RESEARCH PAPERS

Cognitive Warfare: India’s Strategic Imperatives In the Age of Mind Games

Author: Lieutenant General A B Shivane, PVSM, AVSM, VSM (Retd) • **Published:** May 26, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

This paper examines cognitive warfare as an emerging sixth domain of war in which perception, belief, emotion and decision-making become decisive strategic targets. It traces the evolution of cognitive warfare from ancient psychological statecraft and twentieth-century propaganda to contemporary neuro-digital influence operations enabled by artificial intelligence, big data, deepfakes and social media. Through global case studies involving Russia, China, NATO, the United States and Israel, the paper shows how narrative dominance, reflexive control and cognitive security now shape conflict outcomes. It then analyses India’s experience in Kargil, the 2016 surgical strikes, Galwan and Operation Sindoor to demonstrate that battlefield success must be converted into strategic legitimacy through proactive narrative control. The paper argues that India remains vulnerable due to domestic fissures, media saturation, technological manipulation, institutional gaps and hostile external narratives. It recommends recognising cognitive warfare as a formal operational domain, creating dedicated organisational structures, building interdisciplinary human capital, investing in AI-enabled detection and counter-influence tools, integrating cognitive strategy with kinetic operations and strengthening civil-military resilience. While advocating capability development, the paper stresses that India’s approach must remain ethical, legally grounded and democratically legitimate.

In the wars of tomorrow, the battlefield will not just be the land, oceans, or skies; it will be the human mind. Whoever shapes perception will shape the strategic victory.[1]

Cognitive warfare, understood as the weaponisation of perception to shape thought, influence decision-making, and erode national will, has emerged as the defining battlespace of the twenty-first century. Unlike earlier forms of psychological and information warfare, cognitive warfare penetrates directly into the human mind, exploiting vulnerabilities at the level of belief, emotion, and judgment. Nations such as Russia and China have already institutionalised cognitive strategies into their military doctrines, while Western alliances continue to struggle with definitional and operational clarity.

For India, the stakes are particularly high. Historical experiences, from the missteps of narrative control during the Kargil conflict of 1999 to the measured success of the 2016 surgical strikes, to the contested information domain during the Galwan clash of 2020, and the perceptual dominance achieved in *Operation Sindoor* (2025) reveal that cognitive power can determine whether battlefield victories translate into strategic success. The evolution of cognitive warfare, its theoretical foundations, and global and Indian experiences need analysis and evaluation to derive a set of institutional, doctrinal, and technological recommendations for the Indian Armed Forces. Cognitive warfare must be treated as India's *sixth domain of war*.

1. The Mind as a Battlefield

The character of warfare has undergone successive revolutions, from the dominance of massed infantry in antiquity, to the mechanisation of the twentieth century, and now to the informationised and intelligentised wars of the present. Today, the battlefield is no longer defined solely by geography, platforms, or firepower. It increasingly resides in the perceptions of individuals, societies, and leaders. As James Giordano frames it, "the brain is the battlefield of the future."[2]

The intellectual roots of cognitive warfare are deep. Chinese strategists as early as 2070 BC referred to the "war of attacking the heart," signalling that victory derived as much from breaking the adversary's will as from physical destruction.[3] Kautilya's *Arthashastra* similarly implied psychological subversion, deception, and the manipulation of public sentiment as essential elements of statecraft. Modern theorists, from J.F.C. Fuller's articulation of "psychological warfare" after the First World War, to NATO's recent deliberations on "cognitive superiority," have consistently returned to the recognition that war is as much about minds as it is about material.[4]

What distinguishes the present era is the convergence of technology and psychology. Digital platforms, artificial intelligence, big data, and neuroscience have enabled the manipulation of perception at scale and speed unimaginable to earlier generations. Disinformation campaigns, deepfake technologies, and algorithmically targeted narratives now allow adversaries to wage continuous, low-cost campaigns designed to disorient societies, delegitimise institutions, and paralyse decision-making.[5] The People's Liberation Army (PLA) calls this pursuit "mind superiority."[6] At the same time, Russia operationalises it through reflexive control and narrative dominance. The United States, despite its technological edge, has been critiqued by its own Senate Armed Services Committee for lagging in developing clarity and capacity in this new domain.[7]

For India, cognitive warfare is not an abstract concept but a lived reality. Pakistan's manipulation of global narratives during the Kargil War initially constrained India's diplomatic space. China's disinformation campaigns surrounding the 2020 Galwan clash sought to frame India as the aggressor. Conversely, India's own experience during the surgical strikes of 2016 and *Operation Sindoor* in 2025 revealed that controlled narratives and calibrated ambiguity can amplify

battlefield outcomes. These lessons underline the urgency of institutionalising cognitive warfare as a doctrinal and operational priority.

2. Evolution of Cognitive Warfare: From Psychological to Cognitive Dominance

The idea of influencing the adversary's mind is not new. Sun Tzu, in *The Art of War*, declared that "all warfare is based on deception,"[8] placing psychological manipulation at the heart of strategy. In India, Kautilya advocated espionage and subversion as instruments to weaken enemies internally before striking externally.[9] These insights formed the early grammar of what would later be formalised as psychological warfare.

The First World War was a turning point in this respect. British propaganda, German morale operations, and the use of radio and print media demonstrated that mass persuasion could shape battlefield outcomes and political settlements alike. J.F.C. Fuller's 1920 work mentioned the term "psychological power," predicting that in war, as in all other phases of human activity, we find that the elemental psychological power is mind.[10] The Cold War proved him prescient. Both the United States and the Soviet Union invested heavily in information campaigns, cultural diplomacy, and disinformation. From Radio Free Europe to Soviet "active measures,"[11] the objective was less about physical destruction and more about influencing the hearts and minds of populations worldwide.

However, psychological warfare remained largely adjunct to kinetic force. It softened morale, disrupted cohesion, and provided informational cover for physical operations. The twenty-first century has witnessed a qualitative transformation. The proliferation of digital networks, social media, and real-time data analytics has elevated perception itself into an independent battlefield. Here lies the distinction between psychological warfare and cognitive warfare: the former sought to supplement kinetic power by undermining adversary morale. At the same time, the latter aims to substitute for kinetic power by directly reshaping the adversary's cognition.[12]

Cognitive warfare is, in effect, the militarisation of psychological warfare in the digital age. It combines the insights of cognitive science with the tools of artificial intelligence, big data, and neuroscience. Unlike traditional information warfare, which focuses on controlling the flow of information, cognitive warfare prioritises manipulating responses to information. Its goal is not simply to misinform, but to rewire the decision-making process itself.[13]

China has been at the forefront of this transition. The PLA's writings on "national cognitive security" and "cognitive warfare" emphasise the control of neural and perceptual domains as central to future conflict.[14] Russia, for its part, has refined reflexive control, a strategy of planting premises that lead adversaries to act in ways that appear rational but are in fact orchestrated by Moscow. This was visible in Ukraine, where years of narrative conditioning preceded the 2022 invasion, allowing Russia to frame NATO expansion as encirclement and Ukraine as a Nazi outpost. Such narratives paralysed Western responses at critical junctures.

Western militaries, including NATO, have begun to acknowledge the significance of this shift. The U.S. Department of Defence formally recognised "cognitive attributes" as part of the information environment only in 2017, and NATO convened its first scientific meeting on cognitive warfare in 2021.[15] Yet the definitional ambiguity surrounding the term has hampered doctrinal clarity, leaving Western forces vulnerable to adversaries who treat cognitive dominance as a central pillar of military strategy.

The evolutionary arc is therefore clear, from the moral suasion of ancient strategists, to the propaganda wars of the twentieth century, and now to the neuro-digital battles of the twenty-first. What remains consistent is the underlying objective, victory through perception. What has changed is the scale, speed, and intimacy with which the human mind can be influenced.

For India, this evolution carries profound implications. During the Kargil War, Pakistan was able to momentarily seize narrative initiative by portraying its troops as “freedom fighters,” exploiting global ignorance before India corrected the record through diplomatic and media efforts. Two decades later, *Operation Sindoor* demonstrated the reverse: India’s careful control of information, calibrated ambiguity, and management of international narratives allowed it to shape the battlefield environment in its favour. These experiences illustrate that India, like other major powers, is already engaged in cognitive conflict, whether or not it formally recognises it as such.

3. Theoretical Foundations of Cognitive Warfare

At the heart of cognitive warfare lies the deliberate manipulation of how individuals and societies perceive reality. Unlike information warfare, which seeks to distort facts, cognitive warfare aims to recondition the interpretive frameworks through which facts are processed. It is less about what people think and more about how they think.

3.1. Reflexive Control

A central theoretical pillar is the Russian concept of *reflexive control*. Developed during the Cold War, it describes a process in which an adversary is led to make decisions that appear rational but, in fact, serve the interests of the manipulator. This is achieved by feeding selected information, framing narratives, and creating situations that push the adversary toward a desired outcome. As Russian military theorist Vladimir Lefebvre explained, reflexive control exploits the adversary’s “decision rules” by providing stimuli calibrated to their expected responses.[16]

In practice, this means planting assumptions that shape adversary behaviour before the conflict begins. Russia’s framing of NATO expansion as encirclement, or its branding of the Kyiv government as “Nazi,” illustrates how reflexive control creates cognitive conditions that constrain both domestic and international responses.[17] The target is not the physical battlefield but the adversary’s mental map of the conflict.

3.2 Narrative Dominance

If reflexive control focuses on decision-making, narrative dominance targets collective perception. Wars are not only fought for territory or resources but also for legitimacy. The ability to frame a conflict as defensive rather than aggressive, just rather than unjust, determines whether international coalitions support or condemn a belligerent. Narrative dominance also influences domestic morale, which can sustain or erode national will in protracted conflicts.

China’s “Three Warfare” doctrine, comprising public opinion warfare, psychological warfare, and legal warfare, reflects this recognition.[18] During the Galwan clash of 2020, Beijing disseminated images and stories portraying India as the aggressor, even as it delayed acknowledging its own casualties. The effect was to confuse international opinion and dampen India’s ability to secure the moral high ground. Similarly, Pakistan has repeatedly framed Kashmir as a human rights issue, seeking to internationalise the dispute and portray India as repressive.

Narrative dominance requires not only projecting one’s own version of events but also discrediting the adversary’s. *Operation Sindoor* highlighted how India used calibrated ambiguity and selective disclosure to maintain the narrative of restraint, while simultaneously undermining the adversary’s claims of provocation. This demonstrates that narrative control is not ancillary to operations; it is integral to their success.

3.3 Cognitive Security

The emerging concept of *cognitive security* extends these ideas into the realm of resilience. It recognises that societies under continuous information stress must develop antibodies against manipulation. This involves strengthening media

literacy, ensuring transparency in governance, and building trusted communication channels. For armed forces, cognitive security means protecting decision-makers from adversarial influence, safeguarding operational secrecy, and ensuring that soldiers are psychologically resilient against adversarial propaganda and disinformation.

Cognitive security thus has both defensive and offensive dimensions. On the defensive side, it seeks to inoculate societies against foreign manipulation. On the offensive, it provides a framework to exploit adversary vulnerabilities in cognition. India, situated in a volatile information environment with active adversaries on both its western and northern borders, cannot afford to neglect either dimension.

3.4 Cognition as a Sixth Domain of War

The combined effect of reflexive control, narrative dominance, and cognitive dimension elevates the mind into an independent domain of war. NATO scholars have increasingly argued that the cognitive domain must be treated on par with land, sea, air, space, and cyber.[19] This recognition reflects the growing understanding that the outcome of conflicts will hinge not merely on physical destruction but on perceptual legitimacy.

For India, adopting this perspective means acknowledging that adversaries are already fighting cognitive wars within its borders and abroad. Electoral disinformation, communal polarisation, diaspora manipulation, and reputational attacks through NGOs and think tanks are not isolated incidents; they are elements of sustained campaigns to erode India's national will and international credibility. Without a coherent doctrinal response, India risks losing the battle of perception even as it secures victories on the battlefield.

4. Case Studies: Cognitive Warfare in Practice

The theoretical foundations of cognitive warfare are not academic abstractions. They are actively deployed by states across theatres of conflict, with profound consequences for international security. Examining global experiences offers India critical insights into both the opportunities and risks of operating in this new domain.

4.1. Russia: Reflexive Control in Ukraine

Russia's operations in Ukraine provide perhaps the most vivid demonstration of reflexive control in modern warfare. Well before its 2014 annexation of Crimea or the 2022 full-scale invasion, Moscow invested in long-term cognitive conditioning of domestic, regional, and global audiences. Through state media outlets such as *RT* and *Sputnik*, as well as social media troll farms, Russia propagated narratives portraying Ukraine as a failed state captured by fascist elements. At the same time, NATO expansion was framed as a direct existential threat to Russian sovereignty.[20]

These narratives did not prevent Western military support to Ukraine, but they did achieve several objectives. First, they bolstered domestic legitimacy for Russian actions by presenting them as defensive rather than aggressive. Second, they sowed divisions within European populations, where scepticism of NATO's role and fatigue with sanctions diluted consensus. Finally, they complicated Ukraine's diplomatic messaging, forcing Kyiv to spend scarce resources countering delegitimisation campaigns. In short, Russia demonstrated how narrative dominance could strategically offset its conventional military limitations.

4.2. China: Mind Superiority and "Three Warfare's" Doctrine

The People's Liberation Army (PLA) has embraced cognitive warfare as a core component of its future force posture. In Chinese military writing, the pursuit of "mind superiority" is described as central to achieving victory in an era of intelligentised warfare.[21] The PLA's doctrine of "Three Warfares" i.e., public opinion warfare, psychological warfare,

and legal warfare integrates cognitive strategies with broader statecraft.

Beijing's behaviour in the Indo-Pacific illustrates this integration. During the 2020 Galwan clash with India, Chinese state media portrayed India as the aggressor while withholding casualty figures to sustain domestic morale. Beyond the battlefield, Chinese influence operations have leveraged Confucius Institutes, diaspora groups, and digital platforms to shape international narratives about Xinjiang, Taiwan, and the South China Sea. These efforts blur the line between wartime propaganda and peacetime influence, underscoring the reality that cognitive conflict is continuous rather than episodic.

For India, China's approach highlights two dangers. The first is Beijing's ability to mobilise state and non-state assets, media, corporations, and academics, in support of cognitive objectives. The second is its increasing investment in neuroscience and artificial intelligence, with Chinese scholars openly discussing the potential militarisation of brain sciences to manipulate adversary cognition.[22] These developments signal that China views cognitive warfare not as a supplement, but as a decisive domain of operations.

4.3. NATO and the United States: Playing Catch-Up

In contrast to Russia and China, Western alliances have struggled to conceptualise and operationalise cognitive warfare. The US Department of Defence formally recognised "cognitive attributes" in its doctrine only in 2017, and a 2025 Senate Armed Services Committee report criticised the Pentagon for lagging behind adversaries in this domain. [23] NATO convened its first scientific forum on cognitive warfare in 2021, describing it as "the most contested domain of the future," but stopped short of declaring it an independent operational theatre.

This hesitancy has created vulnerabilities. During the COVID-19 pandemic, Western populations were inundated with disinformation campaigns, some traced to Russia and China, that exploited distrust in institutions, thereby undermining crisis response. Similarly, in Ukraine, Western narratives have often been reactive, countering Russian propaganda rather than pre-empting it. While initiatives such as the NATO Strategic Communications Centre of Excellence in Riga represent progress, they remain fragmented compared to the integrated strategies of Moscow and Beijing.

4.4 Israel–Iran Conflict, 2025: Precision Messaging as Deterrence

The brief but intense conflict between Israel and Iran in 2025 illustrates a more sophisticated application of cognitive warfare. When Iran launched a coordinated drone and missile barrage against Israeli territory, Israel responded with not only military precision but also cognitive pre-emption. The Israeli government conducted real-time media briefings, employed calibrated ambiguity about red lines, and highlighted the proportionality of its strikes.[24]

This approach achieved two effects. Internationally, it maintained Israel's moral high ground, securing tacit Western support and avoiding premature censure. Domestically, it preserved public confidence by projecting resilience and control. Meanwhile, Iran's leadership sought to project retaliation strength externally while downplaying domestic damage, revealing the cognitive balancing act of authoritarian regimes.

The key lesson from this conflict is that cognitive precision can multiply kinetic precision. Strategic messaging, disclosure management, and narrative control can deter escalation while reinforcing legitimacy. For India, which must often operate under international scrutiny, the Israel–Iran case underscores the importance of anticipating adversary narratives and pre-empting global reactions through proactive communication.

5. Indian Case Lessons: Kargil, Surgical Strikes, Galwan, and *Operation Sindoor*

India's encounters with Pakistan and China over the past three decades illustrate how cognitive warfare determines whether battlefield outcomes translate into strategic advantage. Each conflict offers distinct lessons about narrative control, perception management, and the costs of neglecting the cognitive domain.

5.1. Kargil War (1999): The Cost of Losing the Narrative

The Kargil conflict revealed how adversaries can seize the cognitive initiative even in the face of battlefield setbacks. In the opening weeks of the conflict, Pakistan portrayed its infiltrators as Kashmiri "freedom fighters," framing the operation as an indigenous insurgency rather than a cross-border incursion. This narrative initially sowed confusion in the international community, buying Islamabad precious time to deny responsibility and obscure the scale of its involvement.[25]

India eventually regained the narrative through diplomatic engagement, releasing captured Pakistani documents, and leveraging international media access to the battlefield. Yet the episode exposed India's vulnerability to adversarial narrative shaping. The lesson from Kargil was clear: battlefield bravery alone cannot secure legitimacy. Unless India shapes perceptions early and decisively, it risks allowing adversaries to frame the conflict on their terms.

5.2. Surgical Strikes (2016): Precision in Kinetics and Narratives

In contrast, the 2016 surgical strikes against terrorist camps across the Line of Control marked a turning point in India's use of cognitive warfare. Following the Uri terror attack, India conducted cross-border operations but paired them with strategic communication calibrated to achieve deterrence without escalation.

By officially acknowledging the strikes, releasing selective information, and maintaining a restrained tone, India achieved three objectives. Domestically, it reinforced national morale and projected decisive leadership. Internationally, it signalled limited aims, ensuring that global opinion did not tilt toward escalation fears. Toward Pakistan, it conveyed that future provocations would invite proportionate retaliation. The surgical strikes demonstrated that narrative control, when paired with operational success, multiplies strategic effects.[26]

5.3. Galwan Clash (2020): Contesting the Information Space

The Galwan Valley clash of June 2020 underscored the challenges of cognitive warfare against China. Beijing immediately launched disinformation campaigns portraying India as the aggressor while suppressing its own casualty figures to maintain domestic morale. Chinese state media released curated images, videos, and commentary to project tactical dominance despite evidence of losses on both sides.

India responded with selective disclosure, honouring fallen soldiers with public funerals and memorialisation, thereby sustaining domestic morale and international sympathy. Yet the absence of a coordinated cognitive warfare doctrine meant India's messaging remained reactive. While New Delhi successfully garnered support from Western partners, Beijing's control of information delayed global recognition of the scale of its casualties. The lesson was twofold: China's integration of state media, digital platforms, and psychological tools gave it a first-mover advantage; India's counter-narratives, though effective domestically, lacked offensive depth internationally.

5.4. Operation Sindoor (2025): Calibrated Ambiguity and Narrative Asymmetry

Operation Sindoor, India's limited but decisive response to cross-border provocations in 2025, showcased the maturing of India's cognitive warfare capability. Unlike earlier conflicts, India adopted calibrated ambiguity: details of the operation

were disclosed selectively, emphasising proportionality, legality, and restraint. Media access was tightly controlled, and official statements reinforced the narrative that India was defending sovereignty while avoiding escalation.

This approach achieved cognitive asymmetry. Adversary attempts to portray the operation as aggression were undermined by India's narrative of restraint. Internationally, India avoided immediate censure, while domestically, the operation boosted morale without overexposing tactical details. *Operation Sindoor* thus demonstrated that when managed as an integrated domain, cognitive warfare can create strategic space, delay adversary responses, and consolidate legitimacy. Yet the global perception was clouded in ambiguity with strong Pakistani narrative warfare.

5.5. Lessons Across Conflicts

- Pre-emption Matters: Kargil proved that once adversaries set the narrative, it is costly and time-consuming to reverse.
- Narrative Precision Multiplies Kinetic Success: The surgical strikes highlighted that cognitive clarity ensures tactical actions translate into strategic deterrence.
- Information Denial and Suppression Can Be Weapons: Galwan revealed how China's withholding of information preserved its domestic morale even when tactically disadvantaged. In 1998, the BBC released a documentary titled *The Shadow Circus: The CIA in Tibet,*[27] which shattered the popular impression that the non-violent Tibetans allowed the People's Liberation Army to stroll into Lhasa in 1951 after half-hearted, token resistance.
- Integrated Cognitive Strategy Delivers Asymmetry: *Operation Sindoor* illustrated how narrative dominance and ambiguity can offset adversary propaganda and international pressure. The need is for a proactive and pre-emptive narrative disposition.

Together, these episodes make one truth evident that in the Indian context, cognitive warfare is not a future risk but an ongoing dimension of conflict. Recognising this formally within doctrine and training is essential if India is to secure its national objectives in an increasingly contested information environment.

6. India's Vulnerabilities in the Cognitive Domain

Despite battlefield resilience and a growing awareness of information threats, India remains exposed to cognitive warfare across multiple axes. These vulnerabilities span political, social, technological, and institutional dimensions. Unless recognised and systematically addressed, they risk being exploited by adversaries to undermine national unity and strategic credibility.

6.1. Domestic Fissures as Cognitive Targets

India's diversity, while a source of strength, also creates exploitable seams. Adversaries have repeatedly sought to amplify internal divisions, whether along religious, caste, linguistic, or regional lines. Disinformation campaigns on social media during episodes of communal tension illustrate how external actors manipulate pre-existing cleavages to magnify discord. As seen in the 2019 Balakot crisis, adversarial information operations targeted Indian audiences with doctored videos and fake news to sow doubt about the credibility of official statements.

The danger is not merely reputational but operational. Polarised domestic discourse can undermine national resolve in crises, erode trust in institutions, and complicate decision-making. This aligns with the global pattern where adversaries view the cognitive domain as an opportunity to weaken a society from within before military confrontation.

6.2. Media Ecosystem and Information Saturation

India’s vibrant but fragmented media environment amplifies vulnerabilities. A 24/7 news cycle incentivises speed over accuracy, making mainstream outlets susceptible to amplification of adversarial disinformation. During the Galwan crisis, Chinese-origin narratives and doctored visuals found their way into Indian discussions before being debunked. The lack of structured fact-checking in real time enabled adversaries to shape perceptions in the critical opening hours of the clash.

Moreover, India’s social media penetration, with over 700 million users, creates an enormous attack surface. Bot networks and coordinated inauthentic behaviour originating from across borders often flood digital platforms during crises. Without an integrated state response, the line between organic domestic debate and adversarial interference blurs rapidly.

6.3. Technology and Emerging Frontiers

The accelerating convergence of artificial intelligence, deepfakes, and immersive platforms like the metaverse magnifies India’s vulnerabilities. Reports highlight how the metaverse and AI-powered manipulation tools can reshape human cognition at scale, creating synthetic but believable experiences. For adversaries, such technologies offer means to undermine trust in Indian institutions, question the integrity of elections, or demoralise armed forces through fabricated combat footage.

India’s regulatory and technological countermeasures remain underdeveloped. While there are ongoing initiatives on cybersecurity, cognitive security, and addressing manipulation of minds rather than machines, they remain poorly institutionalised. This gap is particularly concerning given that adversaries like China are already integrating neuroscience research and AI to militarise the cognitive domain.

6.4. Institutional and Doctrinal Gaps

Unlike cyber or space domains, India does not yet recognise cognitive warfare as a distinct operational sphere. The absence of a doctrine results in fragmented responses: intelligence agencies, armed forces, media regulators, and civil society actors operate in silos without shared frameworks. This institutional lag mirrors challenges noted in NATO and the US, but is riskier in India’s case, given its high exposure to both Chinese and Pakistani influence operations.

Further, cognitive warfare requires specialised human capital, psychologists, behavioural scientists, data scientists, and communication strategists, working alongside the military. Current force structures remain focused on kinetic and cyber domains, with little integration of cognitive expertise. Without institutionalising this talent, India risks remaining reactive rather than proactive in this arena.

6.5. External Narrative Battles

India also faces persistent external framing challenges. On issues ranging from Kashmir to border clashes, adversaries often succeed in shaping initial international narratives, forcing India into damage control. For example, Pakistan has consistently internationalised the Kashmir issue through propaganda, while China has portrayed border clashes as Indian aggression. Delays in countering such narratives allow adversaries to build legitimacy with select international audiences.

6.6. Key Vulnerability Themes

- Societal Fault Lines: Internal divisions magnified by external disinformation.

- Media Saturation and Speed: News ecosystems are vulnerable to infiltration and manipulation.
- Tech-Driven Manipulation: AI, deepfakes, and immersive tools outpacing regulatory frameworks.
- Institutional Lag: Absence of doctrine and integration of cognitive expertise.
- International Narratives: Adversaries often achieve first-mover advantage in framing global perceptions.

Unless systematically addressed, these vulnerabilities risk creating a paradox: India's growing conventional and nuclear capabilities could be offset by adversaries' success in weakening the nation's cognitive resilience.

7. Strategic Recommendations

Recognising the cognitive domain as an operational theatre demands a fundamental shift in doctrine, organisation, and capability development. India's armed forces, already stretched across multi-domain contingencies, must integrate cognitive warfare into their strategic vision if they are to secure national objectives in an era where perception often outweighs firepower.

7.1. Cognitive Warfare as the Sixth Domain

The first step is doctrinal clarity. Just as cyber and space were acknowledged as independent operational domains, cognitive warfare must be recognised as a distinct theatre of operations. This recognition will institutionalise the requirement for training, resources, and integration. A tri-service *Doctrine on Cognitive Operations* should articulate the principles of cognitive security, offensive influence campaigns, and resilience-building. By codifying the cognitive domain as the "sixth domain of war," India would align its doctrine with the realities of twenty-first-century conflict.

7.2. Establish a Cognitive Warfare Structure

India should create a dedicated *Cognitive Warfare Organisation* under the Integrated Defence Staff. This body would serve as the nodal agency to coordinate across services, intelligence agencies, media regulators, and cyber institutions. The organisation should integrate specialists in psychology, behavioural science, linguistics, and artificial intelligence alongside military officers. Such interdisciplinary fusion is essential for designing and executing cognitive campaigns.

A parallel requirement is to embed cognitive warfare cells within theatre commands and frontline units. These cells would provide tactical commanders with the tools to anticipate adversary narratives, craft counter-narratives, and maintain local morale. By decentralising cognitive expertise, India can operationalise influence at the tactical level while maintaining strategic coherence.

The Prime Minister's Office (PMO) should institutionalise a strategic communication wing modelled after the media management architectures of Washington and Beijing, with daily press briefings from the PMO, MEA, MHA and MoD to shape domestic discourse and project a coordinated, assertive message to maintain narrative dominance in the global discourse. Presently, India and the PMO respond reactively, giving the advantage of initiative to the adversary. A lesson learnt even in the recent *Operation Sindoor*.

7.3. Training and Human Capital

Cognitive warfare is as much about minds as it is about machines. India must therefore invest in cultivating a cadre of officers and specialists fluent in cognitive science, narrative construction, and influence operations. Training modules should include exposure to psychological operations, media studies, and neuroscience.

Partnerships with universities and research institutions can help bridge the expertise gap. Just as India developed indigenous cyber expertise through academic–military collaborations, a similar pipeline is necessary for cognitive warfare. Officers with backgrounds in communication, sociology, and data science should be identified early and provided with tailored career tracks within the armed forces.

7.4. Countering AI and Deepfakes

Adversaries are weaponising artificial intelligence, big data, and immersive technologies to conduct influence operations at scale. India must develop indigenous tools for real-time detection of deepfakes, bot networks, and synthetic media. Defence research organisations, in partnership with private industry and start-ups, should prioritise machine-learning systems capable of verifying authenticity in milliseconds, a critical capability during crises where narrative momentum determines legitimacy.

In addition, India should explore offensive cognitive tools. Controlled use of AI-driven narrative generation, immersive simulations for psychological deterrence, and precision influence campaigns targeting adversary decision-makers could give India asymmetric advantages. However, ethical frameworks and legal boundaries must be codified to prevent misuse.

7.5. Integration with Multi-Domain Operations

Cognitive warfare cannot remain siloed; it must be integrated with India's broader *C6SR* (Command, Control, Communications, Collaboration, Cyber, Combat Systems, Intelligence, Surveillance, Reconnaissance) architecture. Every kinetic operation, whether missile strikes, air campaigns, or mechanised manoeuvres, should be paired with narrative strategies designed to amplify effects.

Operation Sindoor demonstrated how calibrated ambiguity could enhance operational surprise and legitimacy. Future operations should formalise this approach by embedding cognitive planning into operational design. For instance, precision strikes should be accompanied by real-time information releases that emphasise proportionality and restraint, thereby shaping both domestic morale and international opinion.

7.6. Civil–Military Fusion: Building National Cognitive Resilience

Cognitive warfare is not confined to the armed forces; it envelops society as a whole. Building resilience requires integrating civil actors into the national cognitive security strategy. Public broadcasters, social media platforms, educational institutions, and civil society organisations must be mobilised to enhance media literacy and inoculate citizens against disinformation.

For the armed forces, this means developing joint frameworks with the Ministry of External Affairs, the Ministry of Information and Broadcasting, and cyber regulators to ensure unified national messaging during crises. Just as China has institutionalised whole-of-nation approaches through its "Three Warfare's, Doctrine", India must embrace a democratic variant that leverages transparency and trust to strengthen societal resilience.

7.7. International Cooperation

India should also explore partnerships with like-minded democracies facing similar cognitive threats. Joint initiatives among the United States, Israel, France, and Japan on deepfake detection, disinformation countermeasures, and ethical frameworks could accelerate capability-building. India's leadership in forums like the Quad provides an opportunity to position cognitive security as a shared priority in the Indo-Pacific. Further, India must ensure its media personnel are embedded in foreign media houses to project narratives that align with India's national interests.

7.8. Summary of Recommendations

- Doctrine: Recognise cognitive domain as the sixth domain of war.
- Organisation: Establish a Cognitive Warfare Organisation and embed cells in field commands. The Prime Minister's Office (PMO) should institutionalise a strategic communication wing with daily press briefings.
- Training: Build interdisciplinary cadres skilled in psychology, media, and AI.
- Technology: Invest in real-time detection of deepfakes and offensive influence tools.
- Integration: Pair kinetic operations with cognitive strategies under C6ISR frameworks.
- Civil–Military Fusion: Strengthen societal resilience through partnerships with civil institutions.
- International Cooperation: Build coalitions for counter-disinformation and ethical cognitive warfare.

These recommendations are not aspirational luxuries but operational imperatives. Without institutionalising cognitive warfare capabilities, India risks winning battles but losing wars in the contested domain of perception.

8. Ethical and Legal Dimensions

While the operational necessity of cognitive warfare is undeniable, its practice raises serious ethical and legal dilemmas. The manipulation of minds, civilian and military alike, poses questions about morality, legality, and democratic accountability. For India, a democracy with global aspirations, it is essential that cognitive warfare capabilities be developed within a framework that balances effectiveness with legitimacy.

8.1. Ethical Concerns: Manipulation and Consent

Cognitive warfare deliberately seeks to shape perceptions, influence emotions, and manipulate decision-making. When directed at adversaries, this may be justified as an extension of strategy. However, when it spills into domestic domains, it risks undermining trust in democratic institutions and eroding the very values India seeks to defend.

For example, excessive information control or the deliberate use of disinformation could alienate domestic populations, turning a tool of defence into a weapon of distrust. The boundary between legitimate influence and unethical manipulation is therefore thin. India must clearly define red lines to ensure that cognitive operations remain outward-facing, targeted at adversaries, and framed in terms of national security.

8.2. International Law and the Grey Zone

International law is ill-prepared for the challenges of cognitive warfare. The UN Charter, the Geneva Conventions, and subsequent treaties primarily address kinetic operations and tangible acts of aggression. Disinformation campaigns, narrative manipulation, or psychological operations fall into a grey zone: they are not formally prohibited, but their impacts can rival kinetic attacks.

India must recognise this ambiguity and prepare for adversaries exploiting it. For instance, China's disinformation campaigns on border clashes do not technically violate international law, but they undermine India's sovereignty and international standing. Similarly, Russian reflexive control campaigns in Ukraine have operated below the threshold of formal war, yet shaped strategic outcomes.

This legal grey zone creates both opportunity and vulnerability. India could use narrative dominance to counter adversaries without breaching international norms, but it must also guard against reputational risks of being accused of propaganda or manipulation.

8.3. Human Rights and Information Integrity

Another ethical dimension concerns the rights of citizens to access authentic information. Cognitive operations, particularly those involving deepfakes or manipulated content, risk undermining public trust in all forms of information. If citizens begin to doubt the authenticity of news, videos, or official statements, the societal cost could outweigh the strategic gain.

India must therefore develop safeguards to ensure that its use of cognitive tools does not corrode public trust. Transparency, fact-based communication, and credible institutions are vital to maintaining a democratic distinction between India's practices and those of authoritarian adversaries.

8.4. The Role of Technology Companies

Private technology platforms play an outsized role in the cognitive domain. Social media giants, messaging apps, and search engines act as both conduits and amplifiers of influence operations. Yet their regulatory frameworks are opaque, inconsistent, and often tilted by commercial incentives.

India must ensure that its cognitive warfare strategy integrates with regulatory measures for technology companies. This includes mandating transparency in algorithms, requiring accountability for inauthentic behaviour, and compelling cooperation in crisis scenarios. Without such frameworks, adversarial narratives can bypass state defences and infiltrate directly into civilian discourse.

8.5. Need for Ethical Doctrine

Finally, India's armed forces must codify an ethical doctrine for cognitive warfare. This doctrine should specify:

- Acceptable targets (adversary combatants, hostile populations in conflict zones).
- Prohibited practices (disinformation aimed at domestic audiences, manipulation of democratic processes).
- Standards of truthfulness (emphasising framing and selective disclosure over fabrication).
- Proportionality (ensuring that influence operations remain calibrated to the strategic objective).

By embedding ethics into doctrine, India can legitimise its use of cognitive warfare as a defensive necessity rather than an authoritarian imitation. This is vital for preserving India's global image as the world's largest democracy and for building international partnerships in the Indo-Pacific.

8.6. Ethical and Legal Balancing

- Manipulation vs. Consent: Ensure outward focus, avoid undermining domestic trust.
- Legal Grey Zone: Prepare for adversary exploitation of the ambiguities of international law.
- Rights and Integrity: Protect citizens' right to authentic information.
- Tech Accountability: Regulate platforms to prevent adversarial infiltration.
- Ethical Doctrine: Codify principles for legitimacy, proportionality, and restraint.

In short, India's cognitive warfare capabilities must be bound by ethics, guided by law, and rooted in democratic legitimacy. Without such safeguards, the very tools meant to defend sovereignty could corrode it from within.

9. Toward a Cognitive Warfare Doctrine for India

Cognitive warfare is no longer an abstract possibility; it is an operational reality. India has already encountered it in Kargil, Galwan, *Operation Sindoor* and hybrid campaigns mounted by Pakistan and China, where adversaries sought to win the war of perception regardless of battlefield outcomes. The global landscape reinforces this trajectory: Russia's reflexive control in Ukraine, China's "Three Warfare Doctrine," and Israel's precision messaging in its conflict with Iran, all demonstrate that the decisive battles of the twenty-first century will be fought in the human mind as much as on the ground.

For India, the stakes are especially high. As a democracy with a diverse social fabric, adversaries perceive cognitive fissures as exploitable vulnerabilities. Disinformation campaigns targeting communal harmony, propaganda on Kashmir, and narratives portraying India as an aggressor in border disputes are all elements of a sustained cognitive offensive. Without a coherent doctrine, India risks fighting with fragmented defences in a theatre where adversaries are already coordinated, integrated, and well-resourced.

The lessons from India's own experiences are clear:

- Kargil taught us that narrative pre-emption is as vital as military mobilisation.
- The surgical strikes showed that narrative precision can multiply kinetic precision.
- Galwan revealed the danger of reactive communication against an adversary skilled in information suppression.
- *Operation Sindoor* highlighted how calibrated ambiguity can create cognitive asymmetry in India's favour, as well as the importance of being proactive.

Together, these lessons underscore the urgency of institutionalising cognitive warfare as the sixth domain of operations. This requires doctrinal recognition, organisational innovation through a Cognitive Warfare Command, interdisciplinary training pipelines, indigenous technological capabilities to counter AI-driven disinformation, and civil–military fusion to build societal resilience.

Yet India's approach cannot be a carbon copy of authoritarian models. For cognitive warfare to succeed without corroding democratic legitimacy, it must be guided by ethics, legality, and transparency. The objective is not to deceive one's own people but to deny adversaries the ability to manipulate them. In the international sphere, India's practice of cognitive warfare must project restraint, truth framing, and proportionality, thereby reinforcing its image as a responsible power while neutralising adversarial narratives.

The roadmap is therefore threefold:

- Define the Cognitive Domain by crafting ethical doctrines that align national security with democratic values, setting India apart from authoritarian practices.
- Defend the Cognitive Domain by inoculating society against disinformation, deepfakes, and psychological manipulation.
- Dominate the Cognitive Domain by pre-empting adversarial narratives, projecting legitimacy, and embedding influence into military planning.

If India fails to act, it risks becoming a victim of narrative encirclement, where battlefield victories are undermined by perception defeats. If it succeeds, it will not only secure its sovereignty but also emerge as a global leader in defining the ethical contours of cognitive warfare in the twenty-first century.

In an era where wars are fought with drones, data, and deepfakes, the most decisive weapon is still the human mind. For India's armed forces, the challenge is not just to fight in the cognitive domain but to master it, turning perception into power and narrative into national strength.

Footnotes:

[1] Lt Gen AB Shivane (Notion of Victory, CENJOWS https://cenjows.in/wp-content/uploads/2025/09/GL_REPORT_26_JUNE_25.pdf)

[2] James Giordano, quoted in, Darshan Gajjar, "Cognitive Warfare," *The Geostrata* March 11, 2023, https://www.thegeostrata.com/post/cognitive-warfare.

[3] Fabio Ibrahim, et. al., "A Systematic Review of Cognitive and Psychological Warfare", *The Defence Horizon Journal*, December 1, 2023, https://www.researchgate.net/publication/376046270_A_Systematic_Review_Of_Cognitive_And_Psychological_Warfare .

[4] Fabio Ibrahim et.al., op. cit.

[5] Bill Gertz, "Pentagon behind on advances in cognitive warfare, Senate report finds," *The Washington Times*, July 23, 2025, https://www.washingtontimes.com/news/2025/jul/23/inside-ring-pentagon-behind-advances-cognitive-warfare-senate-report/.

[6] Rand Corporation, Chinese Next-Generation Psychological Warfare. June 1, 2023, https://www.rand.org/pubs/research_reports/RRA853-1.html

[7] Bill Gertz, *op. cit.*

[8] Sun Tzu, *The Art of War*, 2004, p. 31, https://dn790006.ca.archive.org/0/items/TheArtOfWarBySunTzu/ArtOfWar.pdf.

[9] R. Shamasastry, op. cit., p.25

[10] J.F.C. Fuller, *The Reformation of War,* London, Hutchinson, 1923, p.41

[11] See, for instance, Jeffery Whyte, "Soviet Active Measures and the Second Cold War", *International Political Sociology*, Volume 18, Issue 3, September 2024, https://doi.org/10.1093/ips/olae024.

[12] Fabio Ibrahim et.al., op. cit.

[13] Darshan Gajjar, "Cognitive Warfare," *The Geostrata*, March 11, 2023, https://www.thegeostrata.com/post/cognitive-warfare.

[14] Abhishek Kumar Darbey, "China and Cognitive Warfare: An Overview", *Manohar Parrikar Institute of Defence Studies and Analyses*, September 27, 2024, https://www.idsa.in/publisher/issuebrief/china-and-cognitive-warfare-an-overview.

[15] C. Deppe and G.S. Schaal, "Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept", *Frontiers Big Data*, Volume 7, Issue, 1452129, 2024, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full.

[16] Thomas C. Oden, *The Structure of Awareness: Toward a Symbolic Logic of Human Behaviour*, Abingdon Press, Nashville, 1969,

[17] Timothy Thomas, “Russia’s Reflexive Control Theory and the Military,” *Journal of Slavic Military Studies*, Volume 17, Number 2, 2004, pp. 237–256.

[18] Dean Cheng, “Winning Without Fighting: Chinese Legal Warfare,” *Heritage Foundation Backgrounder*, May 21, 2012, https://www.heritage.org/asia/report/winning-without-fighting-chinese-legal-warfare.

[19] NATO Review, *Countering cognitive warfare: awareness and resilience*, May 20, 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.

[20] Timothy Thomas, op. cit.

[21] Elsa B. Kania, “In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate,” *The Strategy Bridge*, August 27, 2019, https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.

[22] Elsa B. Kania and Wilson Vorn Dick, “Weaponizing Biotech, Military Reform, and Disputed Waters with Vietnam” *Hoover Institution*, August 18, 2019, https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/.

[23] Bill Gertz, op. cit.

[24] S.K. Minhas, “Cognitive warfare: Key Aspects”, *MP IDSA*, August 18, 2025, https://www.idsa.in/wp-content/uploads/2025/08/Issue-Brief-Gp-Capt-Sukhbir-Kaur-Minhas-18-August-2025.pdf.

[25] Praveen Swami, *The Kargil War*, Penguin, New Delhi, 2000.

[26] Karthika Sasikumar, “India’s Surgical Strikes: Response to Strategic Imperatives”, *San Jose University*, April 2019, https://scholarworks.sjsu.edu/pols_pub/29/.

[27] Tensing Sonam, “*The Shadow Circus: The CIA in Tibet”,* June 30, 2015, https://www.youtube.com/watch?v=R_5LOPYzddY.

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

Image Source: ChatGPT