Pakistan Journal of Applied Social Sciences
Vol. 17(1), 2026, pp.17-43, ISSN: 2409-0077(Print), ISSN: 2663-8894(Online)

Emerging Technologies and the Future of Strategic Stability in South Asia: Indo-Pakistani Deterrence, Multi-Domain Conflict, and Crisis Governance

Shanzay Saeed
Cardiff University, Cardiff, Wales, United Kingdom
Corresponding Author: shanzaysaeed01@gmail.com

Dr Farhat Konain Shujahi
IR Department
National University of Modern Languages (NUML).

Prof. Dr. Ahmed Saeed Minhas
DHA Suffa University, Karachi, Pakistan

ABSTRACT

Warfare has dramatically evolved in the last ten years. The emergence of Artificial Intelligence, Autonomous Weapon Platforms, and Cyber and Space-based Surveillance Systems has all helped to reduce the decision-making time of political and military leaders. In the world of milliseconds, there is not a lot of time to think, and a higher chance of getting it wrong. These pressures are much more likely to affect the South Asian strategic theatre, in which nuclear arsenals overlap, the boundaries remain unresolved, and the channels of crisis communication are historically narrow. These dynamics came into stark contrast during the Indo-Pakistani conflict in May 2025, which showcased a level of integration in multi-domain operations that both provided an effective military outcome and created new escalation avenues. The focus of this article is on the convergence of emerging technologies, information warfare and societal resilience and its impact on deterrence stability and crisis governance dynamics between India and Pakistan. It contends that to achieve sustainable peace in the region, not only do military balances need to be considered credible, but also the governance of dual-use technologies, the establishment of institutionalized crisis communication processes and public resilience to disinformation. The study is qualitative, analytical and is based on primary documents, strategic literature and the latest empirical events.

Keywords: Emerging Technologies, Artificial Intelligence, Strategic Stability, Multi-Domain Warfare, Deterrence Dynamics.

1. INTRODUCTION

South Asia is one of the most strategically vulnerable regions in the world. More than seven decades of competitive military posturing, four conventional wars, and a series of crisis situations with the potential to test the limits of deterrence stability have emerged as a result of the India-Pakistan rivalry that began with the violent partition of British India in 1947 and has been fueled by the unresolved

This work is Licensed under a Creative Commons Attribution-Non Commercial 4.0 International License

status of Jammu and Kashmir (Council on Foreign Relations, 2026; Noor, 2023). This rivalry is more than just one more interstate conflict: It is intertwined with a historical grievance, incentivized by domestic political pressures, and, since 1998, has always had the potential of being nuclearized.

The May 1998 nuclear tests by both countries did not change this situation, but added a new layer of danger to an already fragile base. There were many confidence-building measures taken, most importantly the Lahore Memorandum of Understanding of 1999 and the bilateral agreement on advance notification of ballistic missile tests signed in 2005, which recognized the need for structured communication between countries due to their mutual vulnerability (Arms Control Association, 1999; Ali & Sidhu, 2022). However, institutional constraints have not always been able to keep pace with political pressure, and the instruments that are supposed to avoid miscalculation have been tried many times and have proven to be inconsistent in their effectiveness.

In this context, new challenges are emerging in the strategic landscape, which are shaking both sides to their very core. The development of artificial intelligence is rapidly increasing information processing and decision support. The autonomy of systems is expanding military presence, but decreasing human presence. Cyber operations are moving further towards the active attack side of the equation versus collection. Space-based assets are delivering battlefield awareness, on the fly, at miles and miles and miles and miles and miles and miles and miles and miles and miles and miles per minute. Combined, these technologies are shortening the timeframes for decisions over the entire conflict value chain (USIP, 2022; Sandia National Laboratories, 2021). This squeeze, which comes at a time of mounting fear and under-resourced situations, adds qualitatively new risks of inadvertent escalation.

These dynamics were first tested on a large scale in the May 2025 India-Pakistan conflict in South Asia with an empirical test. It proved that the new regional conflict today is no longer just a game of artillery but a simultaneous clash in physical, digital, informational and cognitive spaces. It also showed that deterrence is still relevant, but a less robust and more contingent one, and more reliant on the capacity of governance than was previously thought (Akhtar & Mahmood, 2025; Hussain, 2025).

This article examines the implications for strategic stability of this change. It is structured in sections covering the scope of the study, the problem addressed, the research questions and objectives, a structured literature review, the theoretical framework, empirical analysis of four thematic areas, discussion of findings, limitations of the study, policy recommendations and conclusion.

1.1. Scope of the Study

The study emphasizes the Indo-Pakistani strategic relationship since 1998, and the analysis of this relationship was based on events from 2020 onwards, when the emerging technologies started playing an operational role rather than being prospective. The geographical area covered is South Asia, with the main units of analysis being India and Pakistan. China is recognized as a key contextual actor, but not as a central subject, especially with respect to India's trilateral nuclear context.

The technological scope covers the following areas: Artificial intelligence and automated decision support systems, Autonomous weapons platforms (UAS, loitering munitions), Offensive and defensive cyber capabilities, Space intelligence, surveillance, reconnaissance and communications capabilities and Quantum technologies in emerging military applications. The study does not include biological, chemical, or radiological weapons and is not as detailed regarding conventional force procurement.

The main analytical field is strategic and politico-military. The tactical and operational aspects of the conflict of May 2025 revolve around issues that enlighten the larger deterrence picture rather than being the focus of the discussions themselves. Economical, humanistic and legal aspects of the Indo-Pakistan rivalry are significant but beyond the scope of the study and only mentioned when relevant to the discussion of strategic stability issues. The study is not quantitative, nor does it create quantitative escalation models or statistical projections.

1.2. Rationale

There are three interrelated observations that underlie the rationale of this study, with regard to the state of knowledge and policy in South Asian security today.

The current academic research on deterrence from South Asia was predominantly developed prior to the operational deployment of AI-powered military systems, multi-domain doctrines and large autonomous platforms. The seminal works by Bajpai et al. (1995) on the Brasstacks crisis management, Ganguly and Hagerty (2005) on the recurring pattern of nuclear-shadowed crises, and Noor (2023) on evolving strategic stability challenges were written in a technological environment qualitatively different from the one that produced the May 2025 conflict.

While Topychkanov's (2020) analysis is an important early contribution to deterrence theory applied to the risks from AI in South Asia, the recent rise of large-language-model AI, loitering munitions, and operationally deployed autonomous

systems has largely already preempted the analytical scope of his work. Therefore, it is time for a new systematic scholarly update, based on the empirical evidence since 2025.

Second, the Indo-Pak crisis of May 2025 generated a considerable volume of primary material in the form of operational analyses, reports from institutions, official statements, and think tank evaluations, which are yet to be synthesized into an academic narrative of the implications of the crisis in terms of deterrence. Early operational and institutional analyses have been undertaken by ISFP (2025), the Sanober Institute (2025), Ghalib (2025), Stratheia (2025) and Akhtar (2025), which is the most comprehensive multi-author analysis on deterrence and escalation post-Pahalgam to date. None of these sources is a theoretically informed qualitative synthesis that places the crisis of May 2025 in the broader context of the deterrence stability literature and multi-domain warfare and technology governance. The pace of events and the amount of new commentary make it a risk that key empirical signals will get lost in the partisan or journalistic commentary. This study does just that: It is a structured academic synthesis.

Thirdly, the regulatory lacuna between technological capacity and standards is growing at an increasing rate, with actual implications for South Asian security. While Haider and Azad (2021) trace the gradual development of bilateral confidence-building measures until 2021, they fail to mention any mechanisms that are deemed to be sufficient for the risks posed by the cyber and AI-related crisis. In both cases, Klare (2023) and Paoli (2025) argue that there are equally glaring gaps between international standards on autonomous weapons and military AI and the rate of deployment. In dyads, geographically tightly coupled decision timelines and a lack of crisis communication infrastructure are especially lacking, as noted by Lin and Trinkunas (2026). Bilateral India-Pakistan CBM architecture and multilateral arms control regime are not intended for addressing the dynamics of escalation across various domains, offensive cyber operations targeting nuclear command systems and AI-enabled targeting. Analysis of this gap is thus directly policy-relevant, and concrete governance recommendations can be articulated from it; the authors place this analysis in the nexus of academic knowledge production and of applied policy relevance.

1.3. Problem Statement

The relationship between the two nuclear-armed states in South Asia has hitherto been highly volatile, with limited margins of error, poor crisis communication mechanisms and domestic politics that incentivize signaling of confrontation over caution (Noor, 2023; Ali & Sidhu, 2022). The structural imbalance between the conventional superiority of India and Pakistan's nuclear compensation has constantly encouraged crisis behavior at low levels of the escalation ladder, as Khan (2015) describes it: a situation of mutual vulnerability

and not strategic balance. The integration of new technologies such as AI, autonomous weapons systems, cyber capabilities and space assets into both states' military strategies and operations further exacerbates this fragility (USIP, 2022; Sandia National Laboratories, 2021; Hussain, 2025).

These technologies create three types of destabilizing risk not anticipated by current deterrence strategies and crisis-management processes. The first is the compression of decision time – AI-driven systems can come up with targeting suggestions and start a sequence of responses quicker than political leadership can engage in meaningful decision-making, leaving decision room to de-escalate to minutes or seconds (Raska, 2025; Klare, 2023). The second is the opacity issue – because of the structural nature of AI, cyber, and space capabilities, it is hard in their dual-use nature to distinguish between defensive preparations and offensive ones; between intelligence gathering and attack precursors; and between technical failure and deliberate provocation (Acton, 2020; Manning, 2020). The third is the issue of information integrity: artificial intelligence-generated disinformation, the manipulation of narratives and the compromise of military data systems could pose threats to the informational base of those signaling actions that are important for deterrence (Abbasi & Uzzaman, 2022; Arshad & Sheik, 2022; Farooq & de Vreese, 2025).

The May 2025 situation proved these fears were not imaginary as multi-domain operations, information warfare and AI-manipulated systems were clearly seen in the evolution of the conflict and eventual containment (Ghalib, 2025; Abid & Bano, 2025; Akhtar & Mahmood, 2025). However, the post-crisis era has witnessed the continuation of escalatory rhetoric, the politicization of water resources by a violation of the Indus Waters Treaty (Ahmad, 2025; Banerji & Sitaraman, 2025) and no new bilateral arrangements for the management of new risks of multi-domain conflict (Haider & Azad, 2021; Raeesa & Akhtar, 2025). Paoli (2025) and Klare (2023) each argue that the lack of governance structures that keep up with the rate of new technology adoption is also a source of strategic instability. It is a central problem in this research that in a technology-dominated world where decision space is systematically reduced, and the information underpinning deterrence is increasingly undermined, what conditions are needed for strategic stability to be preserved in South Asia and what governance mechanisms are needed to put these conditions in place?

1.4. Research Questions

This study is organized around the following research questions:

1. In what ways are AI/AS/Cyber/Space based capabilities single-handedly or together changing the Deterrence landscape between India and Pakistan?

2. How is the information domain becoming a strategic field of play, and what impact do disinformation and data integrity issues have on the stability of crises in South Asia?

3. What does the India-Pakistan conflict in May 2025, and in particular Pakistan's Operation Bunyan-un-Marsoos, say about the doctrine and practice of Multi-Domain Deterrence in South Asia?

4. What are the required governance mechanisms and which ones are bilateral, regional and multilateral, in order to ensure that the risks of escalation arising from new technologies in a nuclear-armed dyad are being managed?

1.5. Research Objectives

- To understand the impact of artificial intelligence, autonomous weapons, cyber operations, space systems and quantum technologies on both India's and Pakistan's deterrence stability.

- To analyze the strategic dimensions of Information Warfare, Disinformation and Data Integrity issues in the Indo-Pakistan security scenario in the context of the crisis of May 2025.

- To analyze Pakistan's multi-domain operational response in the context of Operation Bunyan-un-Marsoos (BUM), as a case study of technology-based deterrence practice, its doctrinal importance and implications for future crises.

- To find out the lapses in the existing bilateral confidence-building mechanisms, regional security architecture and international arms control mechanisms in the context of new military technologies in South Asia.

- To develop policy recommendations based on evidence for regional governments, international institutions and multilateral platforms to enhance crisis communications, technology management and societal resilience in South Asia.

2. LITERATURE REVIEW

2.1. Classical Deterrence Theory and Its South Asian Applications

Strategic stability has been conceptualized through the foundational literature on nuclear deterrence, which was developed mainly in the context of the Cold War nuclear superpower competition. Deterrence, according to Freedman (2004), is the message of a credible threat to impose unacceptable costs on an opponent who is considering taking hostile action. Acton (2020), building on this

framework, examines the ways in which new technologies can undermine the credibility of these threats by adding ambiguity, speeding up decision-making and affording opportunities for unintended escalation. The key elements of deterrence instability were laid out in the basic empirical scholarship in the South Asian context: the Brasstacks crisis (Bajpai et al., 1995) and the recurring pattern of Indo-Pakistani crises (Ganguly & Hagerty, 2005).

Noor (2023) gives the latest detailed analysis of South Asian strategic stability, which suggests that the post-2019 era has witnessed the deterioration of the qualitative elements of deterrence due to a series of changes in Indian doctrine, Pakistani compensatory responses, and the rising importance of sub-conventional warfare. Ali and Sidhu (2022) provide an alternative perspective where they have highlighted the structural importance of conventional asymmetry in creating Pakistani escalatory incentives in the context of the dynamics of crisis stability. Hussain (2025) brings these judgments up to date by adding the 2025 crisis, suggesting that nuclear deterrence has been more decoupled from conventional escalation management than ever before, thus raising inadvertent war risks.

2.2. Emerging Technologies and Strategic Stability

Since 2018, the amount of literature on emerging technologies and strategic stability has increased significantly, as these new military systems are rapidly deployed in major-power settings. The most recent full synthesis is the one by Lin and Trinkunas (2026), which identifies four types of stability threats stemming from emerging technologies: the kill chain and its acceleration, ambiguity in terms of dual-use, the possibility of autonomous escalation, and degradation of the informational commons. However, Klare (2023) narrows the discussion to the nuclear aspect of the threats, explaining how artificial intelligence-powered systems that would strike nuclear delivery platforms would create first-strike incentives even among states that have signed no-first-use agreements.

The first systematic analysis of the role of AI in strategic stability in South Asia as a whole was authored by Topychkanov (2020), with contributions from both Indian and Pakistani analysts and international scholars. His collection has laid bare the unique sensitivity of South Asian deterrence, given the proximity between the two countries, the lack of a well-developed hotline system and the politicized information landscape, in which both states operate. The last comprehensive review of this literature is provided by Paoli (2025), which includes the implications of the use of large-language model AI and next-generation autonomous systems for nuclear escalation risk.

In Raska (2025), Raska discusses how the OODA loop is now facilitated by AI and how this change has steadily diminished the need for political judgment in crisis management. This is of special significance to South Asia, where a long-

standing limitation to escalation has been the political control of military activities. Giordano (2026) discusses the ongoing body of theory on quantum technologies, which will change the strategic landscape in ways that are not yet fully understood and has already raised destabilizing hedging incentives.

2.3. Information Warfare and Disinformation in Security Contexts.

The operational use of AI-generated content has been accompanied by a fast-growing strategic literature on information warfare. The operational use of AI-generated content has been accompanied by a fast-growing strategic literature on information warfare. Van Niekerk (2021) offers a doctrinal explanation for the use of information warfare as a component of multi-domain warfare, claiming that information effects are as important as kinetic effects. Benincasa (2023) examines international legal aspects of AI-driven disinformation and outlines the need for a more robust framework to regulate state-sponsored disinformation operations.

Farooq and de Vreese (2025) offer the latest systematic overview of the use of generative AI in disinformation production, which has seen the scale and cost of fake information plummet with the growth of recent AI systems. Fournier-Tombs et al. (2023) explore how AI-powered disinformation can exacerbate conflict, noting patterns in which misinformation acts as a tool to reduce the political decision space that can help ease conflict. Given the context of South Asia, Qasim and Alvi (2026) highlight the use of disinformation as a foreign policy tool in Indo-Pakistani relations and its impacts on bilateral peace processes. Abbasi and Uzzaman (2022) link these information security issues to the larger issue of strategic stability and suggest that informational resilience should now be considered part of deterrence.

2.4. Multi-Domain Operations and the May 2025 Crisis

The literature of multi-domain operations in South Asia, to date, is still a work in progress, largely owing to the events of May 2025. In Bunyan-un-Marsoos, Pakistan's operational approach, Ghalib (2025) presents the first systematic analysis of the conflict, with the argument that it proved multi-domain deterrence could be used as a compensatory measure to counter conventional force asymmetry in the war. The Sanober Institute (2025) provides a more general evaluation of the deterrence implications of the conflict; Stratheia (2025) explores escalation control mechanisms and the effectiveness of these mechanisms during the crisis.

From a European analytical point of view, Trembeczki (2025) draws four lessons from the conflict: the influence of precision weaponry, autonomous platforms and information operations on the results. In the recent crisis of May 2025, Abid and Bano (2025) explore how human factors are essential in AI-driven military decision-making, highlighting the opportunities as well as risks of AI-

supported command systems. As the first edited volume on the May 2025 crisis, Akhtar (2025) brings together various analytical strands on deterrence and escalation management, which are discussed after the crisis in the aftermath of Pahalgam. Kayani, Ashraf and Shahid (2026) evaluate Pakistan's deterrence posture in the wake of the war and highlight its salient features and structural weaknesses that became apparent during the war.

2.5. Crisis Management and Confidence-Building Measures

A thorough review of literature on Indo-Pakistani crisis management and CBMs provides a valuable background for assessing the current governance shortfalls. After examining the development of bilateral CBMs from the 1988 agreement on attacks against nuclear installations to the 2005 ballistic missile notification protocol, Haider and Azad (2021) conclude that there has been incremental progress followed by periods of stagnation or even regression. In this section, Raeesa and Akhtar (2025) examine the coercive diplomacy aspect of the India-Pakistan security dilemma, emphasizing that structural incentives for crisis behavior are present due to the asymmetry in coercive force capabilities that can only be addressed by a combination of CBMs and other measures.

Sood (2022) speaks about the nuclear trilemma of China-India-Pakistan, suggesting that bilateral CBMs are not enough in a trilateral strategic landscape and that India's nuclear ties with China have direct, yet indirect impacts on the India-Pakistan deterrence balance. Banerji and Sitaraman (2025) explore the new dimensions of terrorism, water security and military conflict in the South Asian relationship and flag how conventional crisis management mechanisms fall short of addressing new pathways of escalation. The underlying deficiency that has consistently been identified in the literature is that governance processes are much further behind in terms of technological developments and the nature of South Asian conflict.

3. THEORETICAL FRAMEWORK: TECHNOLOGY, DETERRENCE, AND STRATEGIC STABILITY

In the traditional sense, strategic stability is a state where neither side in a nuclear competition sees an advantage in engaging in a war, nor in acting first in an emerging crisis (Acton, 2020). This concept includes the concept of arms-race stability (no reasons to increase arsenal in order to change the strategic balance) and crisis stability (no reasons to strike first during confrontation). In the past decades, the strategic stability of South Asia has been analyzed mostly in terms of the second-strike capability survivability, threat credibility and command and control arrangements.

This structure is still needed, but it's not enough. Classical deterrence theory has not been equipped to deal with the dynamics brought on by emerging technologies (Lin & Trinkunas, 2026). There are three aspects of these technologies that are especially relevant to stability.

The first is that new technology is dramatically quickening the tempo of conflict. An AI-driven system can analyze sensor data, come up with targeting solutions, and suggest what to do with them in far less time than it takes a human decision-maker to keep up with. A military commander who thinks that an enemy system is already preparing for an attack has a strong reason to take a pre-emptive action even if the intelligence that they have is ambiguous (Klare, 2023; Topychkanov, 2020).

Second, many new technologies are of a dual-use nature, that is, the same capability can be used in defense, offense or intelligence without the adversary being able to distinguish. A cyber attack on an enemy's air-defense network might be a precursor to an attack or just a signal-intel mission. It undermines the interpretive clarity that deterrence needs: no one can interpret the other side's signal well if it is not clear. It compromises the interpretive clarity that deterrence requires: Deterrence requires a reasonable degree of clarity on both sides (Manning, 2020).

Thirdly, there's the possibility of incidents that escalate beyond the control of either of the parties. Spawning, hacking, and simple failure of loitering munitions, drones, and robotic platforms can have lethal consequences without any political will (Klare, 2023). In South Asia, where the reaction time is measured in minutes, an autonomous incident may lead to a chain of reactions without the consultation of the political leadership.

Multi-domain operations are a potentially valuable analytical framework to complement deterrence theory: the deliberate synchronization of military effects over the land, sea, air, cyber, space, and information domains will yield cumulative effects that will not be achieved through any single domain (Ghalib, 2025).

4. EMERGING TECHNOLOGIES AND STRATEGIC STABILITY: CONVERGENCE AND CONSEQUENCE

4.1. Artificial Intelligence and Automated Decision Support

Artificial intelligence (AI) is the most consequential technology of the moment to affect strategic stability. Artificial intelligence (AI) is the technology of the moment that is most likely to impact strategic stability at the moment of decision. Today's military AIs analyze enormous volumes of sensor data, such as radar returns, signal intercepts, satellite images and social media surveillance and combine that into analyses to guide and sometimes trigger a response. The appeal

in the way that AI works is self-evident: it lightens the load on the commander in an information-rich environment and shortens the kill chain in ways that give a tactical edge.

The risks to strategy are of a like magnitude. In a crisis, AI systems work for the goals they are designed to meet, which can sometimes not align with the political priorities of the civilian leadership. Furthermore, violent activities may be confused with peaceable ones, either by AI systems through recognition of false radar signatures or by introduction of false targets (Paoli, 2025; Raska, 2025). In the South Asian context, the OODA loop can be shortened to the extent that the political leaders ratify what is already happening, instead of initiating it. The distances between nuclear assets in this theatre are very short, providing almost no opportunity for human review between the generation of the threat and the employment of nuclear weapons.

4.2. Autonomous Weapons Systems and Escalation Risk

The nature of tactical engagements is changing with autonomous systems such as drone swarms, loitering munitions and remotely operated naval platforms. They do have military uses, as they increase the field of view for surveillance, lower the risk to personnel, and can be used in a very contested environment. During the May 2025 crisis, the use of these systems by several entities highlighted their increasing use in operational planning on both sides of the LOC. That's the same with their role in strategic instability. A system without much human-in-the-loop control can make a lethal decision on the basis of inputs from sensors that would have provoked concern in a human operator. It can be acquired and then programmed by an enemy, or it can malfunction and create kinetic effects close to nuclear facilities. All these cases may trigger an escalatory reaction that the triggering party did not intend or foresee (Klare, 2023). With already high suspicion between actors in a dyad, autonomous weapons bring risks that do not have a strong enough deterrent.

4.3. Cyber Operations and Command-and-Control Vulnerability.

Perhaps the most structurally destabilizing of the new technologies are cyber capabilities, if one considers that their main targets are those systems on which deterrence relies: communication networks, radar systems, command-and-control infrastructure. A compromised early-warning system in a degraded state could leave a state with no way to tell if the warning was a real attack or simply a glitch. A state that suffers from disruption of command and control networks might not be able to confirm orders sent or transmit them to nuclear forces (Haider & Azad, 2021).

These risks are complicated by the attribution issue. A cyber attack is not like a traditional strike, and you won't find a hard-to-ignore trail of debtors or traders. State-sponsored attacks can go through third-country infrastructure. Non-State actors can carry out operations attributed to other governments. If there are already enough reasons to suspect that attribution is likely an incorrect conclusion, the urge to believe that the situation is caused by the most dangerous possible thing, due to time pressure, will be overwhelming in a crisis that already has time pressure and mutual suspicion. Examples of Pakistan's experience of disinformation campaigns purporting to have compromised its nuclear facilities show the real-world harm of unverified cyber-adjacent narratives to crisis management (Shah, 2009; Khan, 2012).

4.4. Space Assets and Real-Time Battlefield Transparency (RTBT)

India and Pakistan have both grown their space-based capabilities, enhancing their intelligence, surveillance, reconnaissance and navigation support for multi-domain operations. They are also becoming increasingly strategic targets due to their ever-increasing military role. A state that is thinking of attacking an enemy's space assets before they attack its own may estimate that such a blow would be debilitating to the integrated operations. It could also be seen as a precursor to a conventional attack or a nuclear attack by a state that thinks it is being harmed by the interferer's space systems. The weaponization of the space domain thus adds an additional dimension of unintentional escalation to an already complicated situation of stability (Giordano, 2026).

4.5 Quantum Technologies and the Emerging Horizon

Quantum technologies are still in the early stages of military use, but they are gaining a lot of interest in their strategic applications. Current encryption standards are at risk of being compromised by quantum computing, which could give an advantage to a quantum adversary in accessing secure military communications. The effectiveness of stealth platforms may be curtailed by quantum sensing. If reliable, quantum communication channels could be used to create new types of secure crisis hotlines (Giordano, 2026). In the context of deterrence relationships, the threat of a change in capabilities in the future can lead to the creation of present instability because states try to position themselves in a better way in anticipation of the change.

5. THE INFORMATION DOMAIN AS A STRATEGIC BATTLEFIELD

The information domain has undergone a complete transformation in scope and pace that to call it a “facilitating” domain of military operations is to concede it is not. The current conflict is characterized by the war's shapeability of perceptions, its narrative control and its protection of the informational foundations

of decisions; a war that is continuous, borderless, and without the formal signaling of the beginning of the conflict, as is traditionally associated with the perception of war (van Niekerk, 2021; Benincasa, 2023).

5.1 The Structural Dynamics of Disinformation

Today's societies are situated in a highly networked digital communication society where information is moving at a greater speed than the verification process. Fact-checking and correction processes are rarely handled by institutions on a timescale of seconds or minutes, and are not done by social media platforms that routinely deliver content to millions of people in a flash. This imbalance makes it conducive to the dissemination of disinformation (Qasim & Alvi, 2026). Today, generative AI can create convincing text, fake images, generated sound, and even synthetic video that can be difficult for more technologically advanced audiences to distinguish from the real (Farooq & de Vreese, 2025; Fournier-Tombs et al., 2023). The strategic payoff is a gradual erosion of the informational commons that underlie the signaling process that is relevant to deterrence.

5.2. Disinformation and Crisis Escalation in South Asia

Strategies that both states use are highly politicized and infested with information, and military crises turn into partisan competitions. A fake video, bogus allegation of a territorial invasion or bogus declaration by the leadership of the terrorists can create demands for retaliation even before the event is confirmed (Qasim & Alvi, 2026). In the case of Pakistan, Operation Rah-e-Raast has been instructive as disinformation campaigns were carried out to spread false claims that the Taliban were close to capturing the country's nuclear facilities, which were clearly aimed at eroding trust in the government within the country (Khan, 2012; Shah, 2009). In response, information resilience, defined as the ability to detect, de-escalate and counter disinformation campaigns, has been incorporated into deterrence stability (Abbasi & Uzzaman, 2022).

5.3. Data Integrity and the Foundations of Military Decision-Making

In the private sector, data integrity is now an important business and competitive concern. For military command and control, early-warning networks, and targeting databases, it is essential that information be transmitted without corruption and in an accurate way. The adversary can cause false data to be created, such as false targets, obfuscating actual troop movements, and creating false signs of incoming strikes, triggering responses to events that are not actually happening (Arshad & Sheik, 2022). The compromise of data integrity strikes at the core of strategic stability in South Asian where the data integrity is measured in minutes and the conventional-nuclear threshold is challenged.

6. THE NUCLEAR CENTRIC STRATEGY STABILITY IN SOUTH ASIA.

6.1. Deterrence under Asymmetric Conditions

South Asian strategic stability remains essentially nuclear, albeit with significant changes in the character of the nuclear core since 1998. The two are capable of sustaining second-strike capacity, but the relationship between the two states is also structurally asymmetric, which has been a challenge to stability in the past (Sood, 2022). India's traditional military edge makes it easy to assume that non-nuclear operations are still a tool of coercive diplomacy. The structural incentives in Pakistan, on the other hand, are more encouraging for reducing nuclear threshold in order to discourage such operations. The result has been a deterrence posture in which Pakistan has adopted a first use policy and tactical nuclear arsenal that is meant to prevent a conventional attack by India from being quick enough on the rise to evade Pakistani response.This has created an environment of deterrence where Pakistan has adopted first use policy and tactical nuclear arsenal with a view to denying space for a rapid conventional incursion by India (Khan, 2015). The stability that emerges is far less robust than the symmetric deterrence that it would be on the basis of mutual recognition of catastrophic risk.

6.2. The Fragility of Domestic Politics, Misperception and Deterrence

One peculiar aspect of South Asian deterrence is that it gets caught up in domestic politics. Political pressures facing leaders have a significant influence on crisis behavior, while the psychological motivation of leaders to look tough in the face of perceived provocation has a significant influence on their crisis behavior (Xiaolian, Siraj & Din, 2024). The Indian side's post-crisis escalation rhetoric is characteristic of a political landscape that encourages aggressive rhetoric for electoral gain and the use of restraint as weakness. It's a matter of public communication in the domestic political arena to convey a signal of preparedness to resume operations; public statements by senior Indian military leadership are representative of how domestic political communication can add an escalatory element to an already fragile deterrence dynamic. In Pakistan, the nuclear deterrent is viewed as an assurance of non-negotiable survival in the absence of any other security measures, thus adding a layer of sensitivity to deterrence signaling over any real threat to perceived sovereignty. The spiral of rhetoric and nuclear signaling, on the one hand and, on the other, is self-propelling and structurally hard to stop (Zaman, 2025; Bajpai et al., 1995).

6.3. Escalation Pathways in the Technology-Infused Environment

With the arrival of emerging technologies, there are three paths of escalation that could not have been foreseen by current mechanisms. The first is the cyber-nuclear nexus: a cyberattack on systems linked to nuclear command and control

could make it hard for the targeted entity to distinguish between a technical error and the onset of an attack or a first strike designed to render the system inoperable. In a situation of high uncertainty and time pressure, it may be the case that the response is not in accordance with what is actually meant (Paoli, 2025). The second is the compression of the political decision-making process by AI, which can generate facts on the ground that civil society leaders are not informed about, let alone consulted on (Raska, 2025). The third is the multi-domain opacity problem: in a conflict played out in all domains (kinetic, cyber, information and space), traditional signals of intent may not get read accurately, and this could make inadvertent escalation because of miscalculation more likely.

7. OPERATION BUNYAN-UN-MARSOOS: MULTI-DOMAIN DETERRENCE IN PRACTICE

7.1. Operational Context and Significance

The India-Pakistan crisis in May, 2025, sparked by the terrorist attack in Pahalgam and followed by Operation Sindoor, offered the biggest empirical demonstration of the multi-domain deterrence theory in South Asian history. The success of Operation Bunyan-un-Marsoos was not only in terms of immediate military results but also as a doctrinal shift that emerged (Ghalib, 2025; ISPR, 2025). The Pakistani response was an integrated effort of conventional air operations, electronic warfare, cyber operations, space-enabled situational awareness, and an information operation that was well coordinated and demonstrated significant institutional coherence (Sanober Institute, 2025; Stratheia, 2025). The reported combat of Indian Rafale planes had them demonstrating that technological dominance in each platform doesn't necessarily translate to an escalation in dominance when faced by an opponent that can organize and execute synchronization in multi-domains (Trembeczki, 2025).

7.2. Doctrinal Implications

Doctrinal lessons can be learned beyond the bilateral context from Operation Bunyan-un-Marsoos. Second, the operational capacity of multi-domains could at least mitigate the conventional force asymmetries, indicating that the future stability of deterrence would be as much a function of integration of domains as of platforms (Abid & Bano, 2025; Kidwai, 2025). Secondly, the conflict highlighted the strategic significance of societal resilience – in the sense of the coherence and resolve of Pakistan's national response, demonstrated in the coordinated messages from the government and the way the conflict was described as "Marka-e-Haq" (Ghani, Nawaz & Khalid, 2025; Kayani, Ashraf & Shahid, 2026; Freedman, 2004). Third, the war proved that the deterrence in South Asia is no less effective but more complex (Akhtar, 2025).

7.3. Post-Crisis Instabilities

In May 2025, active military operations ended, but the underlying working conditions that have led to this crisis have not been addressed. Despite concerted efforts to calm down, Indian political and military leaders have kept playing the escalation game, with top military officials openly declaring their preparedness to resume strikes on Pakistan. India's resolution to keep the Indus Waters Treaty 'in abeyance' added an additional javelin that Pakistani authorities have decried as an act of war (Ahmad, 2025; Banerji & Sitaraman, 2025). The overall post-crisis trend shows ongoing militarization, hostile rhetoric and the lack of any new crisis-communication processes to match the technological conditions of multi-domain conflict.

8. RESEARCH METHODOLOGY

This study takes a qualitative approach, in line with the interpretive and analytical paradigm of strategic studies and international security studies. The central phenomenon to be explored is complex, multi-faceted and difficult to quantify and operationalise, making a qualitative approach epistemologically appropriate. The study's purpose is not to test nor formulate statistical hypotheses; it is to build a theory-based interpretation based on empirical evidence of a highly dynamic strategic reality.

8.1. Research Design

The study uses a case-analytical design of a qualitative approach, which involves combining the thematic synthesis and structured comparative analysis. The focus on the Indo-Pakistani strategic relationship will be used as the basic unit of research while emphasizing the timeframe from 1998 to early 2026. The theoretical propositions that this paper examines are explored in the most current and empirically rich context of the Indo-Pakistani conflict in May 2025. The empirical material is organized into the five technology categories and three categories of stability risk in the theoretical framework, and allows systematic cross-case comparison.

8.2. Data Sources

Official statements, press releases and policy documents issued by the Inter-Services Public Relations Directorate of Pakistan, Indian Ministry of Defence and their respective United Nations bodies are the primary sources. Secondary sources include peer-reviewed journal articles in Web of Science and Scopus, reports from reputable security think tanks (such as SIPRI, ISSI, USIP and the Belfer Center at Harvard Kennedy School) and credible reports of the May 2025 crisis in the

international news media. The reference section gives full citations for all sources (no synthetic or speculative citations).

8.3. Analytical Framework

The analysis is structured on three interrelated theoretical frameworks. The basis for determining stability and instability is deterrence theory (classical and extended). This literature on multi-domain operations provides a doctrinal framework to analyze Pakistan's 2025 response. The discussion of the escalation dynamics theory and the advent of inadvertent escalation and crisis instability scholarship provides the basis for understanding how new technology is changing the risk calculus in nuclear-armed dyads. They are then used deductively for the interpretation of empirical evidence from the sources listed above.

8.4. Quality and Validity

Enhancing the credibility of its qualitative interpretation, the study draws on a variety of sources, including official documentation, independent think-tank analysis, peer-reviewed scholarship, and international news coverage. Interpretive claims are supported by a number of independent sources, whenever possible; when a claim is based on one source alone, this is stated, and the credibility of that source is discussed. The study has used the method of reflexive scrutiny in the national sources from Pakistan and India, and given a secondary place to partisan sources of information in favor of peer-reviewed and institutionally credible sources.

9. DISCUSSION

From its analysis, the following broad conclusions emerge regarding strategic stability in South Asia in the future. Based on the analysis, three broad conclusions emerge regarding the future of strategic stability in the region. First, technology is not what brings instability; it just exacerbates an already unstable situation with potential for catastrophic consequences. Emerging technologies do not bring the scenario of India-Pakistan conflict; they intensify and speed up its effects. Today's political tensions are not created by the new AI-enabled kill chain, which compresses human decision-making from hours to minutes; they are merely exacerbated by the shorter time in which they can be managed before turning into kinetic. Technology governance is thus an imperative complement to political conflict resolution, rather than an alternative.

Second, deterrence in South Asia is not fragile enough to trigger the outbreak of massive war but is sufficiently fragile to have also generated recurring crises, and the addition of multiple domains and AI-laden capabilities is making it even more fragile. The conflict of May 2025 was a reminder of the cost of escalation on both sides of the conflict. However, it was conducted within the context of

persistent coercive signaling, unaddressed grievances and no new institutional structures to deal with new risks of escalation. Deterrence based on the recognition of catastrophic risk is one that is more easily miscalculated than deterrence backed by trustworthy communication and working bilateral institutions.

Third, and most important, has been the development of a need to incorporate a social component into the concept of deterrence stability, that of societal resilience. The informational and social aspect of conflict, meaning the capacity of the public to withstand disinformation, the governments to keep a strategic narrative intact, and the strength of civil institutions in the face of stress, makes for a significant factor in deterrence results. If disinformation is orchestrated, then a society is likely to fracture, limiting the scope of government discretion to be restraining; if it remains coherent, then a society can afford political space for prudent crisis management. The investment in this aspect of security should not be regarded as a soft addendum to hard power deterrence; it is a structural necessity, as part of stable deterrence in the information age.

10. CONCLUSION

South Asia is at a pivotal turning point. Military doctrines are being transformed in two nuclear-armed nations with a fragile deterrence partnership: artificial intelligence, autonomous systems, cyber technologies, space assets, and quantum technologies are being incorporated into their military toolbox to shape how they compete in the future. The lessons from the May 2025 theatre of the India-Pakistan conflict are relevant: deterrence still works; multi-domain operations can be an effective counter to conventional imbalance; and societal will is a strategic factor.

However, the structural factors that render South Asia unsafe are unaddressed. Non-resolved territorial issues, domestic political reasons for posturing for confrontation, historical grievance-based misperception, and inadequate crisis communication mechanisms remain. Technologies that are yet to be developed are not helping to alleviate these conditions; they're just helping to speed up the rate at which they can produce deadly outcomes.

What matters in the future of strategic stability in South Asia is not so much the number of weapons possessed by either side but the governance decisions made concerning the development, deployment and limitation of weapons and the technologies that enable them. Those states and societies that develop resilience in the governance of dual-use technologies, credible and institutionalized crisis communication, informational resilience against disinformation, and a political culture that can recognize prudent restraint from strategic weakness will have the advantage in tackling the multi-domain security environment that is emerging.

How much more unforgiving will deterrence be in the age of AI than its nuclear predecessor? The margin of error is getting smaller, and the complexity of the challenge is increasing. It is in the interest and responsibility of the international community to help build governance mechanisms up to this challenge before the next one comes along to test them.

11. POLICY RECOMMENDATIONS

South Asian governments, the international community and multilateral institutions are targeted by the following recommendations, based on the analysis.

11.1 Develop International Norms for Military Applications of Emerging Technologies.

The current international legal framework – such as international humanitarian law, the UN Charter regime on the use of force, and arms-control treaties – was not developed to deal with autonomous weapons, AI-enabled targeting or offensive cyber operations. In times of crisis, norms binding or politically binding should be created through multilateral forums such as the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems and the Conference on Disarmament for these technologies. Prohibition of targeting of nuclear command-and-control infrastructure and delivery systems with AI should be given priority.

11.2 Preserve Meaningful Human Oversight in Lethal Decision-Making

India and Pakistan need to have a clear-cut doctrinal commitment to human control over nuclear-related domains. Practical institutional arrangements are required, such as establishing clear authorization hierarchies, consistent human oversight of recommendations to target above-set thresholds generated by AI and the periodic review of autonomous-system rules of engagement. Commitment to human oversight should be part of the conditions for technology transfer and defense cooperation agreements, if such agreements are to be made with partners abroad.

11.3 Institutionalize Bilateral Crisis Communication Mechanisms

The existing India-Pakistan hotline and notification mechanisms are not adequate to cope with the tempo and complexity of multi-domain conflict. A dedicated architecture for crisis communication, built from the Cold War-era facilities used by the US and the Soviet Union, should be created, adapted to the current technological conditions. Such an architecture should have direct communications between the head of government, military-to-military

deconfliction procedures for cyber and space operations, and regular tabletop exercises that replicate crisis-management processes.

11.4 Strengthen Cyber Confidence-Building Measures

If a bilateral cyber confidence-building measure is negotiated, similar to that of the 2005 ballistic missile notification protocol, then there is a possibility that the risk of a cyber incident inadvertently escalating may be reduced. At the very least, this should involve banning offensive use of cyber means against nuclear command and control systems, as well as facilitating quick communication in the event that any key cyber event has an impact on security systems.

11.5 Invest in societal resilience and digital literacy.

The two governments need to invest heavily in public digital literacy, anti-disinformation skills and institutional structures for fast and trustworthy public communication in crises. Support independent media, civil society, fact-checking groups and academic institutions with the ability to make rapid public analysis. In May 2025, the conflict itself proved that the ability to stay coherent in a society when under pressure is a strategic asset.

12. LIMITATIONS OF THE STUDY

- First, the availability of open-source material is a constraint. This study has restricted access to classified surroundings where the most operationally relevant decisions on the activation of the AI system, authorization of cyber operations, nuclear alert levels and diplomatic backchannels were made during the crisis in May 2025. Again, the analysis is restricted to what states reported openly, what analysts gleaned from open reporting and what institutional evaluations have been made public. Future documentation will be classified and may change some of the interpretations put forth here.

- Second, the empirical record is still incomplete due to the recentness of the events of May 2025. Operational histories that are written from the viewpoint of authority or government-commissioned after-action reviews will take years to conceive and complete. Some of the assessments presented in this article are thus provisional and may be modified when more detailed documentation is available.

- Third, the study is regionally oriented and therefore is unable to explore the China factor in the strategic stability of S.A. systematically. India's nuclear relationship with China is an indirect but important influence on the India-Pak deterrence balance, while an emerging arms race between the United States and

China, facilitated by the diffusion of artificial intelligence, will impact South Asia in ways that cannot be explored completely in this study.

- Fourth, the qualitative methodology used is not falsifiable, that is, it does not lead to predictions of probabilities or quantified statements. The study pinpoints mechanisms, risk factors, and conditions, but does not offer specific probabilities of escalation or a failure to deter. For academics interested in quantitative modeling of the dynamics of the South Asian crises, reference to related literature will be necessary.

13. SIGNIFICANCE OF THE STUDY

This research has several implications for the study, policy and public understanding of South Asian security.

- **Scholarly Contribution:** The study is the first systematic synthesis of the implications of deterrence of the Indo-Pakistani conflict of May 2025 in a coherent theoretical framework that encompasses classical deterrence theory, multi-domain operations doctrine and escalation dynamics. It makes a contribution to the analytical use of societal resilience as an additional variable in deterrence stability, which the existing literature has recognized but lacks a rigorous theory that has been developed for the South Asian context. It also adds to the body of literature on AI and nuclear risk by offering a region-specific analysis based on empirical events of recent history, instead of abstract modeling.

- **Policy Contribution:** The study outlines specific governance gaps in the existing bilateral, regional and multilateral governance framework for the management of emerging technology risks in South Asia and offers specific and actionable recommendations for regional governments, international institutions and multilateral forums. It comes at a time when the governance system for the use of military AI, autonomous weapons and cyber capabilities is less mature than the rate of technological adoption, and when the political dynamics surrounding the expansion of CBMs could be slightly more conducive than in the immediate aftermath of the crisis.

- **Public Contribution**: The study offers an analytical account of the interplay of AI, autonomous systems, cyber operations and information warfare with deterrence stability in a nuclear-armed region, which is both rigorous and accessible, thus informing public debates on one of the most impactful security challenges of the modern era. An increase in public awareness of these dynamics is itself a part of societal resilience: publics who understand the dynamics of escalation caused by disinformation are more likely to be able to resist manipulation in times of crisis.

- **Temporal Contribution:** This is a point in time for South Asian security that could not be better captured by the study, which is a moment of structural transition in South Asian security. Technologies are transforming the strategic environment, and doctrines for using them will continue to develop; governance mechanisms for managing them are still in the process of formation. Documentational analysis of this transition moment has been performed and provides a ground level for comparative and longitudinal studies in the future.

DECLARATIONS

- **Conflicts of Interest:** The authors have no conflicts of interest to disclose.

- **Data Availability:** All the data mentioned in this study were obtained from open-source, publicly available sources as referenced in full below.

AUTHOR CONTRIBUTIONS:

- **Shanzay Saeed** made conceptualization, literature search and initial drafting.

- **Dr. Farhat Konain Shujahi** was a contributor in the research design, methodological development and critical review of the manuscript.

- **Dr. Ahmed Saeed Minhas** participated in theoretical framing and analytical synthesis and in the final review of the manuscript. All authors read and approved the final version of the manuscript.

REFERENCES

Abbasi, R., & Uzzaman, M. S. (2022). Strategic stability of South Asia in the age of artificial intelligence. *Pakistan Horizon, 75*(4), 41–50. https://www.pakistan-horizon.piia.org.pk/index.php/pakistan-horizon/article/view/256/236

Abid, A. A., & Bano, S. (2025). Artificial intelligence, autonomy and the human factor: Strategic lessons from the 2025 India–Pakistan crisis. *Global Strategic Pulse, 2*(1), 13–17. https://cisss.org.pk/GSP/index.php/Global_Strategic_Pulse/article/download/40/29/210

Acton, J. M. (2020). New technologies and strategic stability. *Daedalus, 149*(2), 150–170. https://doi.org/10.1162/DAED_a_01782

Ahmad, A. I. (2025, May 9). *Interview with The National News*. https://www.thenationalnews.com/news/us/2025/05/10/india-pakistan-indus-water-treaty-act-of-war/

Akhtar, N., & Mahmood, N. (2025). Disruptive technologies and deterrence stability in South Asia. *BTTN Journal, 4*(2), 39–63. https://bttn.org.pk/ojs/index.php/BTTN_Journal/article/view/242

Akhtar, R. (Ed.). (2025). *Strategic reckoning: Perspectives on deterrence and escalation post-Pahalgam–May 2025*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/research-analysis/strategic-reckoning-perspectives-deterrence-and-escalation-post-pahalgam-may-2025

Ali, I., & Sidhu, J. S. (2022). Strategic dynamics of crisis stability in South Asia. *Journal of Asian and African Studies, 57*(7), 1357–1375. https://doi.org/10.1177/00219096211054396

Arms Control Association. (1999, December 31). *India, Pakistan agree on security, confidence-building measures*. https://www.armscontrol.org/act/1999-01/press-releases/india-pakistan-agree-security-confidence-building-measures

Arshad, M., & Sheik, R. (2022). Cybersecurity and data integrity in financial systems: A review of risk mitigation and compliance models. *International Journal of Scientific Interdisciplinary Research, 1*, 27–30.

Bajpai, K. P., Chari, P. R., Cheema, P. I., Cohen, S. P., & Ganguly, S. (1995). *Brasstacks and beyond: Perception and management of crisis in South Asia*. Manohar Publishers.

Banerji, A., & Sitaraman, S. (2025). Terrorism and water wars: India–Pakistan on the brink of a major conflagration. *Security Nexus*. Daniel K. Inouye Asia-Pacific Center for Security Studies. https://dkiapcss.edu/nexus_articles/terrorism-and-water-wars-india-pakistan-on-the-brink-of-a-major-conflagration/

Benincasa, E. (2023). Artificial intelligence-enhanced disinformation and international law. *Journal of International Affairs*. https://jia.sipa.columbia.edu/news/artificial-intelligence-enhanced-disinformation-and-international-law-rethinking-coercion

Council on Foreign Relations. (2026, February). *Conflict between India and Pakistan*. *Global Conflict Tracker*. https://www.cfr.org/global-conflict-tracker/conflict/conflict-between-india-and-pakistan

Farooq, A., & de Vreese, C. (2025). Generative AI and disinformation—Introduction. *International Journal of Communication, 19*. https://ijoc.org/index.php/ijoc/article/download/26088/5137/104469

Fournier-Tombs, E., Brubaker, R., & Albrecht, E. (2023). *Artificial intelligence-powered disinformation and conflict* (Policy Brief). United Nations

University Center for Policy Research. https://unu.edu/cpr/brief/artificial-intelligence-powered-disinformation-and-conflict

Freedman, L. (2004). *Deterrence*. Polity Press.

Ganguly, S., & Hagerty, D. T. (2005). Fearful symmetry: India–Pakistan crises in the shadow of nuclear weapons. University of Washington Press.

Ghalib, S. J. (2025). *Warfare reimagined: Algorithmic warfare and the shifting India–Pakistan strategic landscape* (Issue Brief). Institute of Strategic Studies Islamabad. https://issi.org.pk/wp-content/uploads/2025/06/IB_Jahanzaib_June_4_2025.pdf

Ghani, F., Nawaz, M. U., & Khalid, M. (2025). Operation Bunyan al-Marsoos and national cohesion of Pakistan. *The Government: Research Journal of Political Science, 14*, 1–3. https://sujo.usindh.edu.pk/index.php/THE-GOVERNMENT/article/download/7930/4936/14914

Giordano, J. (2026, January 27). *Quantum technologies: Focusing a bit upon realities*. *Strategic Insights, National Defense University*. https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4390960/quantum-technologies-focusing-a-bit-upon-realities/

Haider, M. W., & Azad, T. M. (2021). The role of confidence-building measures in the evolution of relations between Pakistan and India. *World Affairs, 184*(3), 294–295. https://www.jstor.org/stable/27066284

Hussain, Z. (2025). Strategic stability in South Asia: Nuclear deterrence, crisis escalation, and the India–Pakistan security dilemma. *Pakistan Social Sciences Review, 9*(2), 769–786. https://doi.org/10.35484/pssr.2025(9-II)57

Inter-Services Public Relations (ISPR). (2025, May 12). *Operation Bunyan-un-Marsoos marks a decisive response to Indian aggression* [Press statement]. https://www.nation.com.pk/12-May-2025/operation-bunyan-un-marsoos-marks-decisive-response-to-indian-aggression-ispr

Islamabad Policy Institute. (2026, February 2). *Naval warfare in transition: The rise of non-contact technologies in South Asia*. https://ipi.org.pk/naval-warfare-in-transition-the-rise-of-non-contact-technologies-in-south-asia/

Kayani, T. A., Ashraf, R., & Shahid, F. (2026). Pakistan's deterrence posture after the May 2025 conflict: Relevance, limitations and future trajectories. *Qualitative Research Journal for Social Studies, 1*, 263–265. https://qrjsocial.com/index.php/38/article/view/813

Khan, F. H. (2015). *Going tactical: Pakistan's nuclear posture and implications for stability in South Asia* (Proliferation Papers No. 53). Institut Français des Relations Internationales. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/pp53khan_5.pdf

Khan, K. (2012). Understanding information warfare and its relevance to Pakistan. *Strategic Studies, 32*, 140–155. http://142.54.178.187:9060/xmlui/handle/123456789/1729

Kidwai, K. A. (2025, September 16). *Stability of Pakistan's strategic deterrence* [Address]. Islamabad Policy Research Institute. https://www.app.com.pk/national/pakistans-strategic-deterrence-never-affected-during-may-2025-standoff-gen-kidwai/

Klare, M. T. (2023). *Assessing the dangers: Emerging military technologies and nuclear (in)stability* (Report). Arms Control Association. https://www.armscontrol.org/sites/default/files/files/Reports/ACA_Report_EmergingTech_digital.pdf

Lin, H. S., & Trinkunas, H. (2026). Introduction: Emerging technologies and the future of strategic stability. *Texas National Security Review, 9*, 8–18. https://doi.org/10.1353/tns.00030

Manning, R. A. (2020). *National security impact* (Issue brief). Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/national-security-impact/

Noor, S. (2023). Strategic stability in South Asia: The evolving challenges and potential opportunities for India and Pakistan. *Strategic Studies, 43*(1), 64–94. https://issi.org.pk/wp-content/uploads/2023/08/Sitara_Noor_SS_No_1_2023.pdf

Paoli, G. P. (2025). *Impact of military artificial intelligence on nuclear escalation* (SIPRI Insights on Peace and Security No. 2025/7). Stockholm International Peace Research Institute. https://www.sipri.org/publications/2025/sipri-insights-peace-and-security/impact-military-artificial-intelligence-nuclear-escalation

Qasim, A. W., & Alvi, A. S. (2026). How does disinformation as a foreign policy instrument affect peace in South Asia? *Social Science, Humanities and Research Review, 4*(1), 2–7.

Raeesa, U., & Akhtar, N. (2025). India–Pakistan security dilemma: Analyzing deterrence and coercive diplomacy in the context of regional stability.

Journal of Development and Social Sciences, 6(2), 492–507. https://doi.org/10.47205/jdss.2025(6-II)42

Raska, M. (2025). *AI-driven OODA loops and the transformation of military decision-making* (Expert Policy Note, REAIM Global Conference Series). Hague Center for Strategic Studies. https://hcss.nl/wp-content/uploads/2025/04/Raska.pdf

Sandia National Laboratories. (2021, July 20). *Emerging technologies and strategic stability in Southern Asia*. https://www.sandia.gov/cmc/2021/07/21/emerging-technologies-strategic-stability-in-southern-asia/

Sanober Institute Islamabad. (2025, June 23). *Operation Bunyanum Marsoos: Restoring deterrence in volatile South Asia*. https://sanoberinstitute.com/wp-content/uploads/2025/07/OPeration-Bunyanum-Marsoos-Report.pdf

Setze, J. (2022, June 26). *The cyber and information domain and the space domain: Links and interdependencies*. Joint Air Power Competence Center. https://www.japcc.org/essays/the-cyber-and-information-domain-and-the-space-domain-links-and-interdependencies/

Shah, F. (2009, September 9). *Indo-Israeli cyber warfare against Pakistani nuclear program*. *Asian Tribune*. http://www.asiantribune.com

Sood, R. (2022). *Managing the China, India and Pakistan nuclear trilemma: Ensuring nuclear stability in the new nuclear age* (Toda Peace Institute Policy Brief No. 144). Todo Peace Institute. https://toda.org/policy-briefs-and-resources/policy-briefs/managing-the-china-india-and-pakistan-nuclear-trilemma-ensuring-nuclear-stability-in-the-new-nuclear-age.html

Stratheia. (2025, June 10). *Deterrence and escalation control in the 2025 India–Pakistan conflict*. https://stratheia.com/deterrence-escalation-control-in-the-2025-india-pakistan-conflict/

Topychkanov, P. (Ed.). (2020). *The impact of artificial intelligence on strategic stability and nuclear risk: South Asian perspectives*. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/2020-04/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov.pdf

Trembeczki, Á. (2025). *Four key takeaways from the 2025 India–Pakistan conflict*. Hungarian Institute of International Affairs. https://hiia.hu/wp-content/uploads/2025/08/Trembeczki-Four-Key-Takeaways-from-the-2025-India-Pakistan-Conflict.pdf

United States Institute of Peace. (2022). *Enhancing strategic stability in Southern Asia*. https://www.usip.org/sites/default/files/2022-05/enhancing-strategic-stability-in-southern-asia-final-report.pdf

van Niekerk, B. (2021, November 12). *Information warfare and the connected battlefield*. *The Air Power Journal*. https://theairpowerjournal.com/information-warfare-and-the-connected-battlefield/

Xiaolian, S., Siraj, U., & Din, A. U. (2024). Modi's Hindutva policy and its impact on Indo-Pak relations. *Margalla Papers, 28*(1), 1–5. https://margallapapers.ndu.edu.pk/site/article/view/236

Zaman, S. U. (2025). India's limited war-fighting doctrines and the May 2025 provocation: Challenges to deterrence and stability in South Asia. *Strategic Thought,* 73–75.

Ms. Shanzay Saeed is an MPhil Scholar at Cardiff University, Cardiff, Wales, United Kingdom. She is the corresponding author and can be contacted at **shanzaysaeed01@gmail.com**.

Dr. Farhat Konain Shujahi is an Assistant Professor in the Department of International Relations at the National University of Modern Languages (NUML), Islamabad, Pakistan. She can be contacted at **farhatkonain@numl.edu.pk**.

Dr. Ahmed Saeed Minhas is a Professor and the Vice Chancellor of DHA Suffa University, Karachi, Pakistan. He can be contacted at **ahmedsaeedminhas81@dsu.edu.pk**.