ARTICLES

The Future of Limited War Between Nuclear Powers: Lessons from India-Pakistan Escalation Patterns

Author: Sanjay Panicker Reghulal • **Published:** July 04, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Limited war between nuclear powers is no longer shaped only by missiles, aircraft and artillery. In South Asia, the India-Pakistan rivalry is entering a more unstable phase where drones, AI-enabled systems, cyber operations, information warfare and multi-domain targeting are compressing decision timelines and blurring escalation thresholds. This article argues that nuclear deterrence still constrains full-scale war, but the space below the nuclear threshold is becoming faster, more crowded and more dangerous, making future crises harder to control and limited war more tempting for both sides.

Introduction

Limited war between nuclear power states within South Asia is becoming harder to manage in the age of drones, AI, cyber operations, and multi-domain conflict.[i] While the basic logic of the catastrophic consequences of full-scale nuclear exchange is ingrained in regional deterrence doctrines, the space below that nuclear level has become more crowded, faster, and much more unstable in recent years.[ii] Escalation patterns between Islamabad and New Delhi show that crises are no longer shaped only by artillery, aircraft, and missiles but also by drones, surveillance systems, cyber disruption, information warfare, and autonomous technologies. This creates new opportunities for coercion but

makes escalation control all the more difficult to exercise.

The real issue is not whether nuclear deterrence has disappeared but rather that the layers of conflict below nuclear use are changing in ways that make limited war more tempting and less predictable. In a future crisis, states may believe they can punish, signal resolve, or degrade an adversary without triggering nuclear retaliation and pioneer gray-zone tactics.[iii] However, every new tool that seems to offer precision and control can also compress decision times, blur thresholds, and produce miscalculations. India-Pakistan is especially important because it is one of the clearest examples of two nuclear armed rivals repeatedly fighting under the guise of escalation.

Escalation control is getting harder

The first major lesson is that escalation control is becoming more difficult as contemporary warfare shifts towards an accelerated and non-linear pattern.[iv] Before the Cold War, heads of state had more time to interpret signals, assess damage, and communicate warnings. Today, autonomous systems, drones, and AI-enabled targeting compress the *kill chain,*i.e., the sequence of actions from detection of targets to strike, from minutes to seconds. This is especially dangerous in South Asia where both India and Pakistan have strong incentive structures for rapid signalling but also deep mistrust.[v] Control structures and human oversight remain essential in this environment as they reduce the chance of unauthorized escalation and premature retaliation. However, human oversight itself is under pressure because the speed of modern conflict is reaching a point of *AI Singularity,* where machine driven decisions happen so fast that meaningful human review becomes functionally impossible that a local incident turns into a regional escalation.

Artificial Intelligence becomes especially important here. AI is often described as the third revolution in warfare after gunpowder and nuclear weapons because it changes the speed and structure of military decision making. It allows systems to process information faster, identify targets quickly and support military action within minute response times.[vi] In South Asia, this matters because AI is not just improving weapons performance but also fosters a false sense of supremacy where states believe they can control escalation through superior technology which might potentially lead to more aggressive behavior. This technological shift exacerbates the *Stability-Instability Paradox* which tempts states to pursue limited war under the nuclear overhang. This fragility was evidenced during a May 2025 conflict where AI generated disinformation was weaponized to intensify tensions and compel both governments toward hawkish public stances.[vii] Future stability will depend on whether states can overcome “siloed governance” to develop a common understanding of strategic values. This entails updated crisis communication channels, hotlines, and pre-notification rules for multi-domain operations. [viii] In the absence of such mechanisms, limited war becomes harder to contain.

Drones and AI defining deterrence

While nuclear weapons still create the highest level of deterrence because their destructive power is so extreme that the cost of use is politically and militarily unacceptable, drones and AI have redefined deterrence at the conventional level of military operations.[ix] Drones and other UAS systems are attractive because they are relatively cheap and are capable of performing deep-theater strikes within enemy territory. They can be launched more discreetly than manned aircraft or missile systems and they can be used repeatedly at lower costs. This creates what is defined as an *economy of scale* where the cost of production per unit becomes significantly cheaper in the long run due to intensified production. A state does not need to spend as much as it would large missile or attrition campaigns to create pressure but could rather sustain a lower-cost campaign of reconnaissance or symbolic strikes. This reduced entry level makes limited war more feasible and tempting for hawkish states. In the India-Pakistan context, drones become important because they can target military installations, surveillance systems, logistics nodes, and potentially even sensitive strategic assets. Drones create a more flexible and deniable layer of coercion beneath the nuclear use threshold.[x] Moreover, AI amplifies this effect further as AI-enabled drones can improve targeting accuracy, speed up target selection, and coordinate strikes

efficiently. This means that states may feel they can inflict damage while keeping the intensity of hostilities limited.

South Asian literature also suggests that AI militarization is already changing the deterrence balance.[xi] India has pursued AI development more proactively through institutions such as the Defence AI Council and the DRDO with applications ranging from Indian UAV systems like *Ghatak* and unmanned tanks like the *Muntra.*[xii] In contrast, Pakistan views Delhi's AI buildup as a direct national security concern and is trying to preserve deterrence despite serious economic and technological constraints. This widening gap in AI capabilities between India and Pakistan creates a "technological asymmetry" that threatens the existing balance of power.[xiii] Moreover, there exists a significant risk of AI-enhanced Intelligence, Surveillance, and Reconnaissance (ISR) and counterforce capabilities making traditional second-strike assets vulnerable to preemptive strikes which would undermine the Mutually Assured Destruction principle. In fact, the presence of superior AI capabilities may tempt New Delhi to fight a limited war under the nuclear grey area under the belief that they possess a relative edge at the conventional level.[xiv]

Operational thresholds are shifting

Operational thresholds in modern conflict are becoming much harder to define because war is no longer confined to clearly separated domains.[xv] Cyber operations, space assets, drones, electronic warfare, and precision strikes all blur the line between peace and war, making it difficult to judge when a state has crossed from coercion into escalation. This matters because decision makers now have to respond to actions that may be technically limited but strategically significant and the wrong interpretation can quickly widen a crisis. Cyber incidents are especially important in this regard because attribution is often contested and the legal meaning of an attack is not always clear. The Tallinn Manual which was developed by an international group of experts at NATO's invitation is useful here as it helps clarify how existing international law applies to cyber operations including sovereignty, state responsibility, and thresholds for response.[xvi] While this does not make cyber conflict any simpler, it does give states a framework for thinking about what counts as a hostile act and what kinds of responses might be lawful or proportionate. The ICRC likewise stresses that cyber operations are not law-free and that international humanitarian law still imposes limits on means and methods of warfare.[xvii]

A critical and often overlooked shift in operational logic is the distinction between risk and radical uncertainty.[xviii] While risk can be estimated via probability distributions, radical uncertainty occurs when the consequences of an action are unknown or the likelihood of those consequences cannot be calculated. In such environments, leaders may not actually know their own red lines in advance but instead they may discover their preferences through the Self Perception Theory which lets leaders infer their own attitudes and red lines only after observing their own behavior and the adversary's response.[xix] This creates an undefined threshold where a state might cross a point of no return without realizing it until the conflict has already escalated beyond its control. To manage these shifting thresholds, there is a growing call for behavioral arms control as since traditional arms control negotiations often lie between traditional powers, newer frameworks are needed that include civil society, the private sector, and non nuclear weapon states (NNWS).[xx] By establishing behavioral parameters, nations can begin to account for the increasing asymmetries in their capabilities and reduce the risk of inadvertent strategic escalation.

Operation Sindoor can be used here as a useful example of how limited war logic is evolving. If reports about a strike on Kirana Hills (Pakistan's nuclear testing region) are taken seriously as a point of analysis, it suggests a shift from merely punishing proxy violence via surgical incursions as illustrated in Uri to targeting infrastructure associated with Pakistan's strategic deterrent ecosystem. The broader implication suggests that India is increasingly willing to use limited war tools to deter state-sponsored cross border violence rather than relying only on conventional retaliation at the border. The operation reflects a broader shift in escalation logic where precision strikes and stand off capabilities can be used to signal resolve against both tactical attacks and the wider strategic infrastructure behind them. The significance is not

just the strike itself but rather the message it sends of how sub conventional violence can now trigger consequential retaliation more than before. At the same time, Pakistan's long standing use of low intensity conflict shows how the stability instability paradox continues to shape this region. Pakistan's strategy of prolonged, deniable pressure has often relied on the idea that the nuclear shadow limits India's response options.

A stronger takeaway is that states now need clearer playbooks for cyber incidents, drone incursions, border strikes, and other below-threshold acts. Without such rules even a "limited" operation can be read as a strategic escalation especially when sensitive infrastructure or deterrent related facilities are involved.

Footnotes:

[i]SIPRI, Addressing Multidomain Nuclear Escalation Risk (Stockholm: SIPRI, 2026)

[ii] Texas National Security Review, "Escalation Management in Ukraine: 'Learning by Doing' in Response to the Threat That Leaves Something to Chance," 2023.

[iii] Global Challenges Foundation, Multi-domain Escalation Risk (Stockholm: Global Challenges Foundation, 2026).

[iv] SIPRI, Addressing Multidomain Nuclear Escalation Risk (Stockholm: SIPRI, 2026)

[v] BBC News, "How real is the risk of nuclear war between India and Pakistan?" May 13, 2025.

[vi] Ibid

[vii] Nabiya Khan, Kaushik Raj, and Zenith Khan, "Inside the Misinformation and Disinformation War Between India and Pakistan,"*CSO Hate, May 16, 2025

[viii] Global Challenges Foundation, Multi-domain Escalation Risk.

[ix] International Committee of the Red Cross (ICRC), "The shifting battlefield: technology, tactics, and the risk of blurring lines of warfare," May 21, 2025.

[x] Institute of Strategic Studies Islamabad, India-Pakistan Development of Drones: Implications for Strategic Stability in South Asia (Islamabad: ISSI, 2025).

[xi]Tayyaba Khurshid, "The Impact of Artificial Intelligence Militarization on South Asian Deterrence Dynamics," BTTN Journal (2023).

[xii] Ibid

[xiii] Ibid

[xiv] Ibid

[xv] ICRC, "The shifting battlefield."

[xvi] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, ed. Michael N. Schmitt (Cambridge: Cambridge University Press, 2017).

[xvii] ICRC, "IHL and cyber operations during armed conflicts," 2023 short papers

[xviii] Texas National Security Review, "Escalation Management in Ukraine."

[xix] Rose McDermott, “Self-Perceptions and Nuclear Weapons,” RealClearDefense, July 14, 2023, https://www.realcleardefense.com/articles/2023/07/14/self-perceptions_and_nuclear_weapons_966021.html.

[xx] George Perkovich, *Rethinking a Political Approach to Nuclear Abolition* (Washington, DC: Carnegie Endowment for International Peace, March 2025).

References

1. Javed, Nimra, and Zohaib Altaf. “India-Pakistan Development of Drones: Implications for Strategic Stability in South Asia.” Institute of Strategic Studies Islamabad, March 18, 2025.
2. Khurshid, Tayyaba. “The Impact of Artificial Intelligence Militarization on South Asian Deterrence Dynamics.” BTTN Journal 2, no. 2 (2023): 134–50. https://bttn.org.pk/ojs/index.php/BTTN_Journal.
3. Stein, Janice Gross. “Escalation Management in Ukraine: ‘Learning by Doing’ in Response to the ‘Threat That Leaves Something to Chance.’” Texas National Security Review 6, no. 3 (June 2023): 133–72. https://tnsr.org/wp-content/uploads/2023/06/TNSR-Journal-Vol-6-Issue-3-Stein.pdf.
4. Stewart, Ruben. “The Shifting Battlefield: Technology, Tactics, and the Risk of Blurring Lines in Warfare.” Humanitarian Law & Policy Blog (ICRC), May 22, 2025. https://blogs.icrc.org/law-and-policy/2025/05/22/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/.
5. Wan, Wilfred. “Multi-domain Escalation Risk.” In Global Catastrophic Risks 2026, 30–33. Global Challenges Foundation, December 2025. https://globalchallenges.org/app/uploads/2025/12/GCF-Risk-report-2026-Risk-3-article.pdf.
6. Khan, Nabiya, Kaushik Raj, and Zenith Khan. “Inside the Misinformation and Disinformation War Between India and Pakistan.” CSO Hate, May 16, 2025. https://www.csohate.org/2025/05/16/india-pakistan-digital-war/.
7. McDermott, Rose. “Self-Perceptions and Nuclear Weapons.” RealClearDefense, July 14, 2023. https://www.realcleardefense.com/articles/2023/07/14/self-perceptions_and_nuclear_weapons_966021.html.
8. Perkovich, George. Rethinking a Political Approach to Nuclear Abolition. Washington, DC: Carnegie Endowment for International Peace, March 2025. https://assets.carnegieendowment.org/static/files/Perkovich-Rethinking%20Nuclear%20Abolition-Final.pdf.
9. International Committee of the Red Cross (ICRC), “The shifting battlefield: technology, tactics, and the risk of blurring lines of warfare,” May 21, 2025.
10. https://blogs.icrc.org/law-and-policy/2025/05/22/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/
11. Soutik Biswas, “India and Pakistan's 'Digital War' Is Entering a New, Dangerous Phase,” BBC News, May 16, 2025, https://www.bbc.com/news/articles/c2e373yzndro.

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

Image Source: ChatGPT