Cyber Threats Faced by Pakistan

Pakistan's internal cyber threat environment arises from intertwined structural deficiencies, institutional fragmentation, and persistent non state activity. Although strategic discourse in Pakistan frequently attributes cyber threats to external sources, usually India, the most pressing and persistent dangers stem from domestic digital fragilities. These internal vulnerabilities severely limit cyber resilience and decisively tilt Pakistan's cyberwarfare posture toward offensive, deniable operations rather than comprehensive defensive investment.

A primary obstacle resides in fragmented cyberspace governance. Cybersecurity responsibilities scatter across civilian and military entities, including the Ministry of Information Technology and Telecommunication, the National Centre for Cyber Security, sectoral regulators, and intelligence agencies. The 2021 National Cyber Security Policy promised centralized coordination, yet mechanisms remain feeble, with uneven execution at federal and provincial tiers.[v] Scholarly evaluations repeatedly emphasize that policy aspirations have far exceeded institutional capabilities, yielding fragmented operational responses amid any cyber crises.[vi]

Human capital shortages compound these institutional shortfalls. Pakistan grapples with a severe deficit of qualified cybersecurity experts, fueled by chronic underfunding of specialized education, uncompetitive public sector salaries, and substantial brain drain toward private sector roles and international opportunities.[vii] Consequently, government networks and critical information infrastructure often depend on legacy systems and inadequately skilled staff, heightening risks of intrusion, data exfiltration, and operational disruption. This persistent skills gap erodes proactive defenses and cripples timely incident response, especially under crisis induced strain.

Critical information infrastructure (CII) represents another area of acute vulnerability. Financial institutions, energy networks, telecommunications providers, and government databases have all been identified as frequent targets of cyberattacks. In response, Pakistani authorities have periodically issued advisories warning of increased threat activity against sensitive systems, including tax administration platforms and financial data repositories.[viii] However, these advisories also implicitly acknowledge the reactive nature of Pakistan's cyber defenses, which tend to prioritize post-incident mitigation rather than proactive threat hunting or resilience-building. Studies of Pakistan's cyber threat landscape suggest that legacy systems, poor patch management, and reliance on imported hardware and software compound these risks.[ix]

Non state actors exert a profoundly destabilizing influence on Pakistan's internal cyber environment. Cybercriminal syndicates exploit regulatory voids and lax enforcement to perpetrate financial fraud, ransomware campaigns, and widespread data breaches with near impunity.[x] Concurrently, ideologically driven entities, including extremist organizations, harness digital platforms for recruitment, fundraising, and propaganda propagation. While frequently analyzed through a counterterrorism lens, these efforts erode informational integrity and overburden already strained monitoring resources. The porous boundaries among criminal, ideological, and politically motivated cyber conduct severely hinder attribution and effective countermeasures.

Disinformation and narrative manipulation present a subtler yet comparably corrosive internal threat. Pakistan's digital ecosystem features widespread social media adoption, pervasive low digital literacy, and minimal regulatory scrutiny, rendering populations highly vulnerable to misinformation, rumor cascades, and orchestrated influence operations.[xi] In crisis moments, authorities typically favor narrative dominance via censorship, platform throttling, or punitive legal measures over transparent, trust building communication strategies. Although these tactics may secure fleeting narrative control, they fail to bolster enduring information resilience or public confidence.

The legal regulatory architecture for cyberspace mirrors deeper tensions between security priorities and civilian governance. Laws such as the Prevention of Electronic Crimes Act have broadened state oversight of online

expression, yet enforcement remains patchy and resource constrained. Critics contend that this focus on control and surveillance has not been offset by equivalent commitments to technical defenses or public private partnerships.[xii] Such asymmetry entrenches a securitized cyber paradigm that prioritizes monitoring over genuine resilience building.

Collectively, these internal cyber threats reveal a structural paradox in Pakistan's cyber posture. While the state aspires to leverage cyberspace as a domain of strategic competition, its domestic cyber ecosystem remains vulnerable, reactive, and unevenly governed. These weaknesses do not preclude offensive cyber activity; indeed, they may incentivize it. Offensive and narrative-oriented cyber operations offer relatively low barriers to entry and align with Pakistan's broader preference for deniable, sub-threshold tools of statecraft. However, the same internal vulnerabilities that enable such activities also limit Pakistan's ability to absorb and manage cyber escalation during crises.

External Cyber Threats Faced by Pakistan

Pakistan continues to struggle with domestic cyber vulnerabilities, but its strategic thinking about cyberspace is shaped far more by perceived dangers from abroad. Among these, India plays the most prominent role. Pakistan's view of external cyber threats is deeply connected to its long-standing security rivalry with India, a relationship marked by mutual distrust, asymmetric capabilities, and repeated episodes of low-level conflict. In this setting, cyberspace is understood not just as a technical arena, but as another front in geopolitical competition and a tool for strategic signaling.

Within Pakistani policy and military circles, India stands as the preeminent external cyber adversary. This view draws strength from India's accelerating investments in cyber capabilities, burgeoning public private partnerships in cybersecurity, and intensifying technological collaboration with the United States and Israel.[xiii] Pakistani analysts routinely interpret these advances as evidence of emerging Indian cyber dominance, posing direct risks to Pakistan's military readiness, economic stability, and informational autonomy. Apprehensions reach beyond disruptive attacks to include espionage, pervasive surveillance, and the potential exfiltration of sensitive government and defense data.

Cyber espionage emerges as the most acute external threat. Open source reporting and cybersecurity industry assessments have chronicled sustained intrusion campaigns against Pakistani government bodies, military linked entities, academic institutions, and private sector targets.[xiv] Although attribution remains disputed, multiple campaigns are widely assessed by analysts as tied to advanced persistent threat groups aligned with Indian strategic objectives. From Islamabad's vantage, these operations deliver unrelenting, sub threshold pressure that erodes the distinction between routine peacetime rivalry and latent conflict.

Beyond India, Pakistan registers cyber threats from technologically superior Western states, chiefly in surveillance and intelligence gathering. Disclosures about global surveillance frameworks have deepened a pervasive sense of exposure among Pakistani decision makers, particularly concerning communications security and data sovereignty.[xv] While these concerns rarely assume the confrontational tone reserved for India, they nonetheless underpin Pakistan's growing policy focus on digital sovereignty and data localization initiatives.

Non-state external actors substantially complicate Pakistan's cyber threat landscape. Transnational hacktivist collectives, cybercriminal networks, and ideologically driven groups operate across borders, capitalizing on geopolitical friction for visibility or profit. During India–Pakistan crises, these actors frequently align rhetorically with one side, launching attacks that carry political symbolism yet lack centralized state direction.[xvi] For Pakistan, such incidents generate acute attribution difficulties and elevate escalation risks, as externally triggered actions can readily be misread as state-sponsored aggression.

Regional spillover further shapes threat perceptions. South Asia's tightly interconnected digital infrastructure ensures that cyber incidents in one country often produce cascading consequences elsewhere. Attacks on shared financial platforms, telecommunications networks, or cloud providers can impair Pakistani systems even when Pakistan is not the intended target.[xvii] This structural interdependence deepens a pervasive sense of strategic exposure, especially given Pakistan's heavy reliance on foreign-controlled digital services and infrastructure.

Information warfare amplifies these external pressures. Pakistani analysts increasingly stress the fusion of technical cyber operations with narrative manipulation, viewing adversaries as pursuing not only network disruption but also perceptual dominance both domestically and abroad.[xviii] Coordinated disinformation, social media amplification, and strategic leaks of compromised material are interpreted as deliberate efforts to erode Pakistan's legitimacy, widen internal cleavages, and sway international opinion. This convergence has cemented a securitized conception of cyberspace in which narrative control is regarded as an integral dimension of national defense.

These threats are also framed through the logic of escalation management. Unlike conventional military action, cyber operations are inherently ambiguous and deniable, generating persistent uncertainty about intent and appropriate retaliation.[xix] Pakistani strategic discourse repeatedly warns that misattributed or misinterpreted cyber incidents, whether espionage, disruption, or influence activity, could inadvertently trigger wider conflict. This risk calculus underpins Pakistan's restrained cyber deterrence posture, which privileges operational flexibility and deniability over explicit declaratory commitments.

Taken together, these external cyber threats decisively mold Pakistan's dual approach to cybersecurity and cyberwarfare. The overriding focus on India as the primary adversary fosters a reactive orientation, with cyber investments and planning anchored in crisis contingencies rather than sustained resilience. Simultaneously, the diffuse and ambiguous character of external threats encourages Pakistan to adopt comparable instruments. Cyber operations provide a low-threshold means of countering perceived pressure while remaining below conventional escalation redlines, seamlessly aligning with the country's established strategic culture.

Pakistan's cyberwarfare doctrine has evolved in direct response to these external threat perceptions. The emphasis on intelligence-led operations, narrative influence, and deniable cyber activity reflects an attempt to navigate an environment characterized by technological asymmetry, attribution uncertainty, and persistent strategic rivalry. Understanding the external cyber threats Pakistan perceives is therefore essential for analyzing both its cybersecurity policies and its conduct during crises such as Operation Sindoor.

Pakistan's Cybersecurity Framework: Historical Development, Contemporary Efficacy, and Pathways to Enhancement

Pakistan's cybersecurity policy framework has developed slowly and unevenly, molded by external threat perceptions, persistent domestic capacity limitations, and entrenched civil military tensions. Although successive administrations have formally recognized cyberspace as a national security domain, policy evolution has consistently trailed the rapid growth of digital infrastructure and the accelerating proliferation of cyber threats. The result is a pronounced and enduring misalignment between stated ambitions and operational capability—one that materially weakens both defensive resilience and offensive cyber conduct.

The roots of Pakistan's cybersecurity policy lie in the early 2000s, when accelerating digitization of government services and financial systems prompted initial efforts at information technology governance. These measures remained predominantly economic and administrative, prioritizing e-governance and digital inclusion over security considerations. Cyber threats were largely dismissed as technical inconveniences rather than strategic vulnerabilities, and responsibility

for cyber matters scattered across civilian ministries with minimal coordination.[xx] This fragmented posture endured even as cyber incidents grew markedly more frequent and technically advanced.

A more explicit securitization of cyberspace emerged in the mid-2010s, driven by the rise of cybercrime, extremist online activity, and growing India–Pakistan tensions (After the 2008 Mumbai Attacks). Legislative measures such as the Prevention of Electronic Crimes Act (PECA) expanded the state's legal authority over cyberspace, particularly in areas related to surveillance, content regulation, and law enforcement. However, critics have argued that these measures prioritized control and compliance over technical defense, with limited investment in institutional capacity or public–private cooperation.[xxi] Cybersecurity during this period remained reactive, focused on policing online behavior rather than protecting networks and infrastructure.

The 2021 National Cyber Security Policy (NCSP) represented Pakistan's most ambitious effort to define a coherent national cybersecurity posture. The document prioritized protection of critical information infrastructure, human and institutional capacity building, development of indigenous technologies, and enhanced international cooperation.[xxii] It further called for sector specific standards and improved interagency coordination, aligning Pakistan on paper with prevailing global norms and formally acknowledging cyberspace as a strategic domain of national security.

Implementation, however, has proven markedly uneven. Institutional mandates remain fragmented, with persistent overlaps among civilian ministries, sectoral regulators, and security agencies. The National Centre for Cyber Security, tasked with advancing research and training, has achieved meaningful gains in academic partnerships but lacks the mandate, funding, and leverage required for effective nationwide coordination.[xxiii] Enforcement capacity differs sharply across regulators, and adherence to cybersecurity standards remains patchy across public and private sectors. These deficiencies substantially curtail the policy's impact during periods of elevated cyber risk.

Underlying civil military asymmetries further shape Pakistan's cybersecurity framework. Although formally positioned as a civilian governance responsibility, operational control and strategic direction in cyberspace have increasingly shifted toward military and intelligence entities, especially amid crises. This tilt entrenches a securitized paradigm that privileges surveillance, narrative management, and counterintelligence over systemic resilience and redundancy.[xxiv] Consequently, defensive investments consistently lag behind offensive and intelligence-oriented capabilities, particularly under resource scarcity.

Present-day relevance of Pakistan's cybersecurity policy must therefore be assessed against a backdrop of persistent vulnerability. Government advisories and industry reporting indicate that Pakistan continues to face millions of attempted cyber intrusions annually, targeting financial institutions, government databases, and telecommunications infrastructure.[xxv] Despite policy commitments to critical infrastructure protection, many systems rely on legacy architecture and imported technologies, increasing exposure to supply-chain and zero-day vulnerabilities. Cyber incident response mechanisms remain largely centralized and reactive, limiting adaptability during large-scale or coordinated attacks.

The events of **Operation Sindoor** in May 2025 underscored these policy limitations. While Pakistan demonstrated an ability to engage in cyber and narrative operations externally, its defensive posture appeared strained under sustained pressure. The contrast between offensive cyber activity and domestic resilience highlighted the structural imbalance embedded within Pakistan's cybersecurity framework. Rather than functioning as a robust shield, cybersecurity policy operated as a thin buffer, dependent on ad hoc measures and information control to manage escalation.

Looking ahead, Pakistan's cybersecurity policy faces several strategic choices. Incremental improvements in capacity building, public–private partnerships, and regulatory enforcement are likely, particularly as economic digitization deepens. International cooperation, especially with China and select regional partners, may help address technical

gaps, though it also raises questions about interoperability and dependence. However, absent significant institutional reform and investment, Pakistan is unlikely to achieve comprehensive “cyber resilience” in the near term.

Instead, the future trajectory of Pakistan’s cybersecurity policy is likely to remain defensive in language but limited in practice, functioning alongside a more agile and assertive cyberwarfare posture. This divergence reflects strategic prioritization rather than oversight. Pakistan appears willing to tolerate domestic cyber vulnerability while leveraging cyberspace as a tool of influence, signaling, and sub-threshold competition.

The Evolution of Pakistan’s Cyberwarfare Doctrine

Pakistan’s cyberwarfare doctrine has matured not through explicit declaration but via iterative practice, inference, and seamless integration into longstanding strategic patterns. Unlike states that promulgate formal doctrines or unveil dedicated cyber commands, Pakistan maintains deliberate opacity, that signals doctrinal absence only superficially. In reality, its cyber posture is emergent, intelligence driven, and deeply embedded in a hybrid, sub-threshold-warfare framework that prizes asymmetry.

Historically, Pakistan’s national security calculus has favored deniable, flexible instruments to counter India’s conventional superiority, from proxy militancy and covert operations to information campaigns.[xxvi] Cyberspace extends this tradition organically: low entry barriers, plausible deniability, and persistent operations below armed conflict thresholds enable sustained pressure on a stronger rival while tightly managing escalation risks.

Early evolution unfolded reactively. In the 2000s and early 2010s, Pakistan linked cyber activity centered on loosely coordinated hacktivist efforts, website defacements, symbolic disruptions, and nationalist messaging during bilateral tensions.[xxvii] Though rudimentary, these actions illuminated cyber’s psychological and signaling potential; state tolerance, paired with lax enforcement, hinted at nascent recognition of cyber as a cheap adjunct to political rivalry.

As global cyber capabilities advanced, Pakistan’s posture grew more deliberate yet remained informal. Analysts observe a transition from overt hacktivism to precise intrusion campaigns, espionage, and synchronized information operations.[xxviii] These efforts increasingly serve intelligence goals: adversary surveillance, political monitoring, and digital battlefield preparation during crises. This intelligence centric integration represented a doctrinal milestone, prioritizing information dominance and influence over outright destruction.

Narrative warfare stands as a hallmark. Pakistani strategic thought has long valued perception management; in cyberspace, this manifests through social media orchestration, selective leaks, and exploitation of misinformation channels.[xxix] Cyber actions thus function less as isolated technical strikes and more as force multipliers for comprehensive influence campaigns, treating the domain as cognitive terrain.

Escalation caution defines the approach. Eschewing doctrines of offensive cyber deterrence via massive disruption, Pakistan favors limited, reversible measures—espionage, defacements, leaks, disinformation, that impose costs and mold perceptions while preserving ambiguity on intent and attribution.[xxx]

Institutionally, cyber capabilities reside predominantly within military intelligence organs rather than civilian cybersecurity structures. Official documents emphasize defensive governance, but operational activity aligns with intelligence imperatives and crisis demands.[xxxi] This setup sustains opacity, impedes external analysis, and widens the gulf between resilience focused policy and agile, deniable cyberwarfare practice.

Comparatively, Pakistan diverges from India’s trajectory of formalized cyber commands, overt deterrence signaling, and joint operational integration. India projects visibility to deter; Pakistan, as the conventionally weaker actor, calculates

that ambiguity better preserves maneuver room.[xxxii]

Domestic constraints, fragile resilience, institutional fragmentation, foreign technology dependence, further channel the doctrine toward episodic, crisis tethered operations rather than sustained high intensity campaigns. In Pakistan's case, Cyberwarfare thus supplements rather than supplants other instruments.

Since 2020, Pakistan's cyberwarfare doctrine had coalesced around enduring principles: deniability over declaration, intelligence enablement over disruption, narrative primacy over technical supremacy, and escalation restraint over bold signaling. These tenets, though unwritten, manifest consistently across incidents. Operation Sindoor, emerged as the doctrine's most rigorous real-world examination, exposing both its adaptive strengths and inherent vulnerabilities under multidomain pressure.

Cyber-Operations during Operation Sindoor

The May 2025 India–Pakistan conflict, referred to as Operation Sindoor, represented the most intense bilateral crisis between the two states in recent years and marked a critical moment for cyber and information operations in South Asia. Alongside kinetic strikes, drone activity, and diplomatic signaling, both sides engaged in sustained cyber activity and narrative warfare. For Pakistan, Operation Sindoor functioned as a real-world test of its emergent cyberwarfare doctrine, revealing a preference for narrative dominance, deniable cyber actions, and crisis-linked operations rather than sustained, high-impact cyber disruption.

Narrative Dominance

Narrative warfare dominated as the most concerted and visible cyber enabled dimension of Pakistan's response. Linked information operations aggressively contested Indian narratives, amplified reports of civilian casualties, and projected unflinching resolve despite asymmetries in conventional power. Analysts documented swift, synchronized messaging surges across social media, timed precisely to kinetic developments and official pronouncements.[xxxiii]

These efforts targeted three core audiences: domestically, to bolster perceptions of resilience and deterrence efficacy; internationally, to underscore escalation perils and humanitarian imperatives while casting Pakistan as provocatively restrained; regionally, to muddy India's claims of battlefield dominance and sow interpretive ambiguity.[xxxiv] Beyond overt propaganda, selective dissemination of purported intrusion evidence, data leaks, and inflated success claims functioned as psychological instruments, prioritizing perceptual disruption over verifiability.[xxxv] This cognitive orientation aligns with Pakistan's doctrinal valuation of narrative effects above technical triumph, as witnessed throughout its military history. The best example being the bold headlines of 'War Till Victory' on the front page of the 'Dawn', published on December 17, 1971 after the Commander of Eastern Command, Lt gen A. A. K. Niazi had surrendered to Indian Forces in erstwhile East Pakistan.[xxxvi]

Limited Offensive Operations

Parallel cyberattacks proved more restrained in scope and consequence. Indian authorities and media alleged Pakistan affiliated actors mounted over one million intrusion attempts against government portals, critical infrastructure, and private platforms, though successful breaches remained marginal.[xxxvii] Cybersecurity assessments corroborated spikes in distributed denial of service assaults, website defacements, and exploratory probes of cloud assets.[xxxviii] Notably, Pakistan's Inter Services Public Relations offered no substantiation for asserted strikes on Indian military installations.

Analytically, the attacks' character outweighs their volume: predominantly disruptive rather than destructive, they prioritized symbolic signaling and visibility over enduring degradation. Such reversible tactics imposed psychological costs while steering clear of thresholds tied to infrastructure sabotage, consonant with Pakistan's emphasis on deniability and escalation restraint.

Attribution proved deeply contested. Indian attributions routinely implicated state backed entities, yet analysts highlight opportunistic exploitation by hacktivist collectives and cybercriminals.[xxxix] This confluence of state and non state activity generated profound ambiguity, a fog that strategically benefited Pakistan by sustaining deniability and attempting to complicate the adversary's retaliation calculus.

The conspicuous absence of sophisticated, sustained assaults on core military or infrastructure targets suggests deliberate restraint over capability deficits. In Pakistan's nuclear shadowed strategic culture, the former holds greater explanatory power: operations were meticulously calibrated to demonstrate intent without inviting spiraling escalation.

Cyber Resilience Shortfalls

Operation Sindoor starkly illuminated Pakistan's defensive frailties amid its offensive and influence activities. Pakistani networks endured probing and intrusion attempts, though official acknowledgments remained scant and controlled.[xl] This reticence accords with Pakistan's predilection for opacity in cybersecurity incidents, yet it also betrays underlying capacity constraints, legacy systems, imported dependencies, and disjointed response frameworks hampered effective mitigation under pressure.[xli]

As the crisis intensified, narrative substitution for technical resilience grew evident. Rather than heralding defensive triumphs, messaging pivoted to escalation framing and deterrence posturing. This short-term expedient, while tactically astute, masks persistent vulnerabilities and heightens long term strategic exposure.[xlii]

Doctrinal Insights

Operation Sindoor affirms Pakistan's cyberwarfare doctrine as crisis oriented and perception centric, eschewing dominance or paralysis in favor of signaling, ambiguity, and narrative enablement within hybrid frameworks. Limited, reversible cyberattacks coupled with vigorous information operations enabled digital visibility below escalation redlines, augmenting rather than supplanting conventional tools.[xliii]

Yet the crisis also exposed inherent limits. External cyber agility contrasted sharply with internal fragility, reinforcing doctrinal prioritization of influence and deniability over endurance. Operation Sindoor thus emerges as dual edged: a validation of Pakistan's adaptive, asymmetric approach in crises, and a sobering indictment of its unaddressed domestic liabilities in an increasingly contested domain.[xliv]

Conclusion

Pakistan's approach to cyberspace embodies a coherent strategic logic rooted in asymmetry, escalation awareness, and reliance on deniable power instruments. This analysis has shown that its cyberwarfare doctrine is emergent rather than codified, intelligence driven rather than centralized, and geared toward narrative influence and crisis signaling over disruptive dominance. The May 2025 Operation Sindoor crisis provides the strongest empirical confirmation of this posture.

Domestically, profound vulnerabilities, fragmented governance, limited capacity, and inconsistent implementation, undermine resilience.[xlv] These constraints drive doctrinal emphasis on low-cost offensive and influence activities,

widening the gap between defensive shortfalls and external intent.

Externally, India centric perceptions frame espionage and manipulation as enduring pressures, fostering reactive, crisis driven operations and strategic ambiguity over overt deterrence.[xlvi]

Pakistan's doctrine thus extends its hybrid warfare tradition: cyber tools prioritize intelligence, perception management, and escalation control, with narrative warfare treating the domain as primarily cognitive.

Operation Sindoor exemplified this: vigorous narrative campaigns and restrained attacks avoided escalation thresholds yet exposed internal frailties through muted defensive responses. This asymmetry defines inherent tradeoffs.

In South Asia's nuclearized context, such restraint signals risk awareness, but cyber ambiguity risks miscalculation absent shared norms. Pakistan's engagement reflects continuity,new tools integrated into a culture of deniability and sub-threshold-competition. Operation Sindoor affirmed this pattern, underscoring the need to understand it for anticipating regional cyber conflict and stability challenges.[xlvii]

Endnotes:

[i] Muhammad Riaz Shad, "Hybrid Warfare and Pakistan's Security Environment," Institute of Strategic Studies Islamabad, 2019, https://issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf

[ii] Irta Fatima, *Pakistan's Cyber Threat Landscape and Prospects of Regional Cooperation on Cyber Security* (Islamabad: Institute of Strategic Studies Islamabad, 2023).

[iii] Government of Pakistan, *National Cyber Security Policy 2021* (Islamabad: Ministry of Information Technology and Telecommunication, 2021), https://nccs.pk/

[iv] Economic Times, "Airspace to Cyberspace: How India Fought Swarms of Drones, Wave of Misinformation during Conflict," May 2025, https://economictimes.indiatimes.com/news/defence/airspace-to-cyberspace-how-india-fought-swarms-of-drones-wave-of-misinformation-during-conflict/articleshow/121165746.cms

[v] The News (Pakistan), "Cybersecurity Firm Points Out Seven Persistent Threats to Pakistan," 2025, https://www.thenews.com.pk/latest/1358006-cybersecurity-firm-points-out-7-persistent-threats-to-pakistan

[vi] Diplomatic Insight, "Pakistan Faced Over Five Million Cyber Attacks in 2025," 2025, https://thediplomaticinsight.com/pak-faced-over-5m-cyber-attacks-in-2025/

[vii] Khaama Press, "The Escalating Cybersecurity Crisis in Pakistan," 2025, https://www.khaama.com/the-escalating-cybersecurity-crisis-in-pakistan/

[viii] IJFMR, "Cyber Security Challenges in Pakistan: An Assessment," *International Journal of Finance, Management and Research* (2025), https://www.ijfmr.com/papers/2025/3/49846.pdf

[ix] Federal Board of Revenue (Pakistan), "Advisory No. 60: Cyber Attacks on Pakistan Critical Information Infrastructure," Government of Pakistan, 2021, https://download1.fbr.gov.pk/Docs/20219231293929303AdvisoryNo.60-CyberAttacksonPakistanCriticalInformationStructure.pdf

[x] National Centre for Cyber Security (Pakistan), "Home," accessed February 2026, https://nccs.pk/

[xi] U.S. Department of Commerce, International Trade Administration, *Pakistan – Cybersecurity*, Country Commercial Guide (Washington, DC, 2024), https://www.trade.gov/country-commercial-guides/pakistan-cybersecurity

[xii] Lockton, “The New Reality of Cyber-Physical Risks in Pakistan,” 2024, https://global.lockton.com/mena/en/news-insights/the-new-reality-of-cyber-physical-risks-in-pakistan

[xiii] Institute for Defence Studies and Analyses (IDSA), “Digital War: Pakistan’s Cyber Activity against India,” Issue Brief, 2025, https://idsa.in/publisher/issuebrief/digital-war-pakistans-cyber-activity-against-india

[xiv] CyberPress, “Transparent Tribe Targets Startups,” 2024, https://cyberpress.org/transparent-tribe-targets-startups/

[xv] Canadian Forces College, Yaqub, *Cyber Power and South Asian Security Dynamics* (Toronto: Canadian Forces College, 2022), https://www.cfc.forces.gc.ca/259/290/22/192/Yaqub.pdf

[xvi] ASSA Journal, “Cyber Conflict in South Asia: Trends and Implications,” vol. 36 (2024), https://assajournal.com/index.php/36/article/view/629

[xvii] PACIS / Universitas Katolik Parahyangan, *The New Chapter in India–Pakistan Rivalry: From Water Diplomacy to Cyber Attacks*, 2025, https://pacis.unpar.ac.id/the-new-chapter-in-india-pakistan-rivalry-from-water-diplomacy-to-cyber-attacks/

[xviii] The Stimson Center, *“South Asian Perspectives on Critical Cyber Threats, Law, and Norms,”* Stimson Center, September 16, 2025, https://www.stimson.org/2025/south-asian-perspectives-on-critical-cyber-threats-law-and-norms/

[xix] Stimson Center, “Cyber Quicksand? Uncharted Risks and Escalatory Dynamics in a Future India-Pakistan Crisis,” September 3, 2025, https://www.stimson.org/2025/cyber-risks-and-escalatory-dynamics-future-india-pakistan-crisis/

[xx] Government of Pakistan, *National Cyber Security Policy 2021* (Islamabad: Ministry of IT & Telecom, 2021), https://nccs.pk/

[xxi] Shahrukh Khan, “Cyber Security Challenges in Pakistan: An Assessment,” *Science Diplomacy Perspectives*, March 2022, https://www.researchgate.net/publication/360256123_Cyber_Security_Challenges_in_Pakistan_An_Assessment

[xxii] Government of Pakistan, *National Cyber Security Policy 2021* (Islamabad: Ministry of IT & Telecom, 2021), https://nccs.pk/

[xxiii] National Centre for Cyber Security (NCCS), Pakistan, https://nccs.pk/

[xxiv] Muhammad Riaz Shad, *Cyber Threat Landscape and Readiness Challenge of Pakistan*, Strategic Studies, Vol. 39, No. 1 (Spring 2019), 1-19, https://issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf

[xxv] Web Desk, “Pakistan Faced 5.3M On-device Cyber Attacks in Three Quarters of 2025,” *The Diplomatic Insight*, November 14, 2025, https://thediplomaticinsight.com/pak-faced-over-5m-cyber-attacks-in-2025/

[xxvi] Muhammad Riaz Shad, “Hybrid Warfare and Pakistan’s Security Environment,” Institute of Strategic Studies Islamabad, 2019.

[xxvii] ASSA Journal, “Cyber Conflict in South Asia: Trends and Implications,” 2024.

[xxviii] Varshini, “Transparent Tribe Targets India’s Startup Ecosystem in Renewed Cyber Espionage Campaign,” *Cyber Press*, February 10, 2026, https://cyberpress.org/transparent-tribe-targets-startups/

[xxix] The Stimson Center, *“South Asian Perspectives on Critical Cyber Threats, Law, and Norms,”* Stimson Center, September 16, 2025, https://www.stimson.org/2025/south-asian-perspectives-on-critical-cyber-threats-law-and-norms/

[xxx] Stimson Center, “Cyber Quicksand? Uncharted Risks and Escalatory Dynamics in a Future India-Pakistan Crisis,” September 3, 2025, https://www.stimson.org/2025/cyber-risks-and-escalatory-dynamics-future-india-pakistan-crisis/

[xxxi] Yaqub, *Cyber Power and South Asian Security Dynamics*. Canadian Forces College, 2022. https://www.cfc.forces.gc.ca/259/290/22/192/Yaqub.pdf

[xxxii] Sameer Patil, “From Missiles to Malware: India-Pakistan Cyber Rivalry and Lessons for Taiwan,” *Taiwan Insight*, July 22, 2025, https://taiwaninsight.org/2025/07/22/from-missiles-to-malware-india-pakistan-cyber-rivalry-and-lessons-for-taiwan/

[xxxiii] Times of India (Hyderabad), “Operation Sindoor: As Pak Drones Took to Skies, Hackers Attacked India via Cloud,” May 2025, https://timesofindia.indiatimes.com/city/hyderabad/operation-sindoor-as-pak-drones-took-to-skies-hackers-attacked-india-via-cloud/articleshow/121146853.cms

[xxxiv] New Indian Express, “15 Lakh Cyber Attacks on Key Locations by Pakistan Hackers,” May 14, 2025, https://www.newindianexpress.com/nation/2025/May/14/15l-cyber-attacks-on-key-locations-by-pakistan-hackers

[xxxv] Economic Times, “Pakistan-Allied Hackers Launched 1.5 Million Cyber Attacks on Indian Websites — Only 150 Successful,” May 2025, https://economictimes.indiatimes.com/news/india/pakistan-allied-hackers-launched-15-lakh-cyber-attacks-on-indian-websites-only-150-successful/articleshow/121125557.cms

[xxxvi] Smita Prakash (@smitaprakash), X, *March 5, 2021*, https://x.com/smitaprakash/status/1339243630544838663

[xxxvii] Business Standard, “Cyberwarfare Signs Govt on High Alert, Urges Industry to Boost Security,” May 16, 2025, https://www.business-standard.com/industry/news/cyberwarfare-signs-govt-on-high-alert-urges-industry-to-boost-security-125051601531_1.html

[xxxviii] Cyfirma, *Firewalls and Frontlines: The India–Pakistan Cyber Battlefield Crisis*, 2025, https://www.cyfirma.com/research/firewalls-and-frontlines-the-india-pakistan-cyber-battlefield-crisis/

[xxxix] Radware, “Escalating Hacktivist Attacks Amidst India–Pakistan Tensions,” 2025, https://www.radware.com/security/threat-advisories-and-attack-reports/escalating-hacktivist-attacks-amidst-india-pakistan-tensions/

[xl] Radware, “Escalating Hacktivist Attacks Amidst India–Pakistan Tensions,” 2025, https://www.radware.com/security/threat-advisories-and-attack-reports/escalating-hacktivist-attacks-amidst-india-pakistan-tensions/

[xli] Swadeshi Shodh, “Operation Sindoor: A Narrative Warfare Lens,” 2025, https://swadeshishodh.org/operation-sindoor-a-narrative-warfare-lens/

[xlii] BASIC, “Two Rivals, One Crisis: A War of Narratives,” 2025, https://basicint.org/two-rivals-one-crisis-a-war-of-narratives/

[xliii] Center for Aerospace Power & Strategic Studies (CAPSS India), *Cyber Warfare: Dual Operational Fronts in Contemporary India–Pakistan Conflicts*, 2025, https://capssindia.org/cyber-warfare-dual-operational-fronts-in-contemporary-india-pakistan-conflicts/

[xliv] War on the Rocks, “Deep Learning from Operation Sindoor: Five Takeaways from a Four-Day War,” January 2026, https://warontherocks.com/2026/01/deep-learning-from-operation-sindoor-five-takeaways-from-a-four-day-war/

[xlv] War on the Rocks, “Deep Learning from Operation Sindoor: Five Takeaways from a Four-Day War,” January 2026, https://warontherocks.com/2026/01/deep-learning-from-operation-sindoor-five-takeaways-from-a-four-day-war/

[xlvi]Mrs. Gowri R, “Cyber Frontier: India’s Strategic Leap in Cyberspace,” *CAPSS InFocus*, August 25, 2025, https://capsindia.org/cyber-frontier-indias-strategic-leap-in-cyberspace/

[xlvii] Centre d’Histoire et de Prospective Militaires (CHPM), *Operation Sindoor: The India-Pakistan Air War (7-10 May 2025)*, January 15, 2026, https://chpm.ch/wp-content/uploads/Operation-SIndoor-15-January-2026.pdf

The views expressed are those of the authors and do not represent the views of CNAWS.

Image Source: Gemini