RECASTING COLD WAR LOGICS IN THE DIGITAL AGE: A SOUTH ASIAN PERSPECTIVE

Amjad Fraz
Centre for Aerospace and Security Studies, Lahore

August 2025

ABSTRACT

This paper tests whether Cold War stability logics can be applied to a multi-domain rivalry shaped by artificial intelligence (AI), cyber operations, and space services in South Asia. Using a qualitative, comparative case-study method (2019–2025) that synthesises official documents, reputable analyses, and the May 2025 crisis, it evaluates strategic stability and the security dilemma under conditions of “entanglement,” where dual-use networks support both conventional and nuclear functions. The study finds that India’s integration of AI into sensing, decision support, and air/air-defense teaming compresses decision time and muddies intent, while Pakistan’s institution-first approach (CENTAIC, NASTP, telecom cyber governance) tilts toward denial and human-in-the-loop control. Cyber deterrence works better by denial than punishment; space investments that prioritise resilient communications and rapid reconstitution contribute to crisis assurance if transparently non-weaponised. The 2025 episode, featuring multi-domain operations and effective Pakistani cyber defense (67–0), shows AI/cyber can aid restraint through rapid verification, yet raise pressure through accelerated cycles. The paper proposes adapted Cold War tools: Flexible Response for the digital domain, ring-fencing AI from nuclear C3I and missile-defense cueing, incident channels for cyber/space, and resilience metrics for C3ISR. Cold War dynamics help, but only when re-engineered around human authorisation, transparency, and network resilience.

Keywords: Strategic stability, Artificial intelligence, Cyber operations, Space security, South Asia, Deterrence

TABLE OF CONTENTS

1. INTRODUCTION

The nuclear technology fundamentally reshaped international security dynamics during the Cold War. The development and proliferation of nuclear weapons became central to the strategies pertaining to deterrence between the US and the USSR. The tormenting use of atomic bombs on Nagasaki and Hiroshima showcased the unparalleled destructive power of these weapons, ushering in the nuclear age and catalysing a relentless nuclear arms race. Both superpowers invested heavily in developing hydrogen bombs in the 1950s, which were significantly more potent than their atomic predecessors, thereby exponentially increasing the risks of any potential conflict.

This era was largely defined by the principle of Mutually Assured Destruction (MAD), a precarious balance where the certainty of complete annihilation for both sides deterred direct military confrontation, resting on the logic of catastrophic retaliation. To solidify this deterrent, political authorities invested in developing highly advanced delivery systems, including Intercontinental Ballistic Missiles, Submarine-Launched Ballistic Missiles, and robust second-strike capabilities, ensuring a devastating response even after absorbing an initial nuclear strike.

Simultaneously, the concept of Flexible Response emerged, offering a spectrum of military options beyond the binary choice of massive nuclear retaliation. This strategy, championed primarily by NATO, aimed to provide nuanced responses to aggression, ranging from conventional forces to limited nuclear strikes, thereby reducing the risk of rapid escalation to global nuclear war and tailoring responses to the specific scale and nature of conflicts.

Throughout this period, maintaining the balance of power was a strategic imperative, driving relentless investment in nuclear arsenals, enhancing weapons accuracy and reliability, and developing advanced early warning and missile defence technologies to prevent a first-strike advantage. However, the international security landscape has undergone a profound transformation in the 21st century.

In place of a bipolar nuclear rivalry, a multi-domain competition now shapes deterrence. Contemporary stability depends upon interactions across land, sea, air, cyber, and space, and upon whether states can deter by denial as well as by punishment across these domains. Scholars on cross-domain and integrated deterrence highlight that credibility now hinges on resilience of networks and sensors, not only on warheads and delivery systems.

This paper argues that these technological advancements are fundamentally redefining the dynamics of deterrence and strategic stability, particularly within South Asia, where the enduring rivalry between India and Pakistan continues to shape regional security dynamics. The analytical lens tests whether modern capabilities create stability by improving warning, control and damage-limitation, or whether they degrade stability by compressing decision time, exposing critical networks, and incentivising pre-emption. The assessment proceeds domain by domain, while emphasising cross-domain effects and Pakistan's evolving posture in AI, cyber and space.

Furthermore, the study also comprehensively examines the evolving strategies of both India and Pakistan, their respective technological advancements, and the broader geopolitical context influencing their actions in the realms of AI, cyber, and space.

2. LITERATURE REVIEW

The most salient literature defines strategic stability as the absence of incentives for a first strike and the assurance that a crisis would not escalate inadvertently, building on the Cold War distinction between crisis stability and arms-race stability. Recent work extends this to "cross-domain" and "integrated" deterrence, arguing that credibility, communication, and restraint should operate not within a single arena but across nuclear, conventional, cyber, and space domains. RAND's syntheses outline how deterrence by denial and punishment should be adapted for multi-domain competition and to align with the US' current concept of integrated deterrence,[1] a framing that travels effectively beyond North Atlantic contexts.

A parallel body of literature examines how new technologies complicate older deterrence logics. Acton's "entanglement" thesis highlights that a non-nuclear attack on dual-use command, control, communications (C3), and intelligence systems can

[1] Mallory, King. *New Challenges in Cross-Domain Deterrence*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE259.html.

create significant pressures for inadvertent nuclear escalation, particularly where space and cyber systems underpin early warning.[2] Johnson observes that artificial intelligence and autonomy compress decision time, heighten uncertainty, and strain classical assumptions of rational signalling, thereby challenging established deterrence models.[3] These perspectives converge on the need to harden C3I, enhance transparency, and build resilience rather than relying solely on threat-based deterrence.

Within South Asia, analyses of the nuclear dyad frequently centre on India's limited-war thinking and Pakistan's responses. Ladwig's work on Cold Start details India's pursuit of rapid conventional options intended to remain below Pakistan's perceived nuclear thresholds.[4] Pakistani discourse, as articulated in public statements by Kidwai, describes the progression from minimum credible deterrence to full-spectrum deterrence, a process designed to close gaps at tactical, operational, and strategic levels while remaining within credible-minimum boundaries.[5] Collectively, this literature positions Indo-Pak deterrence as crisis-prone but stable at the nuclear level, with stability underwritten by second-strike assurance and the signalling effects of posture choices.

Governance measures have sought to reduce risks. The Lahore Declaration and its Memorandum of Understanding established a baseline for confidence-building measures. At the same time, the 2005 bilateral agreement on pre-notification of ballistic-missile tests institutionalised predictability in a sensitive area of competition.[6] These mechanisms are frequently cited as practical tools for maintaining open deterrence communication channels, even when political relations deteriorate.

[2] James M. Acton, Li Bin, and Tong Zhao, *Reducing the Risks from Nuclear Entanglement* (Washington, DC: Carnegie Endowment for International Peace, September 2018), https://carnegie-production-assets.s3.amazonaws.com/static/files/Acton_Entanglement_Sept2018.pdf.

[3] James Johnson, "Deterrence in the Age of Artificial Intelligence & Autonomy: A Paradigm Shift in Nuclear Deterrence Theory and Practice?" *Defense & Security Analysis* 36, no. 4 (2020): 422–448, https://doi.org/10.1080/14751798.2020.1857911.

[4] Walter C. Ladwig III, "A Cold Start for Hot Wars? The Indian Army's New Limited War Doctrine," *International Security* 32, no. 3 (2007): 158–190, https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/IS3203_pp158-190.pdf.

[5] International Institute for Strategic Studies, *Transcript of Lt. General Khalid Kidwai's Keynote Address: Seventh IISS–CISS Workshop on "South Asian Strategic Stability: Deterrence, Nuclear Weapons and Arms Control"*, London, February 6, 2020, https://www.iiss.org/globalassets/media-library---content--migration/files/events/2020/transcript-of-lt-general-kidwais-keynote-address-as-delivered---iiss-ciss-workshop-6feb20.pdf.

[6] Government of India and Government of Pakistan, *Agreement between India and Pakistan on Pre-Notification of Flight Testing of Ballistic Missiles*, October 3, 2005, https://www.mea.gov.in/portal/legaltreatiesdoc/pa05b0591.pdf.

Recent empirical episodes underscore both resilience and fragility. Analyses of the 2019 Balakot-Kashmir crisis depict rapid conventional escalation and deliberate signalling that nevertheless remained below nuclear thresholds. In May 2025, crisis literature records concurrent military and cyber signalling, including large-scale hacktivist and denial-of-service attacks against essential services, illustrating how multi-domain operations are taking space in a conventional conflictual environment.[7] In the backdrop of India's failure in cyber defence, the argument is fortified that crisis management now requires multi-domain escalation and de-escalation tools and technologies.

An expanding range of Pakistan-focused sources highlights under-researched developments with direct relevance to regional stability debates. Official materials on the National Cyber Security Policy 2021 and the Pakistan Telecommunication Authority (PTA)'s 2023–2028 strategy indicate a shift from ad-hoc practices to institutionalised cyber governance and sectoral resilience. In space, SUPARCO's communication satellite Paksat-MM1 and the 2025 PRSC-EO1 earth-observation satellite enhance domestic C4ISR-relevant capacity, while iCube-Qamar's role in China's Chang'e-6 mission signals technological collaboration and prestige.[8] These developments have yet to be fully incorporated into formal models of Indo-Pak stability, representing a clear gap.

Comparative research beyond South Asia offers two additional layers. First, European and transatlantic studies emphasise resilience and redundancy, exemplified by the European Union's IRIS² secure-connectivity programme, which aims to reduce vulnerability to space and cyber disruption through a multi-orbital constellation.[9] Second, CSIS assessments of Chinese and Russian space-security capabilities highlight the escalatory potential of destructive counterspace testing, providing cautionary analogues for regions where space systems are integrated with nuclear

[7] CloudSEK, "Brief Disruptions, Bold Claims: The Tactical Reality Behind the India–Pakistan Hacktivist Surge," May 30, 2025, https://www.cloudsek.com/blog/brief-disruptions-bold-claims-the-tactical-reality-behind-the-india-pakistan-hacktivist-surge.

[8] Reuters, "Pakistan Launches First Home-Made Observation Satellite," January 15, 2025, https://www.reuters.com/world/asia-pacific/pakistan-launches-first-home-made-observation-satellite-2025-01-15/; Nadir Guramani, "Pakistan's iCube-Qamar Beams Back First Images from Moon's Orbit," *Dawn*, May 10, 2024, https://www.dawn.com/news/1832658.

[9] European Commission, "IRIS² Secure Connectivity," December 16, 2024.

C3I.[10] These literatures support policies favouring diversified communications, rapid reconstitution, and crisis hotlines for cyber and space.

From this discussion, four themes emerge. First, classic deterrence frames remain necessary but are insufficient without addressing cross-domain spillovers. Second, AI, cyber, and space entanglements elevate inadvertent escalation risks by eroding transparency and compressing decision time. Third, Indo-Pak studies often over-emphasise Indian doctrine while under-analysing Pakistan's recent institutional and space-based advances, leaving an empirical gap. Fourth, comparative cases from Europe and great-power competition point towards resilience-centred stability building.

This study addresses these gaps by examining whether and how cyber, AI, and space capabilities can contribute to strategic stability between India and Pakistan, with particular focus on Pakistan's balancing approach, resilience measures, and the design of domain-specific crisis-management mechanisms.

3. METHODOLOGY: COMPARATIVE STUDY

This paper is a comparative case-study (qualitative) research, drawing on the strategic deterrence theory and augmenting it with findings on AI, cyber, and space trends in South Asia. It examines official reports, think-tank analyses, peer-reviewed journals, and other credible news stories from 2019 to 2025, including the India–Pakistan crisis in May 2025. The research aim is to determine whether artificial intelligence-enabled capabilities support stability by enhancing warning, resilience, and communication or facilitating escalation by reducing decision time.

4. THEORETICAL FRAMEWORK: STRATEGIC STABILITY & SECURITY DILEMMA

The current analysis is based on two complementary theoretical constructs. Strategic stability, rooted in Cold War deterrence theory, holds that first strikes are deterred by mutual vulnerability and the capability to retaliate effectively. Formalised by Thomas Schelling and Herman Kahn, this logic assumes that stability exists when

[10] Clayton Swope, Kari A. Bingen, Makena Young, Madeleine Chang, Stephanie Songer, and Jeremy Tammelleo, *Space Threat Assessment 2024* (Washington, DC: Center for Strategic and International Studies, April 17, 2024).

neither party can gain an advantage without incurring unacceptable risk.[11] In modern multi-domain contexts, the concept has expanded to include resilience, reliable communications, and maintaining human control over AI-enabled systems.

The security dilemma, introduced by Kenneth Waltz and Robert Jervis, posits that defensive measures taken by one state can be perceived as offensive, prompting reciprocal actions and undermining stability.[12] In AI and cyber domains, capabilities such as enhanced sensing or hardened networks may be interpreted as counterforce preparations, fuelling technological competition below the nuclear threshold.

Applied together, these lenses frame the India–Pakistan AI and cyber rivalry as a situation in which each state seeks greater security through denial, resilience, and human control, yet risks accelerating decision cycles, creating ambiguous intent, and heightening crisis instability.

5. CONTEMPORARY DEVELOPMENTS

In an era marked by rapid technological advancements and changing geopolitical landscapes, the dynamics of international security are undergoing profound transformations. The Cold War era, characterised by a bipolar balance of power dominated by nuclear arsenals, has given way to a contemporary environment where emerging technologies, most notably AI, cyber, and space capabilities, play a fundamental role in shaping military strategies and deterrence paradigms. The purpose of this section is to further analyse the implications of these developments within South Asia, where enduring rivalries between India and Pakistan continue to shape security dynamics.

5.1 Artificial Intelligence

The use of AI in the nuclear field poses serious risks, especially with regard to the possibility of accidental or deliberate nuclear missile launches. Designing automated systems for nuclear weapons is extremely complex, making it very difficult to prevent mistakes or failures. While AI and machine learning are useful for enhancing

[11] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966); Herman Kahn, On Thermonuclear War (Princeton, NJ: Princeton University Press, 1960).

[12] Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979); Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics* 30, no. 2 (January 1978): 167–214, https://doi.org/10.2307/2009958.

routine military operations and for defence against high-value targets, it is not wise to rely on AI in managing nuclear weapons or missile defence because such systems can be open to cyberattacks that could prove to be disastrous.

AI systems can influence various aspects, including decision-making processes, command and control systems, and predictive analysis. The speed at which AI can process enormous volumes of data could theoretically improve the detection of submarines, which are key to second-strike capabilities. For example, advancements in underwater drone technology combined with AI-driven pattern recognition could make it easier to locate and track submarines. This development threatens the survivability of a second-strike force, potentially destabilising deterrence by encouraging pre-emptive strikes.

Similarly, AI can enhance missile defence by improving interception accuracy. However, the automation of such systems raises the risk of unintended escalation. For instance, if an AI system mistakenly identifies a civilian aircraft as an incoming missile and launches an intercept, it could trigger a retaliatory nuclear strike. The 1988 downing of Iran Air Flight 655 by the US Navy serves as an example, where human error led to the mistaken identity of the aircraft.

The stakes are even higher with AI at the helm. The risk involves the possibility of AI systems malfunctioning, being compromised, or being used in ways that could destabilise nuclear strategies or lead to unintended escalations. The research literature warns about “entanglement,” where non-nuclear tools can degrade nuclear command, control, and intelligence.[13] This raises inadvertent escalation risks and shortens the window for verification.

However, the swift integration of AI into military systems may provoke a new form of technological arms race, echoing the strategic rivalries of the Cold War era. Ensuring that AI does not exacerbate existing tensions requires robust international cooperation and regulation.

Recent multilateral processes now recognise these risks and offer concrete, near-term policy hooks. In December 2023, the UN General Assembly passed Resolution 78/241 concerning the governance of autonomous weapons. It calls for

[13] James M. Acton, Li Bin, and Tong Zhao, *Reducing the Risks from Nuclear Entanglement*.

national reporting on governance options and has generated formal submissions from many states, including India and Pakistan.[14]

As part of the Convention on Certain Conventional Weapons, the Group of Governmental Experts released an updated draft document in May 2025 that records provisional consensus elements for an instrument on autonomous weapons. These include human responsibility, reliability, traceability, and context-appropriate human control.[15] Pakistan has tabled draft elements for a legally binding protocol. India has submitted views that emphasise compliance with international humanitarian law and a cautious, process-driven approach.[16]

5.1.1 India and the Role of AI

States see AI as a means to manipulate power distribution to their advantage. Within South Asia, India has been proactively advancing AI-based technology for military applications in recent years.

The Joint Doctrine of the Indian Army Forces (2017) and the Land Warfare Doctrine (2018) both highlight how India is incorporating cutting-edge technologies into its armed forces.[17] Its pursuit to rapidly modernise its military by incorporating advanced technologies aligns with its offensive doctrines. A high-level task committee was set up in March 2018, under government leadership, to assess AI’s role in strengthening national defence. At present, India is attracting significant venture capital interest in AI technologies relevant to defence and security.

The Indian government recognises military AI as a critical enabler for meeting its strategic and planning objectives.[18] Currently, a number of Ministry of Defence (MoD) branches use AI products and technologies in their advanced implementation

[14] United Nations General Assembly, Lethal Autonomous Weapons Systems, A/RES/78/241 (22 December 2023).

[15] CCW Group of Governmental Experts on LAWS, Revised Rolling Text as of 12 May 2025.

[16] Pakistan, “Elements of an International Legal Instrument on Lethal Autonomous Weapons Systems (LAWS),” Working Paper submitted to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, March 4–8 and August 26–30, 2024; India, “Submission Pursuant to UNGA Resolution 78/241 (LAWS),” (May 2024).

[17] Dr Masood Ur Rehman Khattak, The Indian Army’s Land Warfare doctrine 2018, Winter 2020, https://ipripak.org/wp-content/uploads/2020/06/Article-5-IPRI-Journal-XX-I-Ind-Arm-New-Lan-ED-SSA-FINAL.pdf.

[18] Vivek ND, “AI and Indian Defence: Enhancing National Security Through Innovation,” *The Diplomat,* October 1, 2024, https://thediplomat.com/2024/10/ai-and-indian-defense-enhancing-national-security-through-innovation/

stages. The Defence AI Council (DAIC) was established by the MoD in 2019 to provide strategic direction for the application of AI in the military sector.

To put these technologies into practice, the Indian government and industry are forming a cooperative alliance. The AI Task Force has been working hard to develop a military strategic advantage. In order to concentrate on AI applications in the defence industry, India has already established a Centre for AI and Robotics (CAIR) under the Defence Research and Development Organisation (DRDO). This goal is to make it easier to integrate AI into military systems, particularly in the domains of non-centralised systems for tactical command, control, Information security, autonomous vehicles, intelligence systems, and communication systems.

The pursuit of artificial intelligence by India, its subsequent application in the military, and its changing strategic roles will have a negative impact on South Asian strategic stability. For instance, if India deploys AI in nuclear command and control systems or Ballistic Missile Defence (BMD) systems, algorithmic biases could lead to unintended use or even pre-emptive strikes. The use of AI in such systems is bound to be fail-deadly, not fail-safe. It means that if an AI system fails, it is likely to result in catastrophic consequences rather than safe outcomes.

India incorporates AI into sensing, decision support, and air combat teaming. As with the Cold War, technology drives instability before balance. In South Asia, AI is progressing faster and with fewer checks. Thus, where India’s integration of AI into air defence and teaming accelerates tempo, Pakistan’s emphasis on decision support and human control is a balancing response. Nonetheless, the action—reaction cycle remains active below the nuclear threshold.

5.1.2 Pakistan’s role and response in AI

Pakistan, recognising the strategic imperative of adapting to the evolving landscape of modern warfare, has embarked on its own journey of AI development and deployment within its defence sector. There continue to be hurdles in this implementation, a primary challenge being its economic limitations and resource constraints. However, despite these challenges, Pakistan has taken several significant steps towards integrating AI into its defence sector.

Pakistan accepts that AI is now part of the military landscape and focuses on building institutions first as a way to anchor its developments in the AI domain.

In 2020, the Pakistan Air Force formed its Centre of Artificial Intelligence and Computing (CENTAIC), a dedicated hub for sensor fusion, decision support, and data engineering.[19] The National Aerospace Science and Technology Park (NASTP), a strategic project of national priority, connects air force units, universities, start-ups, and international partners across space, cyber, and aviation. The Army has also established an Army Cyber Command, with its Army Centre of Emerging Technologies mandated to explore the applications of AI in cyber defence and electronic warfare.

These are credible foundations. Better integration of civilian and military sensor data is enabled by institutional capacity at CENTAIC and NASTP. During the May 2025 crisis, Pakistan's National CERT issued a set of formal advisories. The three advisories issued during and following the Indo-Pak crisis recommended cyber vigilance, disinformation mitigation, and rapid patching of Microsoft Outlook to enhance government and non-government resilience during the increased tensions.[20] These measures are modest on the surface, but they are stabilising in practice, reducing the chance of any mishap that can be read as strategic intent in a tense crisis.

Doctrinally, Pakistan is leveraging AI by manned–unmanned teaming concepts. The model envisions AI handling navigation, threat detection, and information sharing, while lethal authority remains strictly with humans. This not only multiplies capability but also maintains a human in the loop, which is imperative for ensuring crisis stability in nuclearised South Asia.[21]

Training has evolved in parallel. The Pakistan Army has developed an Infantry Tactical Simulator employing adversarial AI capable of adapting to the trainee's actions, generating new engagement scenarios, and sharpening decision-making under time pressure. These measures reveal a deliberate attempt to harness the speed and efficiency that AI can offer while retaining the human edge in fast-moving,

[19] Profit by *Pakistan Today*, "PAF Establishes Centre for Artificial Intelligence and Computing," 31 August 2020, https://profit.pakistantoday.com.pk/2020/08/31/paf-establishes-center-for-artificial-intelligence/.

[20] National CERT Pakistan, "Important Local Remote Code Execution Vulnerability in Microsoft Outlook," Advisory NCA-28.051625, 16 May 2025, https://pkcert.gov.pk/advisory/25/28.pdf.

[21] Centre for Aerospace and Security Studies, *Artificial Intelligence, Electronic & Cyber Warfare and Unmanned Aerial Systems: New Paradigm of Next Generation Aerial War* (Lahore: CASS, July 2025).

AI-dense environments, thereby minimising the risks of miscalculation or inadvertent escalation.

Pakistan is aware that increasing utilisation of AI in military domains, especially within the volatile India-Pakistan relationship, underscores an urgent need for bilateral dialogues. AI decision aides reduce delays in verifying or ruling out rumours or false alarms, lessening the likelihood of hasty action during a crisis. A cautionary lesson is the 2019 discovery of malware in the administrative network of the *Kudankulam* nuclear plant in India, showing how a non-kinetic event at a nuclear-related facility can shape perceptions.[22]

The 2025 crisis, the first at a multi-domain scale, demonstrated that holistic strategic stability now hinges on network resilience, data provenance, and documented human authorisation. In a future India–Pakistan encounter, strong AI-aided cyber resilience and rapid, transparent handling of such incidents will be as important as air defences. That is where Pakistan's institutional focus on resilience can pay dividends for stability. Without bilateral guardrails that define the dynamics of AI in nuclear command, control, and communications, as well as missile defence cueing, any routine experimentation could be interpreted as counterforce preparation and invite pre-emption. Thus, AI can destablise the dyad if it is not restricted to denial and resilience functions and supported by agreed incident channels.

5.2 Cyber Warfare

Cyber warfare has become a critical domain where capabilities to disrupt or protect critical infrastructure can influence geopolitical stability. Cyber strategies can involve both offensive operations, aimed at disrupting an adversary's systems, and defensive measures to safeguard critical assets. Cyber operations influence crisis behaviour because they affect warning, command, and public confidence.

In cyberspace, deterrence is more reliable through denial than through punishment. Coercive punishment by disrupting infrastructure can be a poor signal and is typically counterproductive, as the target is unable to verify authorship or determine limits, or resorts to a skittish response. In nuclear-shadowed rivalries, the greater danger is entanglement: attacks on dual-use networks that support

[22] Melissa Robbins, "Cyberattack Hits Indian Nuclear Plant," *Arms Control Association*, December 2019.

conventional forces may be interpreted as preparations to blind nuclear command, control, and intelligence.[23]

On 24 February 2022, a wiper attack against Viasat's KA-SAT modems degraded satellite connectivity across Europe within an hour of Russia's invasion of Ukraine, illustrating how cyber activity can accompany the use of force and spill across borders. In the Ukraine war, Russia employed wiper malware, cyber espionage, and disinformation campaigns. While these did not alter the strategic balance against a well-defended Ukraine, they caused notable disruptions and delays in military and governmental operations. NotPetya in 2017 likewise produced global collateral losses far beyond its intended target, underscoring the hazards of escalation and misattribution.[24]

Unlike traditional military deterrence, which relies on kinetic force or nuclear capabilities, disrupting infrastructure through the cyber domain offers a non-kinetic approach to exerting pressure and deterring adversaries, allowing for a more nuanced strategy tailored to specific geopolitical situations while avoiding the immediate risks of kinetic warfare. This method can also help control escalation by signalling resolve and capability without resorting to direct military confrontation, which might lead to unintended escalation or broader conflicts.[25]

Implementing infrastructure disruption as a deterrent presents significant challenges, such as the usage of the Stuxnet worm, reportedly developed by the US and Israel, which targeted Iran's nuclear enrichment facilities. This attack demonstrates how cyber tools can be used to physically damage critical systems without traditional kinetic warfare, disrupting a nation's strategic capabilities.

Similarly, Cyber espionage is a significant threat, as it allows adversaries to gain access to sensitive information that could compromise national security. The SolarWinds hack, attributed to Russia, infiltrated numerous US government agencies, potentially exposing classified information and undermining trust in digital infrastructure.[26] Cyber can support strategic stability when it hardens the provision of

[23] James M. Acton, "Escalation through Entanglement.

[24] Cybersecurity and Infrastructure Security Agency, "Petya/NotPetya Ransomware," Alert, February 15, 2018, https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware.

[25] Zafar Nawaz Jaspal, "Paradox of Deterrence: India-Pakistan Strategic Relations," Institute of Strategic Studies, Islamabad, 2014, https://issi.org.pk/wp-content/uploads/2014/06/1299649036_25635225.pdf.

[26] Zafar Nawaz Jaspal, "Paradox of Deterrence: India-Pakistan Strategic Relations".

critical services, improves detection, and enables faster, more accurate verification. On the other hand, it undermines stability when it targets dual-use C3I, causes cascading outages, or is combined with opaque information operations.

5.2.1 India and Cyber Warfare

India seeks a technological advantage in cyberspace and has established dedicated institutions, including the Defence Cyber Agency and the National Technical Research Organisation, to coordinate operational capability and intelligence support. Partnerships reinforce this ambition. India is Israel's largest defence customer, with transfers including radars, drones, and related systems; industry collaborations such as Elbit–Adani on Hermes-900 and the Drishti-10 programme illustrate the pipeline of dual-use sensing and data links relevant to cyber-enabled operations.[27]

India has been developing a robust framework for cyber capabilities. The National Cyber Security Policy 2013 and subsequent updates outline India's goals for becoming a leading cyber power, including strengthening both offensive and defensive cyber capabilities. On the intrusive side, investigations have documented the alleged use of NSO Group's Pegasus against journalists and activists in India; although official confirmation is disputed, forensic analysis and a Supreme Court-mandated inquiry keep the allegation alive.

Open-source threat intelligence links several India-nexus groups to espionage against Pakistani and regional targets. Confucius has deployed Android surveillanceware (Hornbill, SunBird) and conducted spear-phishing against Pakistani military interests.[28] SideWinder has repeatedly targeted Pakistan government entities with custom backdoors such as WarHawk and campaign-specific polymorphism.[29]

The DoNot team has mounted recurring operations against Pakistani Android users.[30] These activities prioritise credential theft, long-dwell collection, and marginal

[27] Stockholm International Peace Research Institute (SIPRI), "Recent Trends in International Arms Transfers in the Middle East and North Africa," April 10, 2025, noting India as 34 percent of Israeli exports.

[28] Daniel Lunghi, "Confucius Uses Pegasus Spyware-Related Lures to Target Pakistani Military," *Trend Micro*, August 17, 2021, https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html.

[29] Niraj Shivtarkar and Avinash Kumar, "WarHawk: New Backdoor Arsenal from SideWinder APT Group," *Zscaler*, October 21, 2022.

[30] Broadcom/Symantec, "DoNot APT Targeting Pakistani Android Mobile Users," July 30, 2024, https://www.broadcom.com/support/security-center/protection-bulletin/donot-apt-targeting-pakistani-android-mobile-users.

disruption rather than destructive effects. FireEye and CrowdStrike have also detailed the 2016 cyber-attacks on Pakistani energy infrastructure, allegedly linked to Indian cyber units, underscoring India’s cyber capabilities and intentions.

These capabilities can strategically undermine crisis stability through entanglement. Attacks on dual-use communications, satellite links, or government networks are difficult to attribute promptly and may be interpreted as attempts to blind command, control, and intelligence, potentially provoking pre-emptive action. Instances of spyware like "Pegasus" have raised concerns about surveillance and espionage, amplifying the already complex and volatile strategic relationship between the two countries.

5.2.2 Pakistan’s role and response in the Cyber Domain

Pakistan faces a rapidly evolving and increasingly dangerous cybersecurity landscape, marked by a significant surge in cyberattacks targeting government agencies, financial institutions, and critical infrastructure. The PTA has acknowledged these escalating threats, highlighting that the cyber risks to the banking sector have increased significantly. Kaspersky, a cybersecurity firm, reported a staggering 114% year-on-year increase in banking and financial malware attacks between January and October 2024, with these attacks primarily targeting digital financial transactions, thereby endangering both individuals and financial institutions.[31]

Phishing attacks, ransomware incidents, Distributed Denial of Service (DDoS) attacks, data breaches, and hacktivism have all become increasingly prevalent. Indian hacktivists, in particular, have been actively targeting the Pakistani government and corporate entities through DDoS attacks and website defacement. A key trend observed is the growing focus on mobile devices, which are becoming increasingly vulnerable to financial cyberattacks. Operationally, Pakistan’s National Cyber Emergency Response Team has begun issuing time-bound advisories to ministries and operators in response to emerging campaigns, reflecting a shift from ad-hoc warnings to coordinated national guidance.

[31] Jawwad Rizvi, “Cyber Threats in Pakistan’s Finance Sector Surge by 114pc in 2024: Report,” *The News International*, November 18, 2024, https://www.thenews.com.pk/print/1252393-cyber-threats-inApakistan-s-finance-sector-surge-by-114pc-in-2024-report.

Indian hostilities are prominent in the cyber domain as well. A prominent example is the discovery by Pakistani intelligence authorities of an Indian spy network's cyberattack aimed at Pakistan's Armed Forces and government leaders. This attack involved sophisticated cybercrimes, including the manipulation of personal mobile devices and the technical equipment of military personnel and government officials.

The ability of cyberattacks to breach sensitive information and manipulate communications directly impacts national security and diplomatic relations. This incident underscores how cyber capabilities can significantly complicate the strategic relationship between India and Pakistan. To close governance gaps, the government announced a National Cyber Security Authority to be operational by 2025, including a certification laboratory whose clearances will be mandatory for critical deployments from July 2028.

The PTA has launched a Cyber Security Strategy for the telecom sector that is being implemented in the period 2023-2028. This five-year project is structured around six pillars: public awareness, technical expertise, proactive surveillance and response, cyber resilience, strengthening the legal environment, and collaborative engagement. The approach is based on a collective governance model that involves dynamic involvement of government agencies, private sector operators, universities, regulatory bodies, telecommunication service providers, cybersecurity companies, and community organisations.

At the same time, Pakistan is strengthening its role in global cybersecurity governance for the purpose of strategic stability. The country is an active member of international forums such as the UN Open-Ended Working Group on ICT security. Within these platforms, Pakistan pushes for the development of a binding international instrument that can help to guide responsible state behaviour in cyberspace.[32] Such cooperation not only enhances Pakistan’s defence mechanisms but also serves as a deterrent against external cyber threats, including those emanating from India.

[32] Permanent Mission of Pakistan to the United Nations, “Formulation of Position for the Annual Progress Report (APR) of the UN Open-Ended Working Group (OEWG) on ICT Security,” statement by Ambassador Usman Jadoon, Julz; UNODA, “General Assembly First Committee, Seventy-Ninth Session: Pakistan submission,” 2024.

In capacity building, NASTP supports Pakistan’s cyber preparedness by co-locating Air University’s National Centre for Cyber Security and the National Cyber Security Academy at NASTP Alpha, linking research, training, and operators. The Academy, inaugurated in November 2021 at Air University, builds practitioner pipelines for defence and incident response. NASTP showcases cyber, secure communications, AI, and simulation capabilities alongside aerospace systems, signalling an integrated R&D-to-fielding pathway for the services. It also hosts industry collaboration and workspace programmes, accelerating adoption and skills development across the ecosystem.

Moreover, while Pakistan’s primary focus has been on defence, the country is also building its cyber intelligence and limited offensive capabilities. Agencies such as the National Technical Research Organisation (NTRO) and others are developing cyber espionage and counterintelligence operations to track and neutralise foreign cyber threats. Though the development of offensive capabilities remains a sensitive issue, particularly in the context of Pakistan’s regional security dynamics, these efforts are necessary to ensure that Pakistan is not left vulnerable in the face of increasingly aggressive cyber operations from adversaries like India.

During the 2025 crisis, Pakistan delivered an effective multi-domain response, with cyber units recording a “67–0” score.[33] However, as with other technologies, cyber is highly exploitable. Its routine civil use may not affect stability, but intrusions into critical military systems carry the risk of escalation and crisis compression.

5.3 Space Asymmetries

The emerging space capabilities of India and Pakistan present both strategic opportunities and potential vulnerabilities that require careful consideration. While the historical context of the Cold War underscores the role of space in strategic modernisation and nuclear arms control, the present environment calls for a reassessment of these dynamics within the South Asian context. For deterrence analysis, space is significant because satellites underpin C3ISR, early warning, and secure communications. Their dual-use nature creates an “entanglement” with nuclear

[33] Centre for Aerospace & Security Studies, *Artificial Intelligence, Electronic & Cyber Warfare and Unmanned Aerial Systems: New Paradigm of Next Generation Aerial War* (Lahore: Centre for Aerospace & Security Studies, July 2025).

command and control, heightening risks if space systems are threatened or misinterpreted during a crisis. Recent behaviour in orbit highlights why South Asia should treat space as a stability variable rather than a backdrop. In May 2025, a Russian 'inspector' satellite (Cosmos-2576) manoeuvred unusually close to a US government satellite,[34] demonstrating the risks of co-orbital proximity operations. Such actions complicate attribution and crisis signalling.

5.3.1 India's Role in the Space Domain

India's space programme is managed by the government-backed Indian Space Research Organisation (ISRO), which has developed a broad range of expertise in space technologies, notably in launching and deploying indigenously designed satellites in different orbits (Geostationary Transfer Orbit, Low Earth Orbit, Medium Earth Orbit). Under Prime Minister Modi, who has made liberalisation of the space sector a key priority of his government, the country is looking to increase its contribution to the global space economy by a factor of five.

This vision is complemented by an extraordinary surge in funding and investments, which are vital for India's rise as a player in the global space arena. Since 2019, India has also established a dedicated defence space architecture (including the formation of the Defence Space Agency) and conducted a successful test of a direct-ascent anti-satellite missile (Mission Shakti). These initiatives are part of India's approach to outer space deterrence and the integration of space-enabled capabilities into its overall defense architecture.

Further, ISRO recently celebrated the first-ever National Space Day with the theme "Touching Lives while Touching the Moon: India's Space Saga," which was celebrated on the first anniversary of the successful landing of the Chandrayaan-3 mission near the lunar south pole. Similarly, certain timelines were reiterated by PM Modi, to chart future space exploration ambitions, such as India's plans for its human spaceflight mission Gaganyaan (2025), the Chandrayaan 4 mission to collect lunar samples and bring it back (2027), its space station between 2028-2035, specific plans

[34] Theresa Hitchens, "Russia's New 'Cosmos' Inspector Satellite Now Orbiting Near US Sat: Space Command," *Breaking Defense*, 30 May 2025, https://breakingdefense.com/2025/05/russias-new-cosmos-inspector-satellite-now-orbiting-near-us-sat-space-command/.

to build a heavy lift rocket, called Soorya (Next Generation Launch Vehicle-NGLV) and the first Indian human mission to the Moon by 2040.[35]

Likewise, India is also working to produce Heavy Lift Launch Vehicles (HLVs) and Super Heavy-Lift Launch Vehicles (SHLVs), which are designed to deliver payloads weighing between 50 and 100 tons, and also reusable launch vehicles. Similarly, its development of anti-satellite capabilities has heightened security concerns in Pakistan and necessitated a strategic response to maintain regional stability. [36] The S-400 missile system and space-based detection were sought to provide early warning of approaching missiles, so the integration of satellite networks in space could strengthen India's BMD even more.

Operationally, the launch of EMISAT (2019) demonstrates a focus on electronic intelligence to map emitters and improve cueing for air and air-defence missions; this strengthens denial against conventional threats but can be interpreted as enabling counterforce if fused with missile-defence sensors during a crisis.[37] Analytically, India’s space posture contributes to stability through enhanced sensing and communications. Yet, it also compresses decision time and complicates signalling if dual-use satellites are perceived to support missions that could degrade an adversary’s nuclear C3I.

5.3.2 Pakistan's contributions in the Space Domain

Pakistan’s civil space activities (led by SUPARCO) are separate from its aerospace initiatives (led by the PAF). Islamabad states that it does not seek to militarise space, and has instead prioritised resilient communications and earth-observation capabilities for socio-economic and disaster-response purposes, with clear defence spillovers in crisis management.

Pakistan's aerospace and space domain also has many important satellites under development, increasing its capabilities. Pakistan successfully launched a Chinese Long March 4B rocket in 2023, marking an important milestone in its earth

[35] Namrata Goswami. “Innovations in Space: How is India Shaping its Space Program.” https://www.natstrat.org, April 22, 2021. https://www.natstrat.org/articledetail/publications/innovations-in-space-how-is-india-shaping-its-space-program-160.html.

[36] Noor, Sitara, “Strategic Stability in South Asia: The Evolving Challenges and Potential Opportunities for India and Pakistan.” Journal-article, n.d. https://www.issi.org.pk/wp-content/uploads/2023/08/Sitara_Noor_SS_No_1_2023.pdf.

[37] Indian Space Research Organisation (ISRO), “EMISAT,” updated 1 May 2023, https://www.isro.gov.in/EMISAT.html.

observation capabilities designed for natural disasters, agricultural development, and monitoring of water resources.[38] The PAKSAT-MM1R communications satellite, launched in May 2024 on a Long March-3B from Xichang, expands sovereign backhaul capability across multiple bands for both government and commercial users.[39]

The iCube-Qamar CubeSat, launched on China's Chang'e-6 mission in 2024, returned imagery from lunar orbit, signalling increased national capacity in small-satellite engineering and international collaboration. PRSC-EO1 entered orbit on 17 January 2025, adding domestic electro-optical tasking to support resource management and disaster response. These are publicly civil assets, yet they also strengthen assured access to imagery and connectivity during a crisis, reducing reliance on foreign providers and enhancing C4ISR resilience.

Analytically, Pakistan's declared "non-weaponisation" stance in space, together with its investments in sovereign communications and data, aligns with deterrence by denial and with reducing misperception. The risk lies in the possibility that dual-use earth-observation or data-links are targeted or jammed; under entanglement, an attack on "civil" satellites that support decision-making could be interpreted as pre-emptive preparation against nuclear C3I. Therefore, Pakistan's "civil-first" space posture is a stabilising factor only if accompanied by norms and incident channels that keep space systems off the escalatory ladder.

6. STRATEGIES TO COUNTER THREATS BY EMERGING TECHNOLOGIES

Cold War strategies allowed the two states to balance deterrence with control: Flexible Response provided graded choices, clear crisis lines reduced chances of misreading the other side's intent, and complete separation of nuclear command and control allowed the states to maintain full control in the strategic domain. The same habits can be adapted to software, networks, and satellites in the India–Pakistan setting.

[38] Andrew Jones and Andrew Jones, "China Launches Earth Observation Satellite for Pakistan," SpaceNews, January 17, 2025.

[39] Dawn, "PAKSAT-MM1R embarks on successful journey into space," 30 May 2024, https://www.dawn.com/news/1837120.

6.1 Flexible Response for the multi-domain era

An array of flexible response options in the cyber and space domains could mirror earlier graded choices by the Cold War states. Clear thresholds for attribution, limited countermeasures that stop short of force, and round-the-clock technical points of contact paired with diplomatic lines would help ensure that malware outbreaks or satellite glitches are not read as intent. Additionally, regular mock exercises across ministries and services can keep these choices familiar and predictable.[40]

6.2 Deterrence by denial and resilience

Redundancy, wide dispersal, and continuity translate into strengthened C3 and intelligence. With emerging technologies, this diversification can be achieved through sovereign satellites and terrestrial backups, and planning for rapid reconstitution of critical services in case of an attack. Steps that echo arms-control instincts may help. This can include pre-notification of high-altitude tests in the space domain, a debris-free moratorium on anti-satellite activity, limited telemetry sharing during missile defence trials, and brief transparency notes on where autonomy is used and how it is overseen. In practice, what tends to matter is uptime, complete audit logs, and credible public messaging during disruption.

6.3 Human control and cyber exclusion zones near nuclear command, control, and communications

Positive human control over all strategic assets remains the anchor in order to maintain full awareness of all functions at all times. This posits ring-fencing nuclear command chains from autonomous functions, keeping human-in-the-loop and air-gapping from the public internet. In addition, keeping human authorisation traceable with clear records and audits can also help in adding a layer of protection while ensuring a chain of command. While such measures may slow decision-making, in the long run, they lower the chance of misinterpretation, while leaving room for modernisation in sensing, denial, and recovery.[41]

[40] North Atlantic Treaty Organization, *MC 14/3 (Final): A Report by the Military Committee on the Overall Strategic Concept for the Defense of the North Atlantic Treaty Area* (Brussels, 16 January 1968).

[41] *UNGA, OEWG on ICTs, A/79/214 (2024).*

7. CONCLUSION

Taken together, the evidence shows that Cold War stability logics still travel in South Asia, but only when three safeguards are built into modern systems: human authorisation, transparent incident handling, and resilient dual-use networks. Where those features exist, AI, cyber, and space tools slow crises and sharpen verification; where they are absent, the same tools compress political time and tangle civilian and military systems, undermining stability. This conditional reading of the results sets up the policy core that follows.

Evidence from 2019 to 2025, especially the May 2025 episode, shows that digital tools can pull in opposite directions. Artificial intelligence and cyber capabilities can cushion escalation by improving verification and disciplining flows of information. The same tools can also compress political time and blur intent when automation, coordinated online activity, or pressure on mixed civilian and military networks enters a crisis. India’s drive for AI-enabled sensing and teaming improves denial against conventional threats, yet invites counterforce ambiguity if combined with missile defence cueing. Pakistan’s path, centred on institutional capacity in centres like CENTAIC and NASTP, telecom sector cyber governance, and a consistent human-in-the-loop practice, leans toward deterrence by denial and helps preserve decision authority. Even so, action and reaction continue below the nuclear threshold.

The Cold War logics travel best when recast for a multi-domain setting. Flexible Response becomes a practical ladder of graded, reversible options supported by staffed incident channels. Restraint around NC£ relies less on counting warheads and more on auditable human authorisation that preserves a deliberate pause at the last step. Deterrence by denial is judged by resilience in C3ISR, and in critical services, including uptime, fail-safe modes, reconstitution speed, and completeness of logs.

Cold War dynamics do not fail in South Asia. They work conditionally when human judgment, transparency, and resilience are built into the AI, cyber, and space architectures that shape decisions in a crisis.

BIBLIOGRAPHY

———. "Confucius Uses Pegasus Spyware-Related Lures to Target Pakistani Military." August 17, 2021. https://social.cyware.com/news/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani-military-008c4a51

———. "Pakistan's iCube-Qamar Takes Images of Moon's Far Side." May 8, 2024. https://www.dawn.com/news/1824687.

———. *Agreement between India and Pakistan on Pre-Notification of Flight Testing of Ballistic Missiles*, October 3, 2005. https://www.mea.gov.in/portal/legaltreatiesdoc/pa05b0591.pdf.

AAJ News (English). "'Cyber Security Authority' to Be Established in 2025." July 26, 2024. https://english.aaj.tv/news/330371465/cyber-security-authority-to-be-established-in-2025.

Acton, James M., Li Bin, and Tong Zhao. *Reducing the Risks from Nuclear Entanglement*. Washington, DC: Carnegie Endowment for International Peace, September 2018. https://carnegie-production-assets.s3.amazonaws.com/static/files/Acton_Entanglement_Sept2018.pdf.

Akram, Muhammad Shahzad. "Digital Shadows: The Menace of Cyber Espionage and Pakistan's National Security." *Journal of Development and Social Sciences* 4, no. III (September 30, 2023). https://doi.org/10.47205/jdss.2023(4-iii)80.

Altaf, Zohaib, and Zohaib Altaf. "Pakistani Perspective on AI, Indian Elections, and Mitigating Technological Risks." *CISSAJK*, June 5, 2024. https://cissajk.org.pk/2024/06/05/pakistani-perspective-on-ai-indian-elections-and-mitigating-technological-risks/.

Amnesty International. "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware." December 28, 2023. https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/.

Arab News Pakistan. "Pakistan Warns Key Ministries of 'Severe' Ransomware Risk." August 11, 2025. https://www.arabnews.com/node/2611347/pakistan.

Bano, Sher. "India's Militarization of Outer Space: Implications for Pakistan." *SVI – Strategic Vision Institute* (blog), August 29, 2020. https://thesvi.org/indias-militarization-of-outer-space-implications-for-pakistan/.

Broadcom/Symantec. "DoNot APT Targeting Pakistani Android Mobile Users." July 30, 2024. https://www.broadcom.com/support/security-center/protection-bulletin/donot-apt-targeting-pakistani-android-mobile-users.

Business Recorder. "'Cyber Security Authority to Be Set Up by 2025'." July 26, 2024. https://www.brecorder.com/news/40314368.

CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems. *Revised Rolling Text as of 12 May 2025*. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_%282025%29/CCW_GGE_LAWS_-_Revised_rolling_text_as_of_12_May_2025.pdf.

Centre for Aerospace & Security Studies. *Artificial Intelligence, Electronic & Cyber Warfare and Unmanned Aerial Systems: New Paradigm of Next Generation Aerial War*. Lahore: Centre for Aerospace & Security Studies, July 2025.

Chopra, Air Marshal Anil. "Space Is the New Frontier: Time for India to Increase Strategic Focus." *Firstpost*, January 1, 2024. https://www.firstpost.com/opinion/space-is-the-new-frontier-time-for-india-to-increase-strategic-focus-13563432.html.

CloudSEK. "Brief Disruptions, Bold Claims: The Tactical Reality Behind the India–Pakistan Hacktivist Surge." May 30, 2025. https://www.cloudsek.com/blog/brief-disruptions-bold-claims-the-tactical-reality-behind-the-india-pakistan-hacktivist-surge.

Cybersecurity and Infrastructure Security Agency. "Petya/NotPetya Ransomware." Alert, February 15, 2018. https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware.

Dawn. "PAKSAT-MM1R Embarks on Successful Journey into Space." May 30, 2024. https://www.dawn.com/news/1837120.

European Commission. "IRIS² Secure Connectivity." December 16, 2024. https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en.

Goswami, Namrata. "Innovations in Space: How Is India Shaping Its Space Program." *NatStrat*, April 22, 2021. https://www.natstrat.org/articledetail/publications/innovations-in-space-how-is-india-shaping-its-space-program-160.html.

Government of India and Government of Pakistan. *Lahore Declaration*, February 21, 1999. https://media.nti.org/documents/lahore_declaration.pdf.

Guramani, Nadir. "Pakistan's iCube-Qamar Beams Back First Images from Moon's Orbit." *Dawn*, May 10, 2024. https://www.dawn.com/news/1832658.

Hitchens, Theresa. "Russia's New 'Cosmos' Inspector Satellite Now Orbiting Near US Sat: Space Command." *Breaking Defense*, May 30, 2025.

https://breakingdefense.com/2025/05/russias-new-cosmos-inspector-satellite-now-orbiting-near-us-sat-space-command/.

Horowitz, Michael C., and Alexander Velez-Green. “A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence.” *Semantic Scholar*, December 11, 2019. https://www.researchgate.net/publication/337904570_A_Stable_Nuclear_Future_The_Impact_of_Autonomous_Systems_and_Artificial_Intelligence.

India. “Submission Pursuant to UNGA Resolution 78/241 (LAWS).” May 2024. https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_%282024%29/78-241-India-EN.pdf.

Indian Space Research Organisation (ISRO). “EMISAT.” Updated May 1, 2023. https://www.isro.gov.in/EMISAT.html.

International Institute for Strategic Studies. “Strategic Stability in South Asia: The Evolving Challenges and Potential Opportunities for India and Pakistan.” *Journal article* , n.d. https://www.issi.org.pk/wp-content/uploads/2023/08/Sitara_Noor_SS_No_1_2023.pdf.

International Institute for Strategic Studies. *Transcript of Lt. General Khalid Kidwai’s Keynote Address: Seventh IISS–CISS Workshop on “South Asian Strategic Stability: Deterrence, Nuclear Weapons and Arms Control”*, London, February 6, 2020. https://www.iiss.org/globalassets/media-library---content--migration/files/events/2020/transcript-of-lt-general-kidwais-keynote-address-as-delivered---iiss-ciss-workshop-6feb20.pdf.

Jadoon, Usman. “Formulation of Position for the Annual Progress Report (APR) of the UN Open-Ended Working Group (OEWG) on ICT Security.” Statement by the Permanent Mission of Pakistan to the United Nations, July 11, 2024. https://pakun.org/uploads/07112024_01_8801ac2dd2.pdf.

Jamal, Sana. “Pakistan’s First National Cyber Academy Launched.” *Gulf News*, November 24, 2021. https://gulfnews.com/world/asia/pakistan/pakistans-first-national-cyber-academy-launched-1.83925731.

Jaspal, Zafar Nawaz. “Paradox of Deterrence: India-Pakistan Strategic Relations.” Institute of Strategic Studies, Islamabad, 2014. https://issi.org.pk/wp-content/uploads/2014/06/1299649036_25635225.pdf.

Javed, Nimrah, and Zohaib Altaf. “The Militarisation of AI in South Asia.” *South Asian Voices*, March 25, 2024. https://southasianvoices.org/sec-c-pk-r-militarisation-of-ai-01-16-2024/.

Jervis, Robert. “Cooperation Under the Security Dilemma.” *World Politics* 30, no. 2 (January 1978): 167–214. https://doi.org/10.2307/2009958.

Johnson, James. “Deterrence in the Age of Artificial Intelligence & Autonomy: A Paradigm Shift in Nuclear Deterrence Theory and Practice?” *Defense & Security Analysis* 36, no. 4 (2020): 422–448. https://doi.org/10.1080/14751798.2020.1857911.

Johnson, Kaitlyn, et al. *Space Threat Assessment 2025*. Washington, DC: Center for Strategic and International Studies, April 25, 2025. https://aerospace.csis.org/space-threat-assessment-2025/.

Jones, Andrew. “China Launches Earth Observation Satellite for Pakistan.” *SpaceNews*, January 17, 2025. https://spacenews.com/china-launches-earth-observation-satellite-for-pakistan/.

Kahn, Herman. *On Thermonuclear War*. Princeton, NJ: Princeton University Press, 1960.

Khattak, Masood Ur Rehman. “The Indian Army’s Land Warfare Doctrine 2018.” *IPRI Journal* 20, no. 1 (Winter 2020). https://ipripak.org/wp-content/uploads/2020/06/Article-5-IPRI-Journal-XX-I-Ind-Arm-New-Lan-ED-SSA-FINAL.pdf.

Ladwig, Walter C., III. “A Cold Start for Hot Wars? The Indian Army’s New Limited War Doctrine.” *International Security* 32, no. 3 (2007): 158–190. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/IS3203_pp158-190.pdf.

Lunghi, Daniel. “Confucius Uses Pegasus Spyware-Related Lures to Target Pakistani Military.” *Trend Micro*, August 17, 2021. https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html.

Mallory, King. *New Challenges in Cross-Domain Deterrence*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE259.html.

Matamis, Joaquin. “India’s Military Modernisation Efforts under Prime Minister Modi.” *Stimson Center*, June 27, 2024. https://www.stimson.org/2024/indias-military-modernisation-efforts-under-prime-minister-modi/.

Mazarr, Michael J., and Ivana Ke. *Integrated Deterrence as a Defense Planning Concept*. Santa Monica, CA: RAND Corporation, 2024. https://www.rand.org/content/dam/rand/pubs/perspectives/PEA2200/PEA2263-1/RAND_PEA2263-1.pdf.

Melissa Robbins. “Cyberattack Hits Indian Nuclear Plant.” *Arms Control Association*, December 2019. https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant.

Ministry of External Affairs (India). “Frequently Asked Questions on Mission Shakti, India’s Anti-Satellite Missile Test Conducted on 27 March, 2019.” 2019. https://www.mea.gov.in/press-releases.htm?dtl/31179/.

National CERT Pakistan. “Important Local Remote Code Execution Vulnerability in Microsoft Outlook.” Advisory NCA-28.051625, May 16, 2025. https://pkcert.gov.pk/advisory/25/28.pdf.

Niraj Shivtarkar, and Avinash Kumar. “WarHawk: New Backdoor Arsenal from SideWinder APT Group.” *Zscaler*, October 21, 2022. https://www.zscaler.com/blogs/security-research/warhawk-new-backdoor-arsenal-sidewinder-apt-group.

Noor, Sitara. “Pakistan’s Evolving Nuclear Doctrine.” *Arms Control Association*, October 2023. https://www.armscontrol.org/act/2023-10/features/pakistans-evolving-nuclear-doctrine.

North Atlantic Treaty Organization. *MC 14/3 (Final): A Report by the Military Committee on the Overall Strategic Concept for the Defense of the North Atlantic Treaty Area*. Brussels, January 16, 1968. https://www.nato.int/docu/stratdoc/eng/a680116a.pdf.

Obaid, Malahat. “PTA Issues Cyber Security Strategy 2023–2028 for Pakistan’s Telecom Sector: A Five Year Plan Towards Digital Resilience.” July 4, 2024. https://www.pta.gov.pk/category/pta-issues-cyber-security-strategy-2023-2028-for-pakistans-telecom-sector-a-five-year-plan-towards-digital-resilience-980103515-2024-07-04.

Pakistan. “Elements of an International Legal Instrument on Lethal Autonomous Weapons Systems (LAWS).” Working paper submitted to the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Geneva, March 4–8 and August 26–30, 2024. https://documents.unoda.org/wp-content/uploads/2024/03/CCW_GGE_2024_WP.4_Pakistan.pdf.

Pandit, Rajat. “India Finally Taking Some Steps to Leverage AI for Military Applications.” *The Times of India*, February 14, 2022. https://timesofindia.indiatimes.com/india/india-finally-taking-some-steps-to-leverage-ai-for-military-applications/articleshow/89559262.cms.

Profit by Pakistan Today. “PAF Establishes Centre for Artificial Intelligence and Computing.” August 31, 2020. https://profit.pakistantoday.com.pk/2020/08/31/paf-establishes-center-for-artificial-intelligence/.

Rafiq, Aamna. “Challenges of Securitising Cyberspace in Pakistan.” *Strategic Studies* 39, no. 1 (April 24, 2019): 90–101. https://doi.org/10.53532/ss.039.01.00126.

Reuters. "Pakistan Launches First Home-Made Observation Satellite." January 15, 2025. https://www.reuters.com/world/asia-pacific/pakistan-launches-first-home-made-observation-satellite-2025-01-15/.

Rizvi, Jawwad. "Cyber Threats in Pakistan's Finance Sector Surge by 114pc in 2024: Report." *The News International*, November 18, 2024. https://www.thenews.com.pk/print/1252393-cyber-threats-inApakistan-s-finance-sector-surge-by-114pc-in-2024-report.

Roy, Annapurna. "Indian AI Startups Funding Plunges 91% to $8.2 Million in Q2." *The Economic Times*, July 17, 2024. https://economictimes.indiatimes.com/tech/artificial-intelligence/indian-ai-startups-funding-plunges-91-to-8.2-million-in-q2/articleshow/111759520.cms?from=mdr.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

SIPRI (Stockholm International Peace Research Institute). "Recent Trends in International Arms Transfers in the Middle East and North Africa." April 10, 2025. https://www.sipri.org/commentary/topical-backgrounder/2025/recent-trends-international-arms-transfers-middle-east-and-north-africa.

Steff. "Nuclear Deterrence in a New Age of Disruptive Technologies and Great Power Competition." 2020. https://www.springerprofessional.de/en/nuclear-deterrence-in-a-new-age-of-disruptive-technologies-and-g/17572052.

Swope, Clayton, Kari A. Bingen, Makena Young, Madeleine Chang, Stephanie Songer, and Jeremy Tammelleo. *Space Threat Assessment 2024*. Washington, DC: Center for Strategic and International Studies, April 17, 2024. https://aerospace.csis.org/wp-content/uploads/2024/04/240417_Swope_SpaceThreatAssessment_2024.pdf.

Syed, Baqir Sajjad. "Probe into Cyberattack by Indian Spy Networks Launched." *Dawn.com*, August 13, 2020. https://www.dawn.com/news/1574108.

Topychkanov, Petr. "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk." *SIPRI Policy Paper*. Stockholm International Peace Research Institute, April 2020. https://www.sipri.org/sites/default/files/202004/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov_1.pdf.

U.S. Department of State. *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy* (inaugural plenary, March 19–20, 2024). https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy.

United Nations General Assembly. *Lethal Autonomous Weapons Systems*. A/RES/78/241. December 22, 2023. https://documents.un.org/doc/undoc/gen/n23/431/11/pdf/n2343111.pdf.

United Nations General Assembly. *Open-Ended Working Group on Security of and in the Use of ICTs (2021–2025), Third Annual Progress Report*. A/79/214. July 22, 2024. https://docs.un.org/en/A/79/214.

United Nations Office for Disarmament Affairs (UNODA). "General Assembly First Committee, Seventy-Ninth Session: Pakistan Submission." 2024. https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_%282024%29/78-237-Pakistan-EN.pdf.

Viasat. "KA-SAT Network Cyber Attack Overview." March 30, 2022. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/.

Vivek, N. D. "AI and Indian Defence: Enhancing National Security Through Innovation." *The Diplomat*, October 1, 2024. https://thediplomat.com/2024/10/ai-and-indian-defense-enhancing-national-security-through-innovation/.

Waltz, Kenneth N. *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979.

Webdesk. "Pakistan to Establish National Cyber Security Authority by 2025." *CSO Pakistan*, August 1, 2024. https://csopakistan.com/pakistan-to-establish-national-cyber-security-authority-by-2025/.