ARTICLES

Psychographic Warfare and India's Battle for Cognitive Sovereignty

Author: Mahima Katiyar • **Published:** July 08, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

This paper examines psychographic micro-targeting as an emerging instrument of cognitive warfare and evaluates its implications for India's cognitive sovereignty. It argues that the convergence of artificial intelligence, behavioural analytics, data harvesting and platform-driven algorithmic amplification has transformed the information environment into a contested cognitive battlespace. Unlike traditional information warfare, psychographic warfare does not merely disseminate falsehoods; it maps individual and collective vulnerabilities, exploits emotional triggers, fragments shared reality and gradually erodes institutional trust. India's vast digital population, linguistic diversity, social complexity and democratic openness create a uniquely expansive psychographic attack surface that can be exploited by hostile actors to deepen polarization, manipulate public discourse and weaken strategic coherence.The paper situates this threat within India's national security landscape and highlights its geopolitical consequences, particularly in the context of hybrid warfare, grey-zone competition and China's evolving cognitive operations. It further argues that protecting territorial and cyber frontiers is no longer sufficient; India must also secure its epistemic and cognitive domains. To address this challenge, the paper proposes a strategic framework built around indigenous AI-enabled cognitive defence, digital literacy, critical thinking, stronger data governance, ethical AI regulation and international norm-building through a possible Cognitive Warfare Conduct Convention. The study concludes that cognitive sovereignty is becoming central to India's democratic resilience, national security and strategic autonomy in the twenty-first century.

1. Introduction: The Silent War for the Indian Mind

The battlefield for the most dangerous wars of the 21st century is no longer confined to physical domains; it has crawled into the very fabric of human cognition. This silent, insidious conflict, known as cognitive warfare, transcends the traditional information warfare by directly engaging with the mind. So, it seeks not to capture the land but to hijack the mind, shape the perceptions, manipulate beliefs, and ultimately influence the decision-making process [1]. As articulated by NATO, cognitive warfare is fundamentally ‘‘a fight for cognitive superiority,’’ it aims to alter how a population thinks and acts to achieve strategic objectives without kinetic force [2]. This evolution has profoundly shifted the battlespace from physical to the neurobiological substrates of human brain and the psychosocial dynamics of targeted population and individual [3]. And at the very heart of this paradigm, lies a particularly potent and cognitively dangerous weapon- psychographic micro-targeting [4]. Rather than addressing the broad demographic groups, psychographic micro-targeting penetrates into the psychological profiles of individuals, it analyses their values, fears, emotions, biases, aspirations and categorizes them [4]. When this vast amount of data is amplified by advanced artificial intelligence, the product is highly personalized, tailored and extraordinarily precise disinformation campaigns, exploiting the cognitive vulnerabilities of the individuals without the target realizing they are influenced [5].

India, a country with a billion population, deep digital penetration and extraordinary linguistic, religious, cultural diversity faces an urgent and unique national security threat from any weaponization of psychographic micro-targeting. With approximately 958 million active users [6] and the world's highest levels of engagement on digital platforms like YouTube and WhatsApp, India presents an immense "psychographic attack surface" [7]. If traditional warfare threatens a country's borders, cognitive warfare threatens the very foundation of its democracy and social cohesion. By invisibly and gradually shaping what people believe to be true, adversaries can conveniently influence political outcomes, fuel polarization and undermine national resilience, all without firing a single shot. This paper argues that India faces a structurally distinct cognitive security challenge which demands a conceptual reconstruction beyond existing NATO centric framework which is designed for a homogenous western threat environment [7]. India's national security challenge is not confined to just territory, space and cyberspace but now it extends to securing its cognitive sovereignty too- the ability of its citizens to think, deliberate and make decisions free from covert psychological manipulative parasites. The battle for future may ultimately be a battle for human mind. This analysis will specifically delve into mechanism of this hovering threat within Indian context, its geopolitical implications and strategic imperatives for India to secure the cognitive spaces of its citizens.

2. Mechanisms of Threat: The Algorithmic Disintegration of Reality in India

The danger posed by psychographic micro-targeting stems from its sophisticated and intricate mechanism. It leverages massive computational power, AI and behavioural psychology to not merely spread false information but to break apart the shared understanding of reality itself- an algorithmic disintegration [7]. In the context of India, these dangers are amplified by its unique socio-technical landscape, linguistic, cultural, religious diversity and multiple other fault lines. Thus, what India is facing is not merely a battle against misinformation but a struggle to preserve its very democratic social fabric. The ultimate danger is not that the citizens are deceived but that they lose the ability to collectively recognize when they are being deceived and ultimately fostering an epistemic chaos.

2.1 Data Harvesting and Profiling: The Digital Panopticon in India

At the very foundation of psychographic micro-targeting lies the pervasive and surreptitious harvesting of vast amount of personal data. This data extends beyond demographic information to encompass online behaviours, political affiliation,

interactions on social media, consumption patterns and the emerging risk of harvesting biometric data for behavioural prediction [6] [7]. Advanced AI then feeds on this data to map out values, beliefs, fears, ideologies, emotional triggers and desires of individuals across diverse linguistic and cultural groups. Algorithms then construct highly granular profiles of individuals based on these mapped psychological charts. Thus, every click, share, like, comment, purchase, location check that appears to be harmless digital activity gradually builds a detailed mosaic of individual's psychological profile. This creates a "digital panopticon" where every online action contributes to a continuously refined psychographic dossier, enabling adversaries to understand and predict cognitive vulnerabilities with unprecedented accuracy [7]. Thus, over time these profiles become so refined that it can predict how specific people or communities are likely to react to particular messages. The humongous scale and depth of this profiling allows adversaries to identify the most "persuadable" individuals- those whose psychological makeup makes them especially susceptible to targeted narratives. In Indian context, these narratives can be customized around religious, linguistic, caste-based, regional identities, historical grievances, or political preferences, making the influence operation appear more authentic and personally relevant.

2.2 AI-Driven Narrative Optimization and Dissemination: The Echo Chamber as a Weapon in India

Once psychological profiles are established, artificial intelligence is deployed to tailor narratives with surgical precision for maximum cognitive impact. The objective is not just to persuade people but to engineer emotional reactions. Therefore, messages are crafted in ways that resonates deeply with individual's pre-existing biases, emotional states, values, effectively bypassing critical rational deliberation [5] [7]. What makes this process so dangerous is that these messages feel neutral, natural, relevant and personally meaningful that causes the target to lower their intellectual defences without realizing it. In India, these optimized narratives are disseminated through a vast ecosystem of digital platforms ranging from social media platforms like WhatsApp, YouTube, Facebook to encrypted messaging platforms, and even seemingly innocuous online forums often in multiple regional languages. Because the content is moulded and customized for different linguistic, cultural, religious, caste-based and political audiences, different sections of society are exposed to different versions of reality. The ultimate goal is not to convince everyone of one truth but to ensure no truth remains. Fragmentation and polarization become the strategic objective. What is most vicious about this is that it creates self-reinforcing "echo chambers" and "filter bubbles" by feeding people the same ideas and content that reinforce their existing beliefs while simultaneously demonizing alternative or opposing viewpoints [7]. These closed information environments over time solidify partisan identities and systematically erode the capacity for critical thinking and empathetic engagement across societal divides. This leads to intensified societal polarization as opposing viewpoints are no longer seen as disagreements but as threats. What makes this pervasively sharp is its adaptability. These narratives are continuously optimized in real time and are amplified through automated bot networks, influencers, coordinated online campaigns and seemingly ordinary users. The attacks evolve constantly, exploiting India's diversity and cultural fault lines to maximize impact. The result is a weaponized information environment where algorithms don't merely reflect social divisions but actively deepen them turning digital platforms into the battlegrounds where perception, identity and reality itself are contested.

2.3 Exploitation of Cognitive Biases and Emotional Vulnerabilities: The Hijacking of Human Cognition in India

The most dangerous dimension of this psychographic micro-targeting is the weaponization of human psychology itself. At its core, it is a sophisticated exercise in exploiting the inherent human cognitive biases and emotional vulnerabilities. While foundational research identifies inherent cognitive shortcuts such as availability heuristics and confirmation bias [11], modern adversaries systematically weaponize these vulnerabilities for strategic advantage [5] [7]. The narratives

are designed to trigger anger, fear to bypass rational processing, provoke emotional and impulsive reactions and thereby increasing the susceptibility to misinformation. The strategic induction of stress and attentional saturation further degrades the capacity for critical evaluation making individuals prone to accepting simplified, sensational and emotionally charged messages. In India, this deliberate cognitive hijacking aims to:

- Degrade information processing: Individuals are flooded with a constant stream of conflicting, sensational and emotionally charged information, often delivered in local languages and cultural contexts. It leads to cognitive overload and impaired decision-making capacity.
- Distort perception of reality: Instead of debating facts, it creates alternative realities in which objective truths becomes secondary to personal perception. Historical events, social issues and political developments are framed through an emotionally compelling and appealing lens, resonating with a specific audience. Over time, facts lose their authority as feelings preside themselves as the primary measure of truth. This fragmentation of reality weakens collective decision-making and fuels an endless cycle of polarization, fostering epistemic relativism.
- Undermine Institutional Trust: It systematically erodes the trust in traditional sources of authority, such as governments, media organisations, academic institutions, and scientists by portraying them as biased, corrupt, deceptive and incompetent. Existing grievances and historical distrust are amplified until citizens begin questioning every source of information except those that reinforce their existing worldview. As trust is not merely about transparency but about the perceived 'trustworthiness' of institutions [9], this collapse leaves citizens more susceptible to emotionally appealing narratives and less capable of distinguishing credible information from manipulation.

By meticulously targeting the cognitive and emotional weak points, psychographic micro-targeting does not merely influence opinions; it reconfigures the cognitive landscape in which opinions are formed. It alters how people process information, whom they trust and how they perceive reality; it attacks the cognitive sovereignty: the freedom to think independently and make informed and reasoned judgement, directly attacking the epistemic integrity of India’s democratic societies. A country can recover from military defeat, political crises and economic crises; recovering from a society that has lost its collective and shared capacity for truth, trust and sense-making is far more difficult. That’s why psychographic micro-targeting is particularly dangerous because it festers and feeds over the human consciousness itself. It’s a struggle for control over human cognition itself.

3. Geopolitical Implications: The External Stakes of an Internal War

This weaponization of psychographic micro-targeting in cognitive warfare carries profound geopolitical implications for India by fundamentally altering the dynamics of its international relations and posing an existential threat to the liberal international order itself. The systemic erosion of democratic epistemology within the domestic boundary inevitably spills over in the international arena as a country internally divided by manipulated narratives becomes less cohesive, less predictable and less capable of acting as a unified strategic actor. Ultimately, fostering a fractured global order characterized by heightened instability, diminished cooperation and a pervasive climate of distrust particularly in Indo-pacific region.

3.1 Destabilization of India's Democratic Alliances and Internal Cohesion

Psychographic micro-targeting campaigns are often designed to exploit the existing societal fault lines within democratic states, exacerbating polarization and undermining internal cohesion. For India; the danger is particularly acute because of its immense diversity. Adversaries do not need to create new divisions; they only need to amplify existing ethnic,

ideological, linguistic, religious and regional fault lines. By continuously feeding different groups narratives tailored to their fears and grievances, it further entrenches the divisions, deepens the polarization and weakens social cohesion. When India is internally divided, its capacity for collective defence, multilateral cooperation and regional leadership is severely hampered [6]. As public trust in institutions declines and internal discord rises, India’s ability to formulate coherent policies, sustain democratic consensus and project strategic confidence abroad becomes increasingly constrained as it leads to decline in public support for international commitments, trade agreements and collective security initiatives. The internal destabilization directly impacts the strength and efficacy of India’s democratic alliances and its ability to project a unified foreign policy. A fragmented society inevitably produces a fragmented state. In this sense, psychographic micro-targeting offers adversaries a method of reducing a nation's geopolitical influence without engaging in conventional military confrontation.

3.2 The Rise of Epistemic Sovereignty as a National Security Concern for India

In an environment where cognitive manipulation is pervasive, the concept of epistemic sovereignty looms as a critical national security concern for India. Traditionally, national security focused on defending territory, borders and physical infrastructure. Later, cybersecurity expanded the definition to include digital systems, the next frontier is the cognitive domain itself. A country may possess strong armed forces, advanced technology and secure borders, yet still be strategically vulnerable if foreign actors can manipulate the perceptions, beliefs and emotions of its population from afar. Epistemic sovereignty, as an emerging concept in cognitive security, refers to a state's capacity to protect its citizen's cognitive processes from external manipulation and maintain the shared understanding of reality necessary for effective governance [12]. The weaponization of psychographic micro-targeting directly challenges this sovereignty, as foreign actors no longer need to occupy territory to weaken a country; it can penetrate and manipulate India's collective consciousness of society through algorithms, personalized narratives and psychological manipulation without crossing physical borders. This necessitates a 'securitization' of the cognitive domain [8], where protecting India's future now requires safeguarding the nation's cognitive infrastructure, public trust, resilience of public discourse and shared reality. This hovering sword is sharper especially given the unique socio-technical landscape and the sheer scale of its digital population [7].

3.3 Amplification of Great Power Competition and Hybrid Warfare in the Indo-Pacific

Psychographic micro-targeting serves as a powerful force multiplier in great power competition and hybrid warfare strategies, particularly in Indo-Pacific where rivalry is intensifying. It can conveniently alter the balance of power while maintaining plausible deniability. By enabling precision at scale, it allows revisionist powers such as China, to achieve strategic objectives below the threshold of armed conflict, avoiding direct military confrontation while still undermining adversaries like India [7]. This approach evolves from traditional frameworks such as China's 'Three Warfares' doctrine encompassing media, psychological and legal warfare [13], into modern, AI augmented cognitive operations that target India's organizational foundation [10]. This includes:

- Shaping global narratives by manipulating international public opinion to gain diplomatic advantage, justify aggressive actions, or isolate India on the global stage.
- Undermining India’s legitimacy by discrediting its government, political systems, and international narratives through the amplification of existing grievances and societal tensions via carefully crafted campaigns tailored to linguistic, cultural, regional, or ideological sensitivities.
- Interfering in India's democratic processes by influencing elections, policy debates, public consultations and social movements to promote favourable outcomes or destabilise political systems, often done through the coordinated disinformation networks and dissemination of deepfakes [7].

These tactics contribute to a more unpredictable and volatile international system where lines between peace and conflict are rapidly eroding. Cognitive Warfare operates in the grey zone where attribution remains challenging. The ability to wage effective cognitive warfare becomes a critical component of state power, countries that master cognitive warfare gain the ability to influence adversaries from within, turning their citizens, institutions and information ecosystems into instruments of strategic competition. The most consequential battles of 21st century may occur inside the minds of societies themselves, compelling India to invest heavily in both offensive and defensive capabilities.

4. The Path to Cognitive Sovereignty: Strategic Imperatives for India

India must acknowledge the uniqueness and urgency of the cognitive security challenge and must develop a doctrinal strategy to achieve the cognitive sovereignty. This involves transforming Indian demographic and institutional assets into a robust cognitive resilience resource rather than merely adopting defence posture designed for smaller, more homogenous polities [7].

The first pillar of this strategy is building indigenous AI for cognitive defence. India cannot rely entirely on foreign technological ecosystems to defend itself against sophisticated psychological operations. India must invest in and develop India specific AI capabilities for sentiment analysis, threat detection and counter disinformation campaigns across India's diverse linguistic and cultural landscape. This includes leveraging India's vast talent pool in AI to create sovereign solutions that can identify and neutralize psychographic micro-targeting campaigns.

Technology alone cannot solve a psychological problem and therefore the second pillar of this strategy is strengthening epistemic immunity through education. A society that understands how manipulation works becomes far harder to manipulate. The strongest defence against cognitive warfare is not surveillance or censorship but a population capable of questioning information, evaluating evidence and resisting emotional manipulation. India must implement comprehensive educational initiatives focused on critical thinking, digital literacy and media discernment across all levels of society.

A third imperative is the development of robust regulatory framework. Since psychographic micro-targeting relies heavily on the collection and exploitation of personal data, establishing clear and enforceable data privacy laws and ethical AI governance guidelines should be put in place. This includes mandating greater transparency from social media platforms and AI developers regarding content dissemination and targeting algorithms. The goal is to prevent digital platforms from becoming unregulated weapons capable of influencing entire population without oversight.

The most ambitious imperative extends beyond India's borders. India must leverage its growing geopolitical influence to foster international norm leadership and champion a Cognitive Warfare Conduct Convention. This multilateral normative framework would establish binding red lines for the use of AI in information warfare operations, positioning India as a leader in shaping global governance for the cognitive domain.

5. Conclusion: Securing India's Cognitive Frontier

The greatest threat to a country in 21st century may not be an invading army but the silent manipulation of its collective consciousness. The weaponization of psychographic micro-targeting represents a profound and evolving national security threat to India's democratic epistemology and national security. The intricate interplay of advanced artificial intelligence, behavioural psychology and India's unique socio-technical environment creates a fertile ground for algorithmic manipulation leading to the disintegration of shared reality and fracturing of societal cohesion. The paper had demonstrated that the mechanism of this threat is deeply embedded in the digital infrastructure, exploiting cognitive biases and emotional vulnerabilities with unprecedented precision. The geopolitical implications are equally severe,

impacting India's internal stability, democratic alliances and its strategic position in the Indo-Pacific particularly in the face of doctrines like Chinese "Three Warfares."

For India, the challenge is particularly consequential as hostile actors can exploit its immense digital population, extraordinary diversity and vibrant democratic ecosystem to deepen polarization, weaken institutional trust, distort public discourse and ultimately reduce India's strategic coherence. What begins as disinformation on a screen can evolve into societal fragmentation, political instability and geopolitical vulnerability. India's path to cognitive sovereignty is not merely a defensive posture but a strategic imperative for its continued growth and influence on the global stage. By investing in indigenous AI capabilities, strengthening epistemic immunity through education, developing robust regulatory framework and fostering international norm leadership, India can transform its vulnerabilities into strengths. The challenge is immense but so is the opportunity for India to lead in defining the ethical and strategic boundaries of cognitive warfare. Securing the cognitive frontier is paramount to safeguarding India's democratic future and ensuring its strategic autonomy in an increasingly complex and manipulated global information environment.

References:

1. NATO Science and Technology Organization (STO). "Cognitive Warfare." Chief Scientist's Report. Accessed June 26, 2026. https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-final.pdf.
2. Giordano, James. "Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness." Strategic Insights, Institute for National Strategic Studies (INSS), National Defense University (NDU), January 6, 2026. https://digitalcommons.ndu.edu/strategic-insights/44/.
3. Claverie, Bernard, and François du Cluzel. "Cognitive Warfare: The New Battlefield Exploiting Our Brains." Polytechnique Insights, February 5, 2025. https://www.polytechnique-insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield-exploiting-our-brains/.
4. Schmidle, Robert (LtGen, USMC, ret). "Cognitive Warfare and the Future of Strategic Competition." Small Wars Journal, June 5, 2026. https://smallwarsjournal.com/2026/06/05/cognitive-warfare-at-the-crossroads-defining-and-developing-capabilities/.
5. Marsili, Marco. "Cognitive Warfare in Historical Perspective: From Cold War Psychological Operations to AI-Driven Information Campaigns." Preprints.org, December 16, 2025. https://doi.org/10.20944/preprints202512.1596.v1.
6. Awasthi, Soumya. "Artificial Intelligence and India's National Security." ORF Online, March 28, 2026. https://www.orfonline.org/expert-speak/artificial-intelligence-and-india-s-national-security.
7. Bandvi, Aman. "Winning Without Losing: India's Cognitive Security Imperative in an Era of AI-Enabled Warfare." SSRN, March 2, 2026. https://ssrn.com/abstract=6326238.
8. Buzan, Barry, Ole Wæver, and Jaap de Wilde. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers, 1998.
9. O'Neill, Onora. A Question of Trust: The BBC Reith Lectures 2002. Cambridge: Cambridge University Press, 2002.
10. Ali, Taha. "Cognitive Combat: Understanding China's Three Warfare Doctrine." Geojuris Today, June 3, 2025. https://www.geojuristoday.in/post/cognitive-combat-understanding-china-s-three-warfare-doctrine.
11. Kahneman, Daniel. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011.
12. Puri, Lakshmi. "We are facing a narrative war on the mind. Cognitive sovereignty is…." X (Twitter), February 15, 2026. https://x.com/lakshmiunwomen/status/2023021583275827410.

13. Singh, Abhijit. “China’s ‘Three Warfares’ and India.” Journal of Defence Studies 7, no. 4 (October-December 2013): 27-46. https://idsa.in/system/files/jds_7_4_AbhijitSingh.pdf.

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

Image Source: ChatGPT