INDIA'S NATIONAL SECURITY IN TRANSITION

MS VAIBHAVI KATAL

www.cenjows.in

India's National Security in Transition

Ms Vaibhavi Katal is a research assistant at CENJOWS

Introduction

National security has been largely perceived as defending and securing the borders of a nation to protect its territorial integrity and political sovereignty against external threats. For much of the twentieth century, this narrative dominated strategic thinking and policymaking around the world, including in India. Security was understood as military might, border security, and the ability to deter or destroy hostile enemies.[i] However, the nature of warfare has changed drastically in recent decades. The advent of globalisation, technological advancement, distribution of power, and the blurring of lines between war and peace have broadened the security agenda beyond traditional military agendas. As a result, states are constantly compelled to reconsider how security is conceptualised, evaluated, and executed.[ii]

In India's context, the necessity to re-evaluate has grown significantly over time, both in extent and depth. India today is confronting a complex and multifaceted security environment characterised by unsettled territorial disputes, rising power politics, ongoing internal security concerns, and the emergence of non-traditional threats like cyber warfare, information warfare, and economic coercion. These interconnected challenges operate in ways that existing security frameworks, rooted in traditional state-centric conflict, are ill-equipped to manage effectively. Consequently, India's security thinking is at a crossroads, where consistency with previous methods clash with the demands of a constantly shifting strategic terrain. This chapter posits that India's security thinking must undergo a thorough re-examination since the conceptual principles, threat perceptions, and institutional frameworks that have governed it have grown out of trend with current reality. The chapter is structured around four sections that elaborate on this argument.

First, it contextualises national security and analyses its progression beyond traditional military conceptions. Second, it explores how past events and strategic culture have influenced India's security policy. Third, it examines the transition from traditional to non-traditional and hybrid challenges that India encounters. Finally, it clarifies why traditional security frameworks are outdated and underlines the need for a more integrated and versatile approach towards national security.

National Security as a Concept: From Survival to Complexity

The concept of national security gained prominence in the aftermath of World War II, particularly within realist schools of international relations. Traditionally, national security refers to a state's capacity to safeguard its sovereignty, territorial integrity, and political independence from external military threats. The state was regarded as the principal guarantor of security, with military power serving as the primary instrument for achieving it. The security strategy was therefore centred on deterrence, force posture, alliances, and war-fighting capabilities.[iii]

During the Cold War, the states and 'their military view of security' were strengthened by bipolar rivalry and the constant fear of large-scale conventional or nuclear conflict.[iv] Security discourse was dominated by strategic stability, balance of power, and deterrence theories. Although political cohesion and economic strength were acknowledged as crucial, they were mostly seen as auxiliary components of military security rather than as separate security realms.

However, the collapse of the Soviet Union and the ensuing transformations in the global political landscape prompted a significant rethinking of the concept of security. Many scholars and professionals started to argue that security could no longer be limited to military matters alone and that the emphasis must also shift to political stability, economic resilience, social cohesiveness, and environmental sustainability.[v] This deeper understanding has paved the way for the emergence of concepts such as human security, socio-economic security, and comprehensive security, thereby broadening the scope of security beyond state survival to include the protection of societies and individuals. At the same time, the nature of warfare has started transforming. Comparatively, Interstate wars between military powers have decreased, whereas intrastate conflicts, insurgencies, terrorism, and low-intensity warfare have increased.

Technological advancements, particularly in information and communication technologies, have generated new arenas of contestation, allowing states and non-state actors to exercise influence without resorting to open armed conflict. Consequently, the security environment has become more intricate due to threats that are increasingly multidimensional and frequently ambiguous. [vi] This conceptual strengthening of security does not imply that military might has become irrelevant. Rather, it implies that military power alone is insufficient to solve the entire range of modern security concerns. In order to provide effective national security in the modern age, the military, political, economic, technical, and informational tools of state power

must be integrated.[vii] It also necessitates the ability to foresee and respond to threats that operate below the level of armed conflict.

National Security in India's Context

India's national security stance has been moulded by its unique historical and geopolitical background. Upon gaining independence, India inherited not just the territorial boundaries of British India but also a slew of complicated security concerns, including partition-related bloodshed, unsolved border disputes, and the overwhelming mistrust of neighbouring countries.[viii] In the early years of independence, India was characterised by principles of sovereignty, territorial integrity, and political autonomy, reflecting the colonial heritage, political autonomy, and the imperatives of nation-building.

During the Cold War, India's stance on non-alignment and strategic autonomy shaped its strategic thought. While India eschewed formal military alliances, it nonetheless insisted on building a legitimate military force to repel foreign threats, first from Pakistan and subsequently from China. The battles of 1947-48, 1962, 1965, and 1971 underlined the importance of conventional military capability in India's security calculations.[ix] These battles also lead to a profoundly ingrained belief that security is essentially about territorial security and military readiness.

At the same time, India's internal diversity and socioeconomic issues meant that internal security remained a major worry. Insurgencies in the Northeast, left-wing extremism, and subsequently terrorism linked to cross-border proxy war in Punjab and Kashmir demonstrated the interdependence of internal and external security. Despite these issues, India's security thinking has remained mainly focused on foreign defence, internal security, and economic growth viewed in separate spheres.[x]

Institutionally, India's national security system developed gradually and often spontaneously. Though the civilian authority over the military was well established, there was still need for more cooperation between the military, bureaucracy, and political leadership for optimising national power. Strategic planning was frequently influenced by acute crises rather than long-term evaluations of security. This gradual approach mirrored both India's democratic political system and its long-standing predilection for prudence in security-related issues.

The post-Cold War period brought new dynamics to India's security landscape. Economic liberalisation increased India's involvement in the global economy, creating new opportunities and challenges. The rise of China as a significant power shifted the regional balance, while Pakistan's ongoing dependence on asymmetric anti-India measures presented long-term concerns. India's rising global prominence resulted in new obligations and expectations, including a larger involvement in regional and global security governance.[xi]

These shifts have highlighted the challenges to the security policy based solely on the Cold War and previous conflicts with neighbours. While traditional challenges have not

gone away, they now cohabit with a variety of non-traditional concerns that necessitate a more complex and comprehensive view of security.

From Traditional to Non-Traditional Threats

Traditional security challenges continue to define India's strategic view, especially in terms of territorial defence and interstate conflicts. Persistent border skirmishes with China and ongoing animosity with Pakistan guarantee that conventional military preparation remains at the heart of national security strategy. The very existence of nuclear weapons exacerbates escalation dynamics and necessitates effective deterrence. Recent conflicts, on the other hand, are increasingly characterised by limited probes, stand-offs, and calculated escalation rather than full-scale war. This shift suggests that while classic dangers remain significant, their manifestation has evolved, necessitating more adaptable and multilayered response techniques.[xii]

The emergence of grey-zone warfare, in which adversaries pursue strategic objectives without declaring war, is a distinguishing element of the present security situation. Examples of such approaches include border salami-slicing and maritime pressure by China, and proxy actors, legal warfare, and covert influence operations by Pakistan.[xiii] These techniques take advantage of ambiguity to postpone or complicate retribution. Grey-zone tactics offer ongoing issues for India along its contentious frontiers and in adjacent countries. Conventional deterrence models are less successful in this situation since attribution is difficult and reactions risk disproportionate escalation, necessitating new policies that combine military prudence with strategic messaging.

Non-traditional threats have broadened the extent and depth of national security beyond the battlefield, encompassing technical, informational, and sociological dimensions. Terrorism, cyber-attacks, vital infrastructure disruption, and international criminal networks have increasingly had a greater impact on national stability. These challenges are frequently networked, fast-moving, and unconstrained by territory.[xiv] Even when the techniques are non-military, they can have a strategic influence. India's rising digital and economic connectivity raises its vulnerability to such dangers. As a result, security strategy must address vulnerability in both civilian and military sectors rather than considering them as distinct domains.

Cyber and information threats constitute a substantial shift in the risk matrix. Cyber operations may attack banking systems, energy grids, government databases, and military networks while maintaining plausible deniability.[xv] Information and narrative warfare may impact public opinion, alter political discourse, and exacerbate societal divisions. These instruments are inexpensive yet highly effective, allowing both governments and non-state actors to project influence asymmetrically. For an open and democratic country like India, protecting the information space has become as crucial as defending land, necessitating collaboration across technology, policy, and public communication agencies.

Economic and technical interdependence have also emerged as security risks in ways that prior models could not completely address. Supply chain vulnerabilities, availability of crucial minerals, technology denial regimes, and sanctions are increasingly being utilised to exert strategic pressure. National security is inextricably linked to trade policy, industrial capacity, and innovation ecosystems. [xvi] India's objectives for strategic autonomy and defence indigenisation reflect an understanding of these threats. Security planning must therefore integrate economic resilience and technological capability, as military preparedness alone cannot offset structural vulnerabilities or external economic pressures.

The presence of conventional, grey-zone, and non-traditional risks results in a complex and coupled risk environment. Threats no longer occur sequentially or independently; they frequently reinforce one another across realms. A border crisis may be followed by cyberattacks and misinformation campaigns, and internal instability may be exacerbated by adversaries, as was seen after 'Operation Sindoor'[xvii]. This convergence poses a problem to linear threat assessment models. India's security strategy must consequently shift from single-domain reactions to integrated, cross-domain tactics that anticipate hybrid circumstances, rather than handling each risk individually.

The Limits of Old Security Frameworks

Older security frameworks in India were based on assumptions about clearly identified, outlined battlefields and visible acts of aggression. These models emphasised territorial security, force ratios, and deterrence through punishment.[xviii] While they are successful in traditional circumstances, they are not well adapted to ambiguous and evolving challenges. Grey-zone operations, cyber-attacks, and narrative campaigns seldom trigger thresholds built into standard doctrines. As a result, reaction mechanisms become inefficient or unreliable. Frameworks intended for proclaimed conflicts falter when enemies purposefully operate below escalation thresholds and take advantage of political and legal uncertainty.

The institutional compartmentalisation of old frameworks is another drawback. External defence, domestic security, economic policy, and technical regulation are frequently controlled in distinct bureaucratic silos, with little real-time coordination.[xix] However, contemporary challenges straddle domains and need coordinated solutions. A cyberattack may simultaneously affect domestic security, the economy, and the military. Fragmented structures impede decision-making and diminish responsibility. Without cross-domain planning and shared assessment processes, security responses may be incomplete and reactive. Structural segregation, which previously provided administrative clarity, now causes operational gaps in convoluted security settings.

Traditional frameworks rely primarily on military tools as their principal reaction mechanism. This leads to an imbalance when threats are unconventional or non-military in character.[xx] Information warfare, legal coercion, and economic pressure

cannot be effectively opposed with force alone. Over-militarised responses may have political or diplomatic consequences. Contemporary security rivalry often focuses on legitimacy, perception, and reliance rather than territory. Frameworks that prioritise kinetic reactions thereby misallocate focus and resources. While not entirely integrated into previous models, a more comprehensive toolset that combines diplomatic, technical, informational, and regulatory approach is required.

Another drawback is that legacy security planning is reactive in nature. Historically, changes and theological transformations in India have occurred in response to crises rather than in anticipation of them. This trend results in gradual adaptability rather than anticipatory planning.[xxi] Rapid technical and geopolitical development has reduced warning time and increased first-mover advantage. Security frameworks based on post-crisis rectification are becoming increasingly dangerous. Without forward-looking evaluation and scenario preparation, institutions remain focused on previous battles rather than potential confrontations. Rigid doctrines in an ever-evolving threat environment cause strategic lag and undermine deterrence credibility.

Why India's Security Thinking Needs Re-examination

India's security thinking has to be reconsidered since the gap between inherited beliefs and current reality is growing. Threats nowadays are multi-faceted, persistent, and diffuse, whereas many policy instruments are domain-specific and episodic. Re-examination does not require abandoning existing military goals but rather repositioning them within a larger security framework. Military preparation must be linked to technical resilience, information defence, and economic security. Without conceptual upgrading, policy solutions may treat symptoms rather than causes. A revamped security outlook would better connect threat perception, capacity development, and institutional design with current conflict patterns.

Re-examination is also required because India's national power profile has shifted. As India's economic might, technical potential, and worldwide connections grow so does its susceptibility to strategic rivalry. Security problems are no longer limited to physical borders but also include marine areas, supply chains, digital networks, and diaspora politics.[xxii] A larger footprint increases vulnerabilities. Security thinking developed at a period of relative isolation cannot effectively guide policy in an era of profound interconnectedness. Conceptual renewal is necessary to link India's global position to the appropriate security obligations and protections.

Domestic transformation reinforces the argument for reappraisal. India's growing digitalisation, urbanisation, and infrastructural growth produce new assets that must be protected. Critical industries such as energy, telecommunications, banking, and space systems are now essential to national operations. Disruption in these sectors can produce strategic impacts without firing a single shot.[xxiii] Security architectures that focuses solely on borders ignores systemic vulnerabilities within. A revamped strategy must prioritise resilience, redundancy, and recovery capacity alongside deterrence and defence.

Finally, reconsideration is required to increase strategy coherence among institutions. National security today is dependent on the cooperation of military, intelligence, economic, technical, and diplomatic institutions. Without a common conceptual framework, coordination is personality-driven rather than system-driven. Updating security framework may give a consistent vocabulary and goals for inter-agency action. Conceptual clarity promotes institutional transformation. It also improves democratic accountability by making security policy more open and rationally organised. In this regard, rethinking security is a strategic and governance necessity.

Conclusion

India's national security environment is experiencing a structural transformation, characterised by hybrid threats, technical disruption, and strategic rivalry across several areas. Traditional military threats remain considerable, but they are increasingly integrated into a broader panorama of cyber, informational, and economic challenges. Conceptual models developed for conventional warfare cannot adequately represent these multifaceted issues. As threats evolve and interact, security policies must become more integrated and proactive. Recognising this change is the first step toward creating more adaptable frameworks that match means to changing realities.

Rethinking security strategy is therefore an extension of previous practice rather than a break from it. The goal is to maintain traditional defence strengths while increasing intellectual and institutional capability for handling challenges of new realms of conflict. Such adaptation necessitates conceptual clarity, institutional cooperation, and strategic planning. By placing India's security in this shifting environment, the chapter establishes an analytical foundation for investigating how various tools of state power, like information, military, institutions, and diplomacy, must adapt to current and future security concerns.

ENDNOTES

[i] Andreas, Peter. "Redrawing the Line: Borders and Security in the Twenty-First Century." *International Security* 28, no. 2 (2003): 78–111. http://www.jstor.org/stable/4137469

[ii] Kay, Sean. "Globalization, Power, and Security." *Security Dialogue* 35, no. 1 (March 2004): 9–25. https://doi.org/10.1177/0967010604042533

[iii] Morgan, Patrick M. "The State of Deterrence in International Politics Today." *Contemporary Security Policy* 33, no. 1 (April 2012): 85–107. https://doi.org/10.1080/13523260.2012.659589

[iv] Buzan, Barry. "New Patterns of Global Security in the Twenty-First Century." *International Affairs (Royal Institute of International Affairs 1944-)* 67, no. 3 (1991): 431–51. https://doi.org/10.2307/2621945

[v] Hirsch Ballin, Ernst, Huub Dijstelbloem, and Peter de Goede. "The Extension of the Concept of Security." *Research for Policy*, April 8, 2020, 13–39. https://doi.org/10.1007/978-3-030-37606-2_2

[vi] Jouini, Mouna, Latifa Ben Arfa Rabai, and Ridha Khedri. "A Multidimensional Approach towards a Quantitative Assessment of Security Threats." *Procedia Computer Science* 52 (2015): 507–14. https://doi.org/10.1016/j.procs.2015.05.024

[vii] ibid

[viii] Center for Preventive Action. "Conflict between India and Pakistan." Global Conflict Tracker. Council on Foreign Relations, May 12, 2025. https://www.cfr.org/global-conflict-tracker/conflict/conflict-between-india-and-pakistan

[ix] Makeig, Douglas C. "War, No-War, and the India-Pakistan Negotiating Process." *Pacific Affairs* 60, no. 2 (1987): 271. https://doi.org/10.2307/2758135

[x] Jadoun, Harshit Singh. "Cross Border Terrorism and Home Grown Militancy - Academike." Academike, November 14, 2015. https://www.lawctopus.com/academike/cross-border-terrorism-home-grown-militancy/

[xi] Mukherji, Rahul. "India and Global Economic Governance: From Structural Conflict to Embedded Liberalism." *International Studies Review* 16, no. 3 (September 2014): 460–66. https://doi.org/10.1111/misr.12155

[xii] Sood, Rakesh. "Escalation Dynamics under the Nuclear Shadow—India's Approach." Carnegie Endowment for International Peace, February 10, 2026. https://carnegieendowment.org/russia-eurasia/research/2026/02/escalation-dynamics-under-the-nuclear-shadow-indias-approach

xiii Le, Kiet Hoang, and Hiep Xuan Tran. "Emerging Maritime Security Strategies of Global Powers." Google Books, 2026. https://books.google.co.in/books?hl=en&lr=&id=bmvCEQAAQBAJ&oi=fnd&pg=PA275&dq=The+emergence+of+grey-zone+combat

xiv Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *SSRN Electronic Journal*, 2011. https://doi.org/10.2139/ssrn.1674565

xv Prasad, Nilantha, Abebe Diro, Matthew Warren, and Mahesh Fernando. "A Survey of Cyber Threat Attribution: Challenges, Techniques, and Future Directions." *Computers & Security* 157 (October 2025): 104606. https://doi.org/10.1016/j.cose.2025.104606

xvi Zhang, Hao. "Resilience of Critical Transition Minerals Supply Chain in the Context of Strategic Rivalry: Implications for the National Policy and Regulatory Frameworks." *Journal of Energy & Natural Resources Law*, May 12, 2025, 1–27. https://doi.org/10.1080/02646811.2025.2495920

xvii MEA . "Statement by Foreign Secretary: OPERATION SINDOOR." Ministry of External Affairs, Government of India, 2019. https://www.mea.gov.in/Speeches-Statements.htm?dtl/39473

xviii Spencer, John. "Blocked Page." Linkedin.com, 2026. https://www.linkedin.com/pulse/end-old-assumptions-what-indias-new-security-paradigm-john-spencer-0n6mc/

xix Dasaka, Sameer. "Cyber Deterrence in the Indian Context: Constraints, Credibility and Escalation Risks." https://www.natstrat.org, 2026. https://www.natstrat.org/articledetail/publications/cyber-deterrence-in-the-indian-context-constraints-credibility-and-escalation-risks-251.html

xx Gadeock, S K. "Preparing for the Future: The Need for India to Develop Hybrid Warfare Capabilities." orfonline.org. OBSERVER RESEARCH FOUNDATION (ORF), June 10, 2024. https://www.orfonline.org/research/preparing-for-the-future-the-need-for-india-to-develop-hybrid-warfare-capabilities

xxi MacKay, Joseph, and Christopher David LaRoche. "The Conduct of History in International Relations: Rethinking Philosophy of History in IR Theory." *International Theory* 9, no. 2 (March 20, 2017): 203–36

xxii Gadeock, S K. "Preparing for the Future: The Need for India to Develop Hybrid Warfare Capabilities." orfonline.org. OBSERVER RESEARCH FOUNDATION (ORF),

June 10, 2024. https://www.orfonline.org/research/preparing-for-the-future-the-need-for-india-to-develop-hybrid-warfare-capabilities

[xxiii] George, A. Shaji, T. Baskar, and P. Balaji Srikaanth. "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities across Key Sectors." *Partners Universal International Innovation Journal* 2, no. 1 (February 25, 2024): 51–75. https://doi.org/10.5281/zenodo.10639463