USI Monograph No 3 - 2026

Cognitive Warfare by China and India's Response

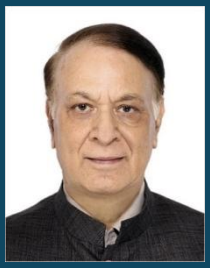
Major General BK Sharma, AVSM, SM** (Retd)

Major General Sanjeev Chowdhry (Retd)

United Service Institution of India (USI)

New Delhi

About the Authors



Major General BK Sharma, AVSM, SM** (Retd) is an Infantry veteran. He is a noted strategic analyst and national security expert with over four decades of experience. He served as Director General of the USI from 2020 to 2025. A recipient of three Presidential award, his career includes diverse command, instructional, and senior staff appointments, including service in the Ministry of Defence. He has served as a United Nations Military Observer in Central America and as India's Defence Attaché in Central Asia. He also commanded a formation as General Officer Commanding and served as Senior Faculty at the National Defence College (NDC). An alumnus of Defence Services Staff College, Higher Command, and NDC, his expertise includes strategic net assessment, scenario building, strategic gaming, red teaming, and multi-domain warfare. He is widely recognised for his insights on emerging security challenges.

Major General Sanjeev Chowdhry (Retd) is a senior Indian Army veteran with extensive experience in military operations and strategic studies. During his distinguished service, he held key command and staff appointments and contributed significantly to professional military education and strategic discourse. An alumnus of the Defence Services Staff College and the College of Defence Management, he has served as an instructor at the Defence Services Staff College and the Special Frontier Force Academy and has also served as a United Nations Military Observer. He is currently associated with the USI as Director, Centre for Publications and Library. His areas of interest include emerging technologies, net assessment, and strategic affairs.

Cognitive Warfare by China and India's Response

Cognitive Warfare by China and India's Response

Major General BK Sharma, AVSM, SM (Retd)**

Major General Sanjeev Chowdhry (Retd)

***(Estd.* 1870)**

United Service Institution of India (USI)

New Delhi

Published by
The United Service Institution of India
Rao Tula Ram Marg,
New Delhi - 110 057
website: www.usiofindia.org

First Published in India in 2026

₹350

Contents

Introduction

"In modern war, the battlefield extends into the human brain. The aim is no longer to destroy the enemy's forces, but to erode his will, distort his perception, and capture his decision-making space"

- **Adapted From People's Liberation Army's Doctrinal Writings on Cognitive Domain Operations.**

Cognitive Warfare as the New Battlespace

Cognitive warfare has become a central feature of modern strategic competition, where shaping perceptions, narratives, and decision-making is increasingly decisive. Unlike traditional information operations, it targets the mind as the primary battlespace, aiming to weaken the will, fracture societies, and influence political outcomes without using force. This reflects a broader shift toward systems confrontation, where control of information and perception is key to strategic advantage.[1]

Cognitive warfare is distinguished by several defining features that reveal how it operates and why it is increasingly central to modern competition. Its nature lies in deliberately shaping or altering how individuals and societies perceive reality, make judgments, and process information. Its purpose is not merely to inform or persuade but to secure strategic advantages—political, military, economic, or ideological—without resorting to open conflict. Its method revolves around exploiting the inherent limits

and biases of the human mind, including fear, emotion, trust, identity, and social cohesion. Technology amplifies these effects by enabling rapid, precise, and large-scale dissemination through digital platforms, AI-based tools, bots, deepfakes, and data analytics. Finally, the target of cognitive warfare is broad: it seeks to influence entire populations, not only decision-makers, recognising that societal attitudes, morale, and collective behaviour can shape national outcomes as decisively as elite actions.

China is the leading practitioner of this model, combining its philosophical traditions, the People's Liberation Army's (PLAs) Three Warfares' strategy, and new institutions like the 'Information Support Force' to execute integrated influence campaigns across political, military, and societal domains. Its goal is clear: achieve Mind Dominance' by controlling narratives, weakening cohesion, and shaping adversary choices without direct conflict.

The Globalisation of the Cognitive Battlespace

Digital platforms have expanded cognitive warfare into a persistent, borderless contest. Through social media, streaming platforms, online gaming, and artificial-intelligence-driven content engines, influence operations now reach individuals continuously, making every citizen a potential receiver and transmitter of hostile narratives. Certain Chinese digital platforms and technology firms—such as TikTok, WeChat, other ByteDance or Tencent services, and Huawei's telecom infrastructure—

operate primarily as commercial products. However, because they are subject to China's data and cybersecurity laws, some governments view them as potential channels for influence, data access, or content curation that could align with Beijing's strategic interests. While no definitive evidence shows systematic ideological use abroad, the structural risk remains part of the broader cognitive security debate. This environment blurs the lines between peace and conflict: there are no frontlines, no ceasefires, and no distinction between combatants and civilians. The Communist Party of China (CPC) and PLA view this cognitive turn as the apex of future warfare, blending neuroscience, Artificial Intelligence (AI), and behavioural science to shape emotions, disrupt cohesion, and capture decision space faster than an adversary can counter.

Implications for India and the Strategic Response Required

For India, cognitive warfare presents a direct and complex challenge. China's India-focused operations seek to weaken national cohesion, undermine institutional trust, distort public discourse, and reduce India's regional influence. These efforts exploit India's open information environment, linguistic diversity, civil society networks, and South Asian geopolitics by influencing media, academia, the diaspora, and public sentiment. The aim is not kinetic damage but strategic paralysis—dividing society, demoralising institutions, and constraining India's decision-making.

Addressing this requires a whole-of-nation cognitive warfare strategy that maps vulnerabilities, strengthens societal resilience, enhances strategic communication, ensures rapid attribution of malign activity, and integrates diplomatic, technological, and military instruments into a coherent national response.

This monograph examines China's philosophy, doctrine, and practice of cognitive warfare, assesses its manifestations across regional and global theatres, and evaluates their implications for India's national security. It proposes a comprehensive response framework—doctrinal, organisational, technological, and societal—that can equip India to safeguard strategic autonomy, strengthen cognitive resilience, and contest adversarial influence in the evolving battlespace of the 21st Century. It ultimately argues that India must institutionalise cognitive security as a core pillar of national security, embedding it across doctrine, governance, technology, and society to safeguard decision-making and strategic autonomy.

China's Cognitive Warfare: Philosophy and Evolution

China's contemporary cognitive warfare framework is the product of a long civilisational tradition in which strategy, governance, and political authority have converged around the management of perceptions and the shaping of human behaviour. Its evolution reflects an unbroken continuum—from classical

philosophy to modern communist political practice—through which the Chinese state has consistently treated the mind as the decisive terrain of conflict. The architecture of China's cognitive warfare cannot be understood without tracing its civilisational lineage of perception control, a tradition that predates the modern state by millennia. At its core lies a uniquely Chinese synthesis of Sun Tzu's military philosophy, Confucianism, Legalism, and Daoism, which collectively underpin the strategic culture of the CPC.

Sun Tzu (544–496 BCE). He laid the earliest intellectual foundations of what is now understood as cognitive warfare through *The Art of War* (c. 5th century BCE).[2,3] He reconceptualised warfare as a contest of perception, judgment, and will, rather than brute force, famously asserting that 'All warfare is based on deception'.[4] By elevating deception, indirectness, and ambiguity to core strategic principles, Sun Tzu argued that the highest form of victory is to subdue the enemy without fighting.[5,6] His emphasis on manipulating adversary calculations, inducing uncertainty, and achieving psychological paralysis established the human mind as the primary battlefield, a logic that continues to underpin modern approaches to cognitive and information warfare.[7,8]

Confucius (551–479 BCE). He provided a complementary foundation to what is now understood as cognitive warfare by linking political power to moral authority, legitimacy, and psychological influence rather than coercion alone.[9] Confucian thought

emphasised governance through *de* (virtue), *li* (ritual propriety), and exemplary conduct, shaping societal norms and emotional stability from within.[10] By cultivating obedience through belief, trust, and ethical leadership, Confucianism demonstrated that durable control is achieved when authority is internalised rather than imposed.[11] This logic—that influence over perception and legitimacy can secure long-term order—remains central to modern cognitive warfare, strategic influence, and legitimacy-based governance.[12]

Legalism. Founded by Shang Yang (c. 390–338 BCE) and later systematised by Han Fei (c. 280–233 BCE), introduced a distinct and enduring contribution to cognitive warfare.[13,14] In contrast to Confucian moral suasion, Legalism advanced a cognitive logic rooted in fear, predictability, and control, treating behaviour as something to be engineered rather than inspired.[15] Legalist governance sought to dominate the psychological environment by tightly managing information flows, standardising rewards and punishments, and eliminating ambiguity in authority.[16] Compliance was achieved not through belief, but through calculated anticipation of consequences, leading individuals to internalise state power.[17] This fusion of virtue (Confucianism) and fear (Legalism) became central to China's enduring dual-track approach to cognitive warfare, shaping behaviour by influencing both belief and risk perception.[18]

The Thirty-Six Stratagems. An anonymous compendium originating in the Warring States period (c. 475–221 BCE) and later systematised during the Ming–Qing eras—represents one of the earliest handbooks of cognitive warfare in practice.[19,20] Rather than prescribing moral authority or legal control, the stratagems codified a repertoire of ruses, deception, misdirection, and psychological manipulation, focusing explicitly on shaping an adversary's perceptions, expectations, and decision-making rather than defeating them through force.[21] Each stratagem is designed to engineer miscalculation, induce confusion, or exploit emotional and situational biases, thereby, gaining advantage through mental disruption.[22] This logic continues to inform China's contemporary approach to cognitive warfare, visible in strategic signalling, crisis manipulation, and calibrated narrative operations aimed at controlling how events are interpreted rather than fought.[23]

Mao Zedong (1893–1976). He transformed classical Chinese strategic thought into a modern, mass-based doctrine of cognitive warfare by embedding psychological influence at the core of revolutionary and state power.[24] Maoist warfare operationalised cognition through propaganda, United Front work, and organised mass mobilisation, making control over beliefs, narratives, and political consciousness as decisive as military action itself.[25] By embedding ideology into daily life and framing struggle as

continuous, Mao elevated political warfare into a permanent condition, deliberately blurring the boundaries between war and peace.[26] This approach institutionalised cognitive warfare at the societal level, using narrative dominance and emotional mobilisation to sustain internal cohesion while contesting external adversaries.[27,28]

The Three Warfares (2003). The PLA institutionalised modern Chinese cognitive warfare through the doctrine of the Three Warfares (2003), developed and promulgated via its General Political Department—now the Political Work Department of the Central Military Commission—and formally codified in the PLA Political Work Regulations (2003).[29,30] Rather than reflecting the ideas of a single strategist, the doctrine represents collective authorship by the PLA's political–strategic establishment, including political commissars and military theorists responsible for integrating ideology, law, and information into warfare.[31] The framework institutionalised public opinion warfare, psychological warfare, and legal warfare as standing instruments of state-directed cognitive warfare, enabling China to shape global narratives, manipulate adversary perceptions, and legitimise state actions in international forums—below the threshold of armed conflict.[32]

Xi's Cognitive Operations. Under Xi Jinping, cognitive warfare has evolved into a highly sophisticated, globally coordinated, and ideologically

Framed instrument of state power.[33] Xi's emphasis on 'Mind Dominance' extends the Three Warfares into digital, psychological, and emerging neuro-technological domains, explicitly treating the human brain as the primary battlespace.[34] With the establishment of the PLA Information Support Force, China has unified cyber, space, information, and cognitive operations under a single operational framework.[35] This structure enables the coordinated use of AI-driven tools, data analytics, and influence ecosystems to shape global narratives, undermine adversary cohesion, and influence perceptions at strategic, operational, and tactical levels.[36] Xi's overarching objective is to set the terms of global discourse and secure strategic outcomes without resorting to major kinetic force, reinforcing cognitive warfare as a central pillar of China's contemporary statecraft.[37]

Together, the above traditions form an integrated cognitive warfare doctrine that enables China to shape perceptions, manipulate decision-making, and secure strategic advantage without open conflict.

Chapter 1

The Game of Go

The Game as Metaphor: Encirclement over Annihilation

Among China's most enduring strategic metaphors, none captures its intellectual and cultural approach to conflict more vividly than the ancient board game *Weiqi* (Go).[38] Unlike chess—which prizes decisive, head-on engagements culminating in the annihilation of the opponent's pieces—Go rewards patience, encirclement, and positional advantage. Its essence lies not in destruction but in gradually constraining the adversary's options until capitulation becomes inevitable.

In this worldview, each move is deliberate and multidimensional, representing a narrative, alliance, or an act of influence. The objective is to control the cognitive and strategic space, not merely to win a battle. The parallels with China's evolving doctrine of cognitive warfare are striking. As articulated by PLA theorists, the decisive contest is no longer kinetic but psychological—a struggle to shape perceptions, guide decision-making, and dominate the adversary's understanding of reality.

Translating Go Logic into Doctrine

The PLA's concept of Cognitive Domain Operations closely mirrors the strategic grammar of Go. In this ancient game, the expert player anticipates not just one or two moves ahead but dozens of them, weighing local

engagements against the board's global configuration. Likewise, the PLA envisions cognitive warfare as a multidimensional and continuously adaptive contest, integrating diplomacy, technology, military posture, and narrative control within a dynamic strategic geometry.

Go Board Strategy of Influence and Control

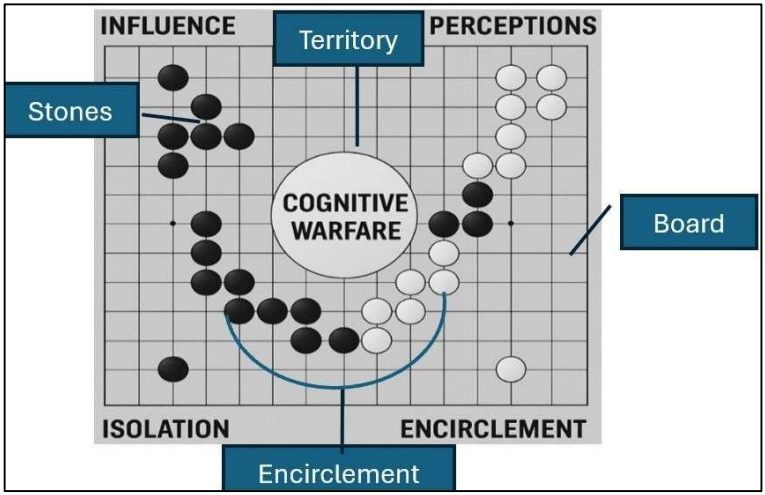


Figure 1: Cognitive Warfare and *Weiqi*

Source: Created by Authors

China's Game-of-Go Approach. Building on the philosophical lineage and institutional evolution described in Philosophy and Evolution—China's Cognitive Warfare, the Game-of-Go analogy translates classical strategic precepts and modern PLA practice into an operational model for cognitive competition. Viewed through the strategic lens of Go, China's long-standing intellectual traditions—ranging from the classical principles associated with Sun Tzu, Confucianism, Legalism, and

the 36 Stratagems—converge with Maoist-era political warfare and the PLA's institutionalisation of the Three Warfares to form a coherent cognitive strategy. Together, these elements produce a patient, sequenced, and multidomain campaign in which dispersed influence activities accumulate into durable strategic advantage.

Board: The Cognitive Domain. The 'Board' refers to the full space where opinions and narratives are shaped—publics, leaders, allies, and media. China treats this as a real battleground, acting early to influence key people and institutions so that later events are seen through a favourable lens. Its Three Warfares strategy provides organised methods to shape these arenas, treating information as an active domain of operations.

Stones: Influence Tools. The 'Stones' are the actual tools China places on the information battlefield. These include its state media, friendly foreign media, social-media platforms and algorithms, diaspora networks, and academic or think-tank channels. Through these tools, China spreads targeted messages. Importantly, these tools are not used randomly—they are coordinated across the party, government, and military to work together toward the same influence goals.

Territory: Control of Perceptions. In cognitive warfare, 'Territory' is the space of accepted beliefs and interpretations in a population or audience. It

means the beliefs, views, and assumptions that people already accept and is the mental space where certain narratives feel normal, trustworthy, or legitimate. Once this space is shaped, people tend to interpret new events through these existing ideas. China aims to control this territory by presenting its actions as lawful, moral, or civilisational. By doing so, it creates stable narratives that are harder for others to challenge.

Encirclement: Isolation of Adversary Options. 'Encirclement' means limiting an adversary's choices. When China places its stones in a way that surrounds the opponent—through legal arguments, media pressure, economic tools, and influence on allies—it gradually reduces the other side's political and diplomatic room to act. This makes any strong response costly or difficult. This approach reflects older Chinese ideas: using rules to control behaviour and applying broad, non-military pressure to wear down the opponent.

Sacrifice: Tactical Narratives Traded for Strategic Legitimacy. 'Sacrifice' means giving up a small narrative advantage now to gain a bigger strategic legitimacy later. China may accept minor criticism, concede a small point, or take a short-term reputational hit if it helps build a long-term image of fairness, responsibility, or moral authority. By trading short-term narratives for long-term legitimacy, it strengthens its position and shapes the wider story in its favour.

End Game: Strategic Exhaustion. The 'Endgame' is when many small information advantages accumulate and produce significant political effects. The goal is to wear down the opponent's will, weaken their alliances, and make the challenger's position seem normal and acceptable. This reflects the classic Sun Tzu idea of winning without fighting, now done with modern tools such as AI-driven messaging, targeted online influence, and steady diplomatic pressure that drain the opponent's attention, credibility, and desire to continue resisting.

Strategic Implication. China's cognitive warfare model shows a deliberate strategy to win advantage without fighting by shaping how audiences think, decide, and interpret events. It treats the information space as a battlefield, deploys coordinated influence tools, works to control accepted beliefs, constrains opponents' options through legal, economic, and media pressure, trades small narrative losses for greater legitimacy, and accumulates these incremental gains to wear down adversaries and normalise outcomes favourable to China. The strategic effect is a gradual but powerful shift in the political and perceptual landscape that makes resistance harder and China's preferred positions increasingly acceptable.

Cognitive Warfare: Strategic Guidance Three Warfares (2003). China's origins of cognitive warfare lie in the Three Warfares framework introduced in 2003—Legal Warfare, Psychological Warfare, and

Public Opinion Warfare.[39] These tools were designed to shape the information environment well before conflict began—legal warfare aimed to justify China's actions internationally and constrain adversaries through selective interpretation of laws. Psychological warfare focused on weakening morale, cohesion, and decision-making. Public opinion warfare sought dominance over domestic and global narratives to influence perceptions of legitimacy. Together, these mechanisms allowed China to sow confusion, manipulate global sentiment, and create strategic advantages without resorting to kinetic force.

Cognitive Warfare (2020s). By the 2020s, China's approach had evolved into a far more advanced, technology-driven architecture of influence. Cognitive warfare now leverages AI, big data, social media manipulation, and automated messaging systems to shape perceptions at a population scale.[40] This era marked the shift from narrative control to perception engineering, enabling China to conduct rapid, adaptive influence operations that were increasingly difficult to counter. With pervasive digital platforms and algorithmic targeting, cognitive warfare became a seamless blend of information manipulation, psychological conditioning, and technological exploitation aimed at weakening adversaries from within.

Global Civilisational Initiative (GCI-2023). China's GCI is a persuasive strategy to win popular support across the globe. President Xi Jinping introduced this initiative on 15

Mar 2023 at the CPC in Dialogue with the World Political Parties High-Level Meeting.[41] The GCI is designed to soften perceptions of Chinese neo-imperialism associated with the Belt and Road Initiative (BRI) by promoting cultural exchange and cooperation amid a divided international environment. President Xi highlights tolerance, coexistence, and mutual learning as crucial to shared modernisation and global harmony. Beyond projecting soft power, the GCI seeks to reshape international narratives on culture and identity, complementing China's broader strategic objectives and reinforcing the BRI's global reception.

Information Warfare. Information warfare is the deliberate control and manipulation of information flow to influence perceptions and operational outcomes. It shows two converging pathways: one on the left, where Electronic Warfare (EW)—including jamming, spoofing, and suppression of radar or communications—creates confusion and undermines morale by disrupting an adversary's ability to access accurate information. On the right, cyber operations targets networks and data—through hacking, disruption, and the spread of disinformation—erode trust, and enable deceptive narratives. Together, these complementary approaches shape the information environment by simultaneously denying enemy reliable information and adding manipulated content,

thereby, achieving cognitive and psychological advantage in conflict.

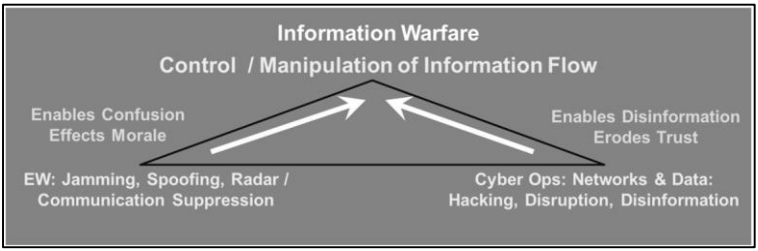


Figure 2: Information Warfare

Source: Created by Authors

Cyber Warfare. Cyber warfare comprises offensive and defensive operations conducted in the digital domain to infiltrate, disrupt, degrade, or manipulate an adversary's information systems. China uses cyber warfare to steal sensitive data, alter digital records, compromise critical infrastructure, and exploit vulnerabilities to influence political and military outcomes. Unlike traditional information warfare, cyber warfare operates directly on the architecture of digital networks, enabling silent penetration, persistent access, and covert disruption. This capability allows China to prepare the battlefield in peacetime, weaken institutional trust, and support broader cognitive and influence campaigns with precise, deniable digital attacks.

Influence Operations. Influence operations seek to shape perceptions, strategic choices, and political behaviour in targeted societies. They use disinformation, propaganda, strategic messaging, and targeted digital content to manipulate how

individuals and institutions interpret events. Their objective is to alter public sentiment, weaken alliances, create internal divisions, and influence national decision-making. By harvesting data and using AI-enabled sentiment analysis, influence operations have become more precise and scalable, allowing adversaries to reach populations directly without reliance on traditional media.[42]

Psychological Warfare. Psychological warfare targets the mindset, morale, and social cohesion of adversaries. Its purpose is to degrade willpower, create fear or uncertainty, exploit cognitive biases, and erode trust in institutions. Methods include coercion, deception, tailored propaganda, psychological pressure, and manipulation of identity or social vulnerabilities. By attacking the psychological foundations of a society—its unity, confidence, and conviction—psychological warfare seeks to achieve strategic outcomes without kinetic confrontation**.**

Together, these strands constitute the modern architecture of cognitive warfare—where information, psychology, and influence converge to shape decisions, perceptions, and national resilience. The evolution from the Three Warfares to a fully integrated cognitive warfare doctrine marks a decisive shift in global competition, one where the human mind has become the principal battlespace.

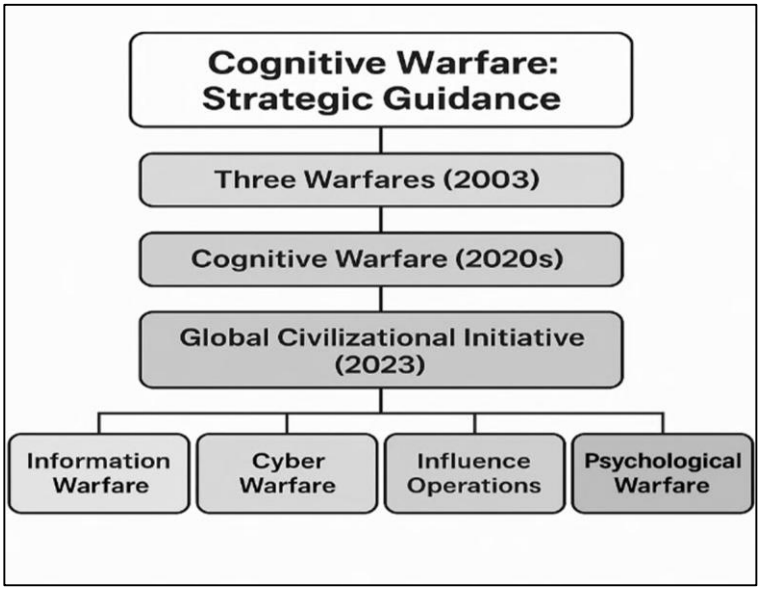


Figure 3: Evolution of Cognitive Warfare in China's Strategic Framework

Source: Created by Authors

Chapter 2

China's Cognitive Warfare Architecture and Ecosystem

Tenets of Chinese Cognitive-Warfare Strategy

China's concept of 'National Cognitive Security' is the security of its cognitive domain, i.e., the social cognition of the Chinese population against the forces that aim to interfere with and control cognition by using artificial intelligence, technologies such as deep fakes, social media robots, and precise algorithms.[43] China's cognitive operations can be sorted into four main categories: military intimidation, influence via bilateral exchange, religious interference, and disinformation and content farms on the internet.[44]

Modern conflict increasingly unfolds in the grey zone—a fluid space between peace and open war where states pursue strategic advantage by targeting perception, cohesion, and decision-making without triggering outright hostilities. This environment, characterised by deniability, calibrated actions, and attribution friction, enables adversaries to weaken morale, exploit societal divisions, and pressure political elites through a wide array of coercive tools. Within this context, the following framework explains how grey-zone operations focus on the human mind, employ multiple instruments simultaneously, pursue nested military-political-societal-strategic objectives, and seek an end state defined by sustained pressure in a 'No war, no peace' continuum. To understand how grey-zone and cognitive operations generate strategic

effects, we can break the mechanism down into five clear elements as tenets:

- **Target: Human Mind**. Demoralisation aims directly at unit and public morale; destabilisation exploits societal fault-lines and political legitimacy; indirect conflict and intervention pressure elites' decision calculus.
- **Means: Multitude**. The ambiguous arrow across the grey zone implies simultaneous use of many tools (media/Input/Output (I/O), cyber or EW, economic levers, United Front networks, legal narratives) that create attribution friction and plausible deniability.
- **Objectives (Nested Levels)**.
  - **Military**. Demoralisation reduces cohesion and the political will to sustain force.
  - **Political**. Destabilisation and lawfare shape domestic legitimacy and electoral or elite outcomes.
  - **Societal**. Exploiting fault lines accelerates fragmentation and civic distrust.
  - **Strategic**. Narrative control in the grey zone normalises outcomes and limits outside intervention, generating long-term advantage.

- **End State**. 'No War' toward 'No Peace' signals the strategic payoff—competitive advantage through persistent pressure short of open hostilities.

Figure 4: Grey Zone Conflict: Strategic Competition Between War and Peace

Source: Created by Authors

The diagram illustrates how modern conflict increasingly unfolds in the grey zone, a space between no war and no peace where states compete without crossing into open hostilities. In this ambiguous environment—defined by deniability, calibrated actions, and difficulty of attribution—adversaries employ a spectrum of coercive tools that escalate from demoralisation and destabilisation to indirect conflict and, at the upper edge, intervention. These actions deliberately exploit the threshold between peace and war, allowing a state to weaken an opponent's cohesion, institutions, and decision-making while avoiding the costs and risks of conventional warfare. The grey zone, thus, becomes the primary arena for cognitive warfare, influence operations, hybrid tactics, and strategic manipulation, enabling actors to achieve political or strategic gains without triggering formal conflict.

From Concept to Command: Institutionalising Cognitive Power

China operates a vertically integrated system directed from the apex of political power and executed through multiple functional layers.[45] The CPC designs cognitive objectives, defines ideological boundaries, and coordinates propaganda, cyber, and psychological operations across civilian and military institutions. Cognitive warfare is a permanent peacetime function aligned with the goal of 'Winning Without Fighting'.

Party level (Strategic). At the apex, the CPC provides strategic direction for informationised and intelligentised warfare, including cognitive warfare. The Politburo Standing Committee sets the overall political line, while the Central Propaganda Department controls ideology, narrative framing, media, and cultural outputs, shaping both domestic and international cognitive environments. The United Front Work Department (UFWD) spearheads influence operations abroad, focusing on diaspora control, elite co-option, and narrative penetration as part of wider 'Cognitive Infiltration'. Complementing these efforts, the Central Cyberspace Affairs Commission, chaired by President Xi Jinping, oversees cyber operations, online propaganda, and the deployment of digital tools that increasingly serve as instruments of cognitive warfare.

Central Military Commission (CMC) (Strategic–Military Integration). At the CMC level, the CPC guidance is translated into military doctrine and operational structures. The Political Work Department, successor to the PLA's General Political Department, directs psychological operations, propaganda, cultural-political indoctrination, and morale-shaping campaigns. The Strategic Support Force (SSF), established in 2015, integrates cyber, space, electronic, and psychological operations, with its Network Systems Department and Psychological Warfare units, providing direct support to cognitive warfare. Meanwhile, the Joint Staff Department, as the CMC's operational planning arm, incorporates the Three Warfares—public opinion, psychological, and legal warfare—into the design of joint campaigns.

Below the CMC (Operational/Execution). Below the CMC, a wide array of PLA, state, and auxiliary organs operationalise cognitive warfare. The PLA's SSF employs base units to conduct psychological warfare, social media operations, and AI-driven influence campaigns, with PLA Base 311 in Fuzhou serving as a flagship unit specialising in psychological operations against Taiwan. The PLA Academy of Military Sciences develops doctrine on 'Mind Superiority', human–machine integration, and cognitive domain operations, while the PLA National Defence University trains officers to incorporate cognitive warfare into joint campaign planning. Civilian intelligence services play a crucial role as well: the

Ministry of State Security undertakes covert influence, disinformation, and overseas psychological operations, coordinating with the UFWD and SSF's cyber-psychological units. Meanwhile, the Ministry of Public Security enforces domestic cognitive control through mass surveillance and 'Social Stability Maintenance', ensuring psychological dominance within the home front.

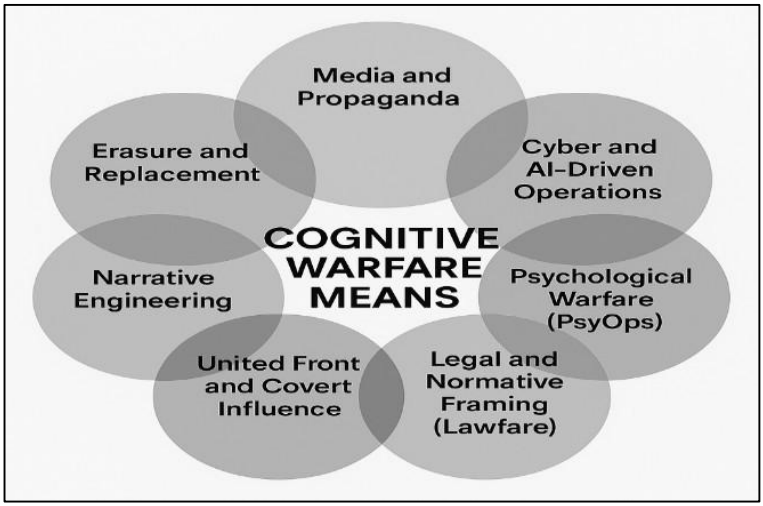
How the Architecture Functions. The architecture is explicitly whole-of-state and tightly networked: policy and narrative originate at the apex level in the party, is operationalised through military planners at the CMC, and executed by a layered set of civilian, military, and quasi-state actors that combine covert tradecraft, technical capabilities, and platform amplification.[46] Feedback loops matter: tactical effects are measured by Signal Intelligence (SIGINT) or cyber and media analytics, which inform doctrinal adjustments at research institutes and strategic refinements at the CPC's organs. Ambiguity and plausible deniability are operational features—covert nodes and proxy amplifiers permit aggressive cognitive action while reducing direct attribution to political leadership. The net effect is the capacity to calibrate persistent influence campaigns across peacetime and crisis, exploiting speed, scale and multi-modal integration to shape perceptions and constrain adversary choices.[47]

Chapter 3

Cognitive Warfare Means and Execution

Doctrine: The Conceptual Basis

China's cognitive warfare doctrine rests on shaping the adversary's perceptions, emotions, cohesion, and decision-making while reinforcing its own legitimacy and strategic freedom of action. The foundational logic integrates:



Cognitive Warfare Means

Figure 5: Instruments of Cognitive Warfare

Source: Created by Authors

- Narrative dominance and legitimacy shaping (rooted in public opinion Warfare).
- Psychological degradation of adversary morale and cohesion (psychological warfare).
- Legal positioning to constrain adversaries diplomatically (legal warfare).

- Technological systems enabling perception engineering at scale.

These doctrinal elements provide the strategic frame within which all subsequent means, mechanisms, and actions operate.

Media and Propaganda. State and state-aligned media outlets, official spokespersons, and surrogate channels such as think tanks, friendly foreign outlets, and sponsored influencers craft and amplify coherent narratives to shape what audiences accept as legitimate facts.[48] Tactics include editorial framing, selective release of imagery or documents, seeding sympathetic commentary in third-party media (borrowed boats)[49], and coordinated timing to outpace rebuttals.[50] Defensive measures focus on rapid evidence-based responses[51], platform cooperation for labelling or removal of coordinated inauthentic behaviour, and the creation of independent and trusted information channels.

Cyber and AI-Driven Operations. Technical means are employed to manipulate, scale, or corrupt information flows. Botnets and troll farms are used for amplification, while AI-generated content and deepfakes enable deception.[52] China's approach to cognitive warfare is rooted in the CPC's long-standing priority of maintaining ideological control. Domestically, this has been achieved through the 'Great Firewall', a combination of technical filtering, online monitoring, and platform manipulation that controls the flow of information. The CPC has

mastered the use of cyber tools to suppress dissent, censor unfavourable narratives, and flood digital spaces with state-approved messaging.[53] These techniques increase reach, speed, and attribution uncertainty. Defence requires hardened cyber hygiene for critical systems, advanced forensic and AI-detection tools, cooperation with digital platforms on takedowns, and resilient alternative communications.[54]

Psychological Warfare. Cognitive warfare is rooted in Sun Tzu's philosophy of winning without fighting. Over time, it has evolved through psychological operations, propaganda, cyber tactics, and the rise of AI.[55] Methods include targeted messaging to lower morale, sow doubt about leadership, or suspect reliability, staged incidents or leaks to incite fear, and repeated themes that exploit cultural or situational anxieties. Effective mitigation relies on transparent leadership communication, morale-building, and cohesion programs, trusted direct information channels for vulnerable groups, and rapid contextual rebuttals to disinformation.

Legal and Normative Framing (Lawfare). Legal and normative tools are applied strategically to legitimise one's own actions while delegitimising adversary's response. This includes selective treaty interpretations, international complaints, publicised legal opinions, and the use of legal proceedings to reshape diplomatic space. Defensive measures involve proactive development of legal briefs,

anticipatory engagement in international fora, and dedicated legal-diplomatic teams to rapidly rebut spurious claims.

United Front and Covert Influence. Networked and often deniable activity leverages diaspora groups, business elites, cultural organisations, and covert operatives to propagate narratives and influence decision-makers from within.[56] Techniques include cultivating and funding local actors, orchestrating advocacy campaigns, and providing covert assistance to sympathetic voices.[57] Defences combine activities such as funding or affiliation disclosures, targeted outreach to strengthen community resilience, vigilance in civil-society partnerships, and law-enforcement preparedness against covert interference.

Taxonomy of Cognitive Operations Adversary Analysis. Every cognitive campaign starts with mapping an opponent's mental and social weak points—beliefs, institutions, media habits, elite networks, and cultural fault lines. This is done through social listening, network analysis, audience segmentation, Open-Source Intelligence (OSINT) mapping, and red-team probes. Warning signs of targeting include sudden narrative surges, coordinated fake accounts, elite splits, and declining trust in institutions. Defence requires strengthening key communicators, running regular vulnerability audits, pre-bunking hostile narratives, and building resilience among at-risk groups.

Figure 6: Monitoring the Cognitive Battlefield: Adversary Analysis

Source: Created by Authors

Narrative Engineering. This represents the active phase of cognitive operations in which tailored stories, frames, and visual assets are designed, tested, and sequenced to shift beliefs or sow division. Techniques range from A/B-tested messaging and influencer seeding to 'Borrowed Boat' amplification, platform micro-targeting, and coordinated timing across multiple outlets. Indicators include sudden framing consistency across diverse sources, influencer surges, and synchronised bursts around key events. Counters include AI-assisted narrative tracking, deployment of trusted local messengers, platform cooperation for removal or labelling, and pre-crafted strategic communication playbooks.

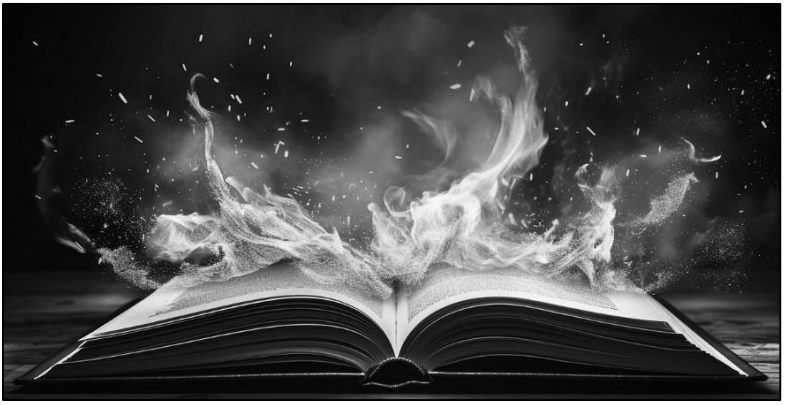


Figure 7: Narrative Engineering: Crafting Power Through Stories

Source: Created by Authors

Erasure and Replacement. PLA theorist Zeng Huafeng's concept of 'Erasure and Replacement' describes a deliberate cognitive strategy that first weakens a society's historical memory and cultural anchors, and then fills the resulting void with the CPC-aligned narratives. Zeng identified four tactics to win 'Mind Superiority' in the cognitive space: 'Perception Manipulation' through propaganda narratives; 'Cutting off historical memory' so that targets will be open to new values; 'Changing the paradigm of thinking' by targeting elites to change their ideology; and 'Deconstructing Symbols' to challenge national identity.[58] For Zeng, cognitive warfare is the ultimate form of winning without fighting.

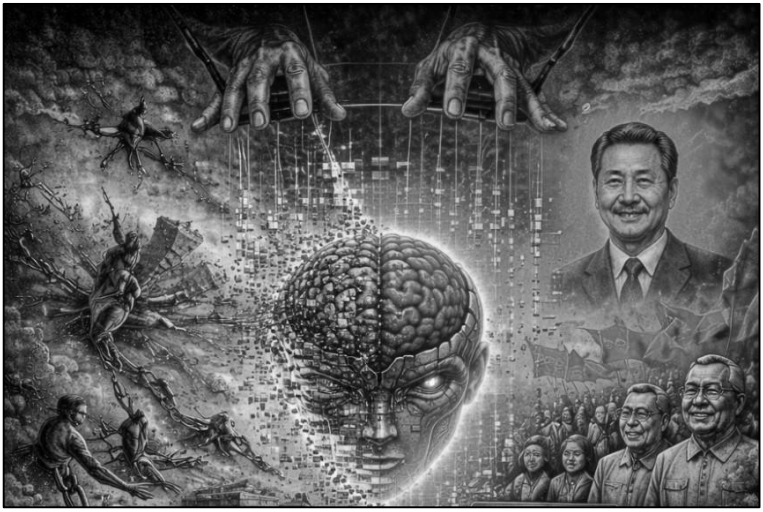


Figure 8: Erasure and Replacement: Rewriting Minds and Memories

Source: Created by Authors

Execution of Cognitive Warfare

Preparation Phase. Actors conduct audience reconnaissance, segment target populations, and seed initial narratives through carefully chosen channels. Activities include social-listening and OSINT to map attitudes and influence networks; cultivation of influencers and borrowed boats (friendly media, think-tanks); creation of message architecture and A/B testing of variants; and technical setup (botnets, troll farms, micro-targeting lists). This phase establishes footholds and baseline credibility so that later operations can scale up rapidly.

Engagement Phase. During crises, elections, or geopolitical flashpoints, the campaign switches to synchronised, multi-vector engagement: coordinated

state media releases, proxy op-eds, targeted social-media pushes, legal claims (lawfare) and diplomatic messaging are timed to amplify chosen frames. Civil-military assets (cyber, EW, SIGINT) may be used to shape the information environment, while United Front and commercial conduits provide plausible non-state reinforcement. The objective is rapid narrative dominance at moments when audiences are most receptive or most uncertain.

Saturation Phase. The operator floods the information ecosystem with volume, velocity, and repetition—the 'Firehose of Falsehoods'.[59] Automated amplification, deepfakes, coordinated bot or troll bursts and repeated framing across multiple outlets to overwhelm verification channels, degrade signal-to-noise ratios, and impose cognitive load on fact-checkers and decision-makers. Saturation creates ambiguity and attribution friction, making it difficult for defenders to mount timely, authoritative rebuttals.

Normalisation Phase. Over time, repeated framing, coupled with curricular and cultural initiatives, lawfare, and economic levers, converts tactical gains into durable interpretive territory. Adversary confidence erodes, contested facts become routinised, and the operator's narratives achieve partial acceptance or, at times, resigned acquiescence. This phase institutionalises advantage—through media ecosystems, education, legal precedents, and diasporic networks—so that

strategic outcomes are realised with reduced need for kinetic coercion.

Desired Outcomes

Strategic Level. At the strategic tier, the desired outcome is to reshape the international security architecture by weakening collective responses to coercion. Campaigns aim to drive wedges between partners (erode burden-sharing, create bilateral frictions), seed doubts about the credibility or political will of external guarantors (notably the United States), and simultaneously normalise China's policies through a long-term narrative of benign development and mutual benefit. Success is judged by measurable shifts in partner rhetoric, reduced coalition interoperability or political willingness to escalate, and wider diplomatic or economic accommodations that expand China's freedom of action without direct confrontation.

Operational Level. At the operational level, the goal is to create time-and-space advantages by degrading an adversary's ability to respond coherently in crises. Effects sought include slowed or confused national decision cycles (delays in mobilisation or coalition coordination), politically costly internal debates that constrain military options, and intensified social cleavages that consume national attention and legitimacy. Operational success is indicated by delayed or diluted policy responses, visible political infighting at key decision points, and measurable

declines in public support for robust counter-measures.

Tactical Level. Tactically, the aim is immediate influence on behaviour in the identified theatre: lower unit morale, foment protests or public campaigns that exert pressure on military and political leaders, and undermine confidence in command communications and logistics. Methods include targeted psyops against frontline units, rapid dissemination of demoralising narratives about supply or leadership failures, and localised lawfare or I/O campaigns that spotlight operational setbacks. Tactical success is evident when units report decreased cohesion, when domestic political pressure forces constrained rules of engagement, or when commander communications lose authority among key audiences.

Chapter 4

Neural Weapons in China's Cognitive Warfare Toolkit

Figure 9: Neural Weapons and Cognitive Influence in China's Strategic Toolkit
Source: Created by Authors

Neural weapons in China's cognitive warfare framework refer to a range of emerging technologies and strategies, still largely in research phases, that target human neurobiology and cognitive functions to degrade enemy situational awareness, decision-making, and neurological functions. These efforts integrate neuroscience, AI, and novel weapon systems, and represent a key component of China's 'Intelligentised Warfare' doctrine.

Emerging Neuro-Cognitive Frontiers

Brain Targeting. This refers to efforts—theoretical or experimental—to exploit insights from neuroscience about how cognition, emotion, and attention are formed and shifted.[60] In a cognitive-warfare context, it

means using psychological, informational, and biomedical knowledge to design messages, stimuli, or environments that preferentially influence particular cognitive states (fear, distrust, apathy) in targeted audiences. The ethical and legal risks are substantial: deliberate manipulation of mental states raises human rights, medical-ethics, and international-humanitarian concerns. Defence focuses on public-health monitoring, clinical forensic capability to detect unusual patterns of neuropsychological harm, media-literacy and resilience programs, and strict research oversight to prevent weaponisation of neuroscience.

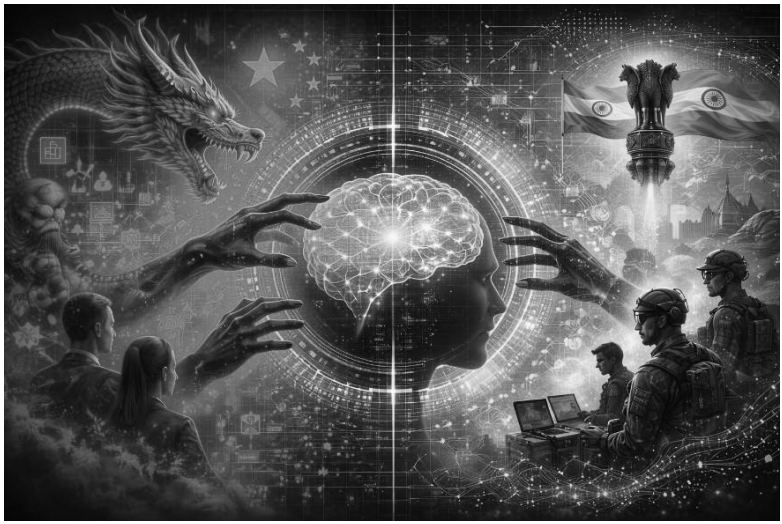


Figure 10: Brain Targeting: The Cognitive Battlefield of Strategic Competition
Source: Created by Authors

Directed Energy. Recent open-source analysis suggests that PLA and affiliated Chinese defence-research establishments are actively pursuing high-

power directed-energy weapons—especially microwave and electromagnetic systems—that could be used not only to disable electronics but also, potentially, to affect human neurological functions. High-Power Microwave (HPM) development in China is closely linked to its evolving doctrine of 'Cyber-Electromagnetic Space' warfare. The PLA's emphasis on informatized warfare highlights HPM weapons as a bridge between kinetic and non-kinetic operations, targeting adversaries' command, control, and communication infrastructure.[61] Reports as recent as 2024 describe new microwave-weapon systems (e.g., mobile-platform high-power microwave systems) designed for counter-drone and air-defence roles, indicating rapid technological progress in this field.[62] Some analysts argue that these capabilities could be extended or adapted toward 'Cognitive' or 'Brain-impact' operations—a form of non-kinetic, non-lethal warfare intended to impair enemy decision-making, morale, or perception without visible physical injury.[63] If realised, such weapons would represent a serious expansion of the PLA's psychological and information warfare toolkit, blurring the line between technical systems targeting infrastructure and systems targeting the human mind.

Figure 11: Directed Energy Weapons: The Next Frontier of Strategic Warfare
Source: Created by Authors

Cognitive Overload. Cognitive overload is a non-kinetic technique that relies on scale, speed, and complexity of information to overwhelm attention and decision loops—flooding channels so that human operators and institutions cannot parse reliable signals.[64] This is readily achievable via existing social media, rapid messaging, synchronised I/O and automated content amplification; it is, therefore, arguably the most immediate and available 'Neural' lever. Mitigations are practical: resilient information architectures, prioritised channels for authoritative signals, training to manage overload, automated filtering and verified rapid-rebuttal systems, and organisational procedures that slow decision cycles when inputs are unreliable.

Brain–Computer Interfaces (BCI): Societal and Surveillance Concerns. BCI technologies promise therapeutic and human-machine advantages but also raise surveillance and autonomy concerns if misapplied. In a hostile context, the worry is less about direct mind-control (which remains speculative and highly constrained) and more about privacy, coercive data collection, and misuse of neural data for profiling or targeted influence. Policy responses should emphasise data protection, consent regimes, export controls on dual-use neurotech, and standards that prevent covert collection of neural signals for influence or targeting. Ethical review and commercial transparency are essential.

Figure 12: Brain–Computer Interface: Connecting the Human Mind to Digital Systems

Source: Created by Authors

How These Elements Function as a Toolkit

China's emerging neuro-cognitive toolkit integrates four mutually reinforcing vectors—brain-targeted psychological manipulation, directed-energy anxieties, cognitive overload, and BCI-enabled surveillance—to influence perceptions and disrupt decision-making in ways far more sophisticated than traditional information operations. Brain targeting provides the behavioural blueprint for shaping emotions and attention; directed-energy narratives create fear, uncertainty, and psychological pressure; cognitive overload overwhelms institutional and public bandwidth by saturating information channels; and BCI-linked neuromeric data enables profiling and tailored influence. Together, these elements form a layered system designed to erode morale, distort judgment, fracture social cohesion, and weaken national resilience, allowing China to achieve strategic effects in the cognitive domain without escalating to kinetic confrontation.

Chapter 5

China's Cognitive Operations: Internal and External Scans

Domestic Cognitive Operations

Cognitive Operations (Internal). Cognitive operations (internal) refer to the deliberate use of information, narratives, and psychological techniques within one's own society, institutions, or armed forces to shape perceptions, attitudes, and decision-making in ways that reinforce cohesion, discipline, and alignment with national or organisational objectives.

Figure 13: Internal Cognitive Operations: Consolidating Power through Narrative and Influence

Source: Created by Authors

Narrative Domination and Propaganda. Narrative domination in China fuses aspirational themes, curated history, and tight information control to align public identity with Party objectives[65]: the 'China

Dream' packages national resurgence and personal fulfilment into a broadly patriotic loyalty to the CPC, while sustained patriotic education campaigns (recasting episodes like the 'Century of Humiliation') create a shared historical grievance that legitimises state policy and seeds social cohesion around regime narratives; these efforts are buttressed by pervasive censorship and the Great Firewall, which restricts access to competing viewpoints, channels discourse into approved frames, and thereby prevents rival interpretations from gaining traction domestically or among vulnerable external audiences—together producing a resilient, state-directed information environment that strengthens political legitimacy and shapes both domestic behaviour and external perceptions.

Cognitive Control Mechanisms.

- **Social Credit System**. China's 'Social Credit System' is a decentralised network of local, sectoral, and institutional databases—rather than a unified national 'Trust Score'—designed to track compliance with laws, court orders, contractual obligations, and regulatory requirements. This system (also known as 'China's Ranking System') refers to a diverse network of initiatives aimed at enhancing the amount of trust within the Chinese society. The goal of the social credit system is to make it easier for people and businesses to make fully informed business decisions. A high social

credit score will be an indicator that a party can be trusted in a business context.[66] China's social credit mechanisms create red lists for good conduct and blacklists for serious legal or administrative violations, affecting access to services or opportunities only when linked to documented infractions—without any universal score for all citizens. Although intended to encourage lawful behaviour and improve governance, the system's fragmented structure leads to inconsistent enforcement, opaque criteria, and occasional wrongful listings. These shortcomings raise concerns about fairness, due process, and potential overreach. Effective safeguards—transparent rules, accessible appeals, independent oversight, and unified national standards—are essential to ensure accountability and protect individual rights.

- **AI-Driven Surveillance**. As an extension of China's broader strategy of internal legitimacy and behavioural control, the state's use of sensors, facial and gait-recognition systems, mobile-data fusion, and automated analytics normalises continuous monitoring and enables real-time assessments of population movements, social ties, and anomalous conduct. When embedded into governance, these tools support predictive interventions and subtle 'Nudges' such as heightened scrutiny, invitation to re-education,

or administrative friction—mechanisms that steer individuals toward conforming norms without overt coercion. Policy responses should prioritise strong data-protection regimes, strict limits on automated decision-making in sensitive domains, independent audits of algorithms, and privacy-preserving technical measures such as encryption and data minimisation to safeguard legitimate civic space.

- **Online Thought Guidance**. Closely intertwined with China's broader propaganda system and its extensive censorship architecture, online thought guidance represents the digital arm of state-managed discourse control.[67] Cyber and information units actively curate the boundaries of public debate by seeding preferred themes, amplifying compliant voices, suppressing dissenting content, and manufacturing a sense of consensus through coordinated inauthentic activity. Operating in parallel with propaganda—which floods the information space with approved narratives—and censorship—which removes or downranks competing interpretations—these techniques make selected political positions appear ubiquitous, natural, and uncontested. The combined effect is to marginalise countervailing views, stigmatise alternative perspectives, and channel public discussion

into safe, state-approved frames. Democratic safeguards require strengthened platform transparency, rapid factual rebuttal capabilities, support for independent media ecosystems, and legal protections for free expression calibrated to counter covert influence operations without restricting legitimate debate.

External Cognitive Operations (Regional Scans)

Figure 14: Xinjiang and Tibet
Source: Reuters Photo Archive

Cognitive Operations in Xinjiang and Tibet. China's cognitive operations in Xinjiang and Tibet combine cultural suppression, social re-engineering, psychological coercion, pervasive surveillance and targeted legitimisation to reshape identities and neutralise dissent: language, religion and local traditions are marginalised or replaced to weaken communal memory; compulsory 'Re-education' and administrative controls remake social behaviour and reduce avenues for mobilisation; fear tactics and coerced confessions condition compliance and self-censorship; AI-enabled mass surveillance and

predictive policing monitor and pre-empt perceived risks; and sustained propaganda demonises symbolic opponents to erode alternative sources of authority—together producing durable political control that blends legal, technical, informational, and social instruments.

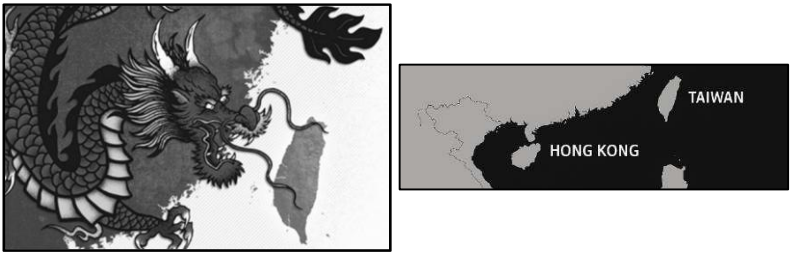


Figure 15*:* Hong Kong and Taiwan
Source: Adapted from editorial graphics used in international media commentary

Cognitive Operations in Hong Kong and Taiwan. Beijing's dominant cognitive play in Hong Kong has been to delegitimise protest movements by framing them as externally driven, violent, and unlawful rather than home-grown political expression. This reframing serves to justify security measures domestically and internationally, reduce sympathy for protesters among undecided publics, and shift the debate from political grievance to law-and-order. The effect is to narrow political space for protest actors and to present state intervention as a defensive necessity. China pursues long-term political influence in Taiwan by cultivating political actors, social networks and opinion leaders who are willing or ambivalent about

closer ties. Engaging parties (or factions within parties), funding or informal support to sympathetic media/non-governmental organisations and promoting narratives favourable to accommodation are all elements of this axis. The intent is to shape Taiwan's domestic balance so that political leadership is less inclined to resist Beijing's preferences.

Figure 16: Pakistan

Source: Adapted from editorial media graphics

Cognitive Operations in Pakistan. In Pakistan, cognitive warfare is advanced primarily through narrative construction and psychological appeal. Beijing leverages the China–Pakistan Economic Corridor media campaigns to frame itself as Pakistan's indispensable economic lifeline, while simultaneously amplifying anti-India narratives across local media and social platforms with the CPC's support. At the psychological level, messaging centred on the 'Iron Brothers' theme fosters a sense of loyalty and cognitive alignment among both the Pakistani elite and the wider public. The overarching

goal is to cement Pakistan as China's strategic partner and reliable information ally in South Asia.

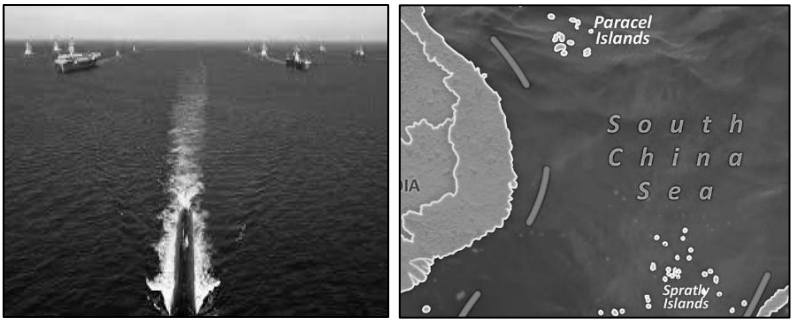


Figure 17: South China Sea
Source: US Department of Defence Photo Archive

Cognitive Operations in the South China Sea. China leverages cultural, digital, and commercial tools to embed its geopolitical claims into everyday life, normalising them through subtle but pervasive channels. Online games like Glorious Mission Online condition players to view aggression as patriotic play; consumer goods and official items routinely display the nine-dash line to entrench territorial entitlement; films and cultural products launder disputed narratives into emotionally resonant global media; and private brands reproduce contested symbols, amplifying state agendas under a veneer of commercial normalcy. Together, these strategies transform maps, stories, and play into instruments of persuasion, lowering cognitive resistance and projecting sovereignty claims as 'Natural'. Defence requires societal and institutional resilience—media

literacy, rapid counter-messaging, cultural diplomacy, and regulatory safeguards—to expose revisionism and promote rules-based alternatives.

Figure 18: Thailand, Myanmar, Malaysia, and Indonesia
Source: Wikimedia

Cognitive Operations in Thailand, Myanmar, Malaysia, and Indonesia. China's cognitive operations in Thailand, Myanmar, Malaysia, and Indonesia follow a common template that blends cultural centres, social media platforms (WeChat, TikTok), cultivation of friendly electoral candidates, support to militant groups, infrastructure investment, and expanding maritime footprints to shape perceptions and policy orientations.[68] In Thailand, the Bangkok–Nong Khai rail link projects China as a regional connectivity hub; in Myanmar, the Kyaukpyu Port and special economic zones provide an economic lifeline while concealing dual-use naval potential; in Malaysia, the East Coast Rail Link is framed as a 'Win–Win' development model; and in Indonesia, the Jakarta–Bandung high-speed rail is showcased as a symbol of shared prosperity. Collectively, these initiatives fuse economic

enticement with strategic signalling, normalising China's presence while embedding influence in the political, cultural, and security ecosystems of Southeast Asia.

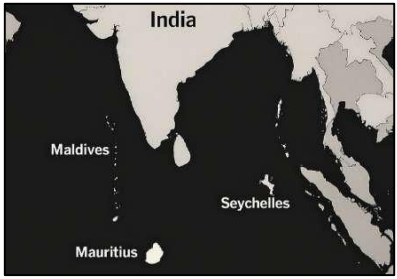


Figure 19: Maldives, Mauritius, and Seychelles
Source: Xinhua News Agency

Cognitive Operations in Maldives, Mauritius, and Seychelles. China's cognitive operations in the Maldives, Mauritius, and Seychelles combine narrative shaping, economic tools, and symbolic solidarity to entrench influence in the Indian Ocean Region. In the Maldives, the 'India Out' campaign and ocean-mapping projects undermine India's primacy while positioning China as a maritime partner.[69] In Mauritius, Beijing leverages infrastructure projects, invokes South–South solidarity, and backs Port Louis' stand on the Chagos Archipelago to frame itself as a principled ally. In Seychelles, China finances government buildings and extends soft loans, embedding its presence in the political economy. Together, these approaches weave strategic geography, financial inducements, and cultural narratives into a long-term effort to legitimise China

as the preferred external stakeholder in small island states.

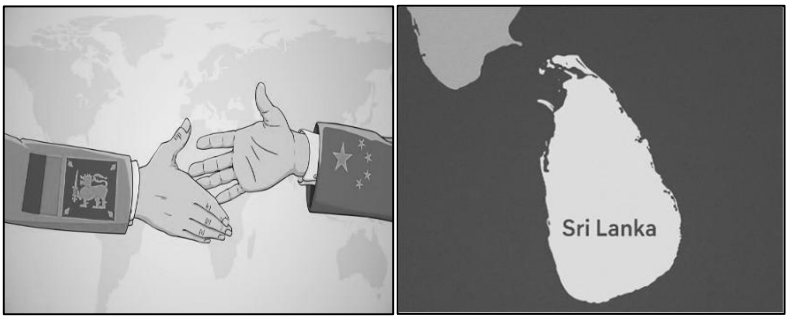


Figure 20: Sri Lanka

Source: Adapted from editorial media graphics

Cognitive Operations in Sri Lanka. China's cognitive operations in Sri Lanka blend education, culture, media, and science to cultivate long-term influence and strategic legitimacy. Collaboration with local universities, promotion of Chinese language, scholarships, and marine science research projects position China as a knowledge partner, while through BRI in Sri Lanka, it frames its role as an educational and consulting benefactor. Simultaneously, funding of think tanks through the China Journalist Forum and activities of the Sri Lanka–China Buddhist Friendship Association, including charity projects, leverage soft-power narratives of cultural affinity and benevolence. Strategic undertones are evident in initiatives like the Xiang Yang Hong six seabed research mission, which masks dual-use potential under the guise of scientific cooperation. Collectively, these instruments

normalise Chinese presence in Sri Lanka's intellectual, cultural, and maritime spheres, reducing resistance and deepening dependency.

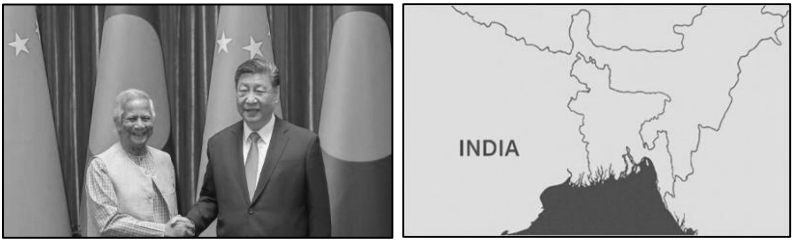


Figure 21: Bangladesh
Source: Reuters

Cognitive Operations in Bangladesh. China's cognitive operations in Bangladesh combine media sponsorship, education, infrastructure, and strategic investments to project benevolence while embedding influence.[70] Funding of state-run Bangladesh Television enables narrative shaping at the national level, while Huawei's donation of tablets preloaded with Bijoy Digital apps positions Chinese technology as an enabler of education. The establishment of a Belt and Road Research Centre at the International University fosters intellectual alignment with Beijing's agenda, while investments in dual-use infrastructure such as ports and airports expand physical and strategic leverage. During COVID-19, China sponsored media portrayals of itself as a 'Saviour', reinforcing gratitude narratives. Together, these initiatives fuse soft power, economic enticement, and strategic signalling to normalise China's role as Bangladesh's indispensable partner.

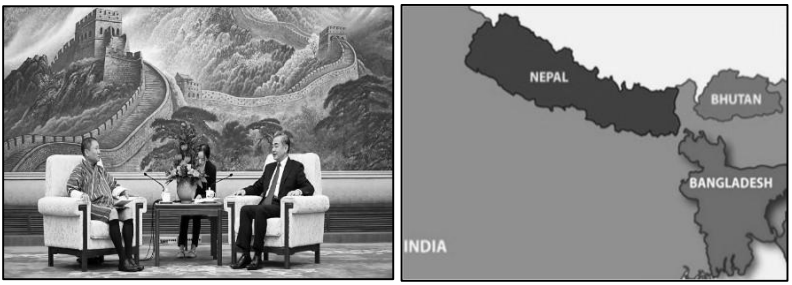


Figure 22: Nepal and Bhutan
Source: Xinhua News Agency

Cognitive Operations in Nepal and Bhutan. China's cognitive operations in Nepal and Bhutan exploit narratives, soft power, and grey-zone tactics to erode Indian influence and advance strategic aims.[71] In Nepal, Beijing fuels the 'India Hegemon' campaign to reshape public sentiment, establishes China Study Centres along the India–Nepal border to cultivate pro-China intellectual ecosystems, and intensifies activities in Eastern Nepal to build presence near sensitive frontier zones. In Bhutan, China combines territorial coercion through grey-zone intrusions with quieter soft-power engagements, while pressing a three-step border resolution plan that reframes negotiations on its terms. Collectively, these approaches weave political influence, cultural penetration, and calibrated coercion to normalise Chinese leverage in two Himalayan states critical to India's security buffer.

India-Centric Cognitive Warfare

Figure 23: Cognitive Warfare in the India–China Strategic Contest

Source: Created by Authors

China's India-centric cognitive warfare represents a sustained, multi-domain campaign aimed at shaping India's perceptions, weakening its narrative autonomy, and subtly conditioning elite, societal, and youth constituencies to accept Beijing's strategic worldviews. This cognitive campaign operates across five principal vectors—education, culture, media, technology, and symbolism—each reinforcing the others to create a long-term ecosystem of influence rather than short-term propaganda.

Educational and Youth Outreach. Beijing invests heavily in cultivating future Indian opinion-makers through exposure, exchange, and indoctrination mechanisms masquerading as educational diplomacy. Sponsored school and university visits to China, Chinese-language institutes, and youth-focused initiatives such as the Mastermind Entrepreneurs Forum and the China–India Youth

Dialogue create an enduring reservoir of individuals predisposed to view China sympathetically.[72] These efforts are reinforced by Confucius Institutes and China Studies Centres, which offer access, funding, and visibility to scholars willing to adopt China-friendly positions under the veneer of academic cooperation.

Cultural and Symbolic Engagement. At the cultural and societal level, China employs symbolic signalling to engage across India's socio-political and intellectual spectrum. Carefully choreographed gestures—ranging from outreach to major socio-cultural organisations and interactions with influential political currents, to engagement with prominent think tanks and academic institutions—serve dual purposes: They humanise Beijing before key domestic constituencies while simultaneously projecting political flexibility and a willingness to engage beyond formal state-to-state channels. Such symbolism allows China to position itself as an interlocutor capable of engaging across India's ideological spectrum, subtly diluting long-standing suspicions.

Media and Narrative Penetration. Chinese influence operations within Indian think tanks, academic forums, and mainstream media are designed to embed pro-China narratives within opinion-shaping ecosystems.[73] Sponsored research grants, editorial fellowships, and partnership-driven events often lead to 'Balanced' perspectives translating into self-censorship or narrative dilution.

By nurturing select analysts and opinion-makers, Beijing gains sustained access to elite discourse, particularly in policy circles sensitive to 'Non-Alignment' rhetoric or economic partnership narratives.

Entertainment and Cultural Industries. China's strategic investments in India's entertainment sector provide another lever of influence. The infusion of Chinese capital—such as Xiaomi's USD 25 mn investment in Hungama[74] and Tencent's USD 115 mn in Gaana[75]—has woven Beijing into the financial fabric of Bollywood and India's digital content industries. These stakes afford indirect control over distribution algorithms and content partnerships, enabling subtle censorship and shaping of public imagery. Cases such as the Rockstar film's edited versions exemplify how economic stakes can translate into cognitive moderation—normalising the erasure of politically sensitive material.

Technological and Cartographic Influence. A subtler dimension of influence appears in the way some China-based digital platforms and device ecosystems display maps according to PRC-defined territorial boundaries. Certain applications—particularly mapping or weather apps configured for the China region—may show Arunachal Pradesh and Aksai Chin as parts of China, reflecting official PRC cartographic standards. While this behaviour is not uniform across all Chinese-manufactured phones or applications and often depends on regional settings

or app-specific data sources, it nevertheless illustrates how territorial narratives can be normalised through everyday digital interfaces. Repeated exposure to such representations can shape user perceptions over time, making digital cartography a subtle vector for reinforcing Beijing's preferred territorial framing.

Figure 24: China–India Border Dispute: Aksai Chin and Arunachal Pradesh in the Himalayan Theatre
Source: Wikimedia

Strategic Convergence and Impact. Collectively, these operations reflect a deliberate fusion of economic penetration, cultural leverage, and narrative manipulation. The overarching objective is to erode India's cognitive resilience—its ability to control its own narratives, maintain epistemic sovereignty, and resist external framing. By colonising attention, infiltrating cultural industries, and subtly rewriting social semantics, China seeks to normalise its preferred frames of coexistence and superiority within Indian consciousness. The danger

lies not in overt propaganda, but in the quiet conditioning that makes Beijing's worldview seem plausible, pragmatic, and inevitable.

Chapter 6

India's Cognitive Warfare Strategy

Mapping China's Cognitive Threats to India's Vulnerabilities

China's increasingly integrated approach to cognitive warfare exposes several structural weaknesses in India's current cyber and information-security framework. Designed primarily for technical response and infrastructure protection, India's architecture struggles to counter Beijing's rapid, centralised, AI-enabled influence operations targeting institutions, public opinion, and decision-making. The gap between China's offensive cognitive capabilities and India's fragmented, often reactive system underscores the need for a more unified, anticipatory, and strategically coordinated national posture.

Existing Architecture

The national cybersecurity architecture is generally structured around three interlinked functions: response, protection, and central coordination.

On the response side, a designated lead authority is responsible for incident detection, real-time response, and coordinated mitigation across government and private sectors. Authority typically flows from the policy ministry through a central response body to Chief Information Security Officers (CISOs) across organisations. This response mechanism operates through an intelligence-fusion and coordination platform and works closely with law enforcement agencies, intelligence entities, sectoral

regulators, and the armed forces. Its primary role is to manage cyber incidents, issue advisories, and ensure timely information-sharing during crises.

On the protection side, a specialised organisation is tasked with safeguarding Critical Information Infrastructure (CII). This includes sectors such as energy, banking, and finance, telecommunications, transport, and other systems essential to national functioning. The emphasis here is on preventive security, risk assessment, standards enforcement, and resilience building, with operational responsibility again cascading to CISOs across critical sectors.

Central coordination is provided by a national security mechanism that ensures strategic oversight, policy coherence, and integration between response and protection functions. A dedicated cyber security coordinator plays a key role in aligning technical, operational, and strategic efforts, while a central coordination centre enables shared situational awareness and threat visibility. Together, this layered architecture integrates technical response, infrastructure protection, and strategic governance to create a resilient national cybersecurity framework.

Existing Vulnerabilities

Fragmentation of Responsibilities. The Indian Computer Emergency Response Team (incident response) and National CII Protection Centre (infrastructure protection) operate in parallel under different ministries or agencies, which can cause silos and slow cross-domain coordination.

Central Coordination Gaps. While the National Cyber Security Coordinator (NSCS) provides oversight, the integration of multiple agencies (law enforcement, intelligence, armed forces, ministries, private sector) remains complex and prone to bureaucratic delays.

Reactive Posture. Much of the current cyber setup is geared towards response and protection, rather than anticipatory and pre-emptive cognitive defence.

Slow Narrative Response. Adversaries (e.g., China) can shape perceptions more quickly than India can respond, undermining deterrence.

Fragmented Messaging. Absence of a unified strategic communication authority means multiple narratives can emerge, diluting credibility.

Dependence on Ad-hoc Countermeasures. Current emphasis on 'Blunting' disinformation lacks systematic pre-bunking or proactive narrative shaping.

Limited Offensive Capacity. India has begun conceptualising 'Spear' (offensive information operations), but lacks mature AI-driven influence platforms, bot networks, or predictive sentiment analysis labs compared to adversaries.

Insufficient Integration of AI or Machine Learning (ML) tools for automated detection, attribution, and counter- influence.

Redundancy Gaps. Critical command-and-control and Intelligence, Surveillance, and Reconnaissance (ISR) systems remain vulnerable to EW, cyberattacks, and deception.

Lack of Specialised Cadre. No dedicated, institutionalised Cognitive Operations Command or cross-domain cadre exists yet; expertise in psychology, semiotics, narrative design, and multilingual influence is underdeveloped.

Training Gaps. Social-media literacy, deepfake recognition, and cognitive resilience are not systematically built into civil services, education, or the armed forces.

Diaspora Engagement. While potentially powerful, India's diaspora influence is not yet strategically coordinated.

Over-reliance on Military or Security Sector. Current posture risks being seen as military-first, whereas adversary campaigns cut across diplomatic, media, economic, and legal fronts.

Weak Public Trust Channels. Disinformation, polarisation, and erosion of institutional credibility can undermine resilience if proactive transparency and trusted communication channels are absent.

Limited Allied Integration. Although Indo-Pacific collaboration is envisaged, India lacks real-time interoperability mechanisms for attribution, disruption, and counterinfluence with partners.

The 5 'S' Model

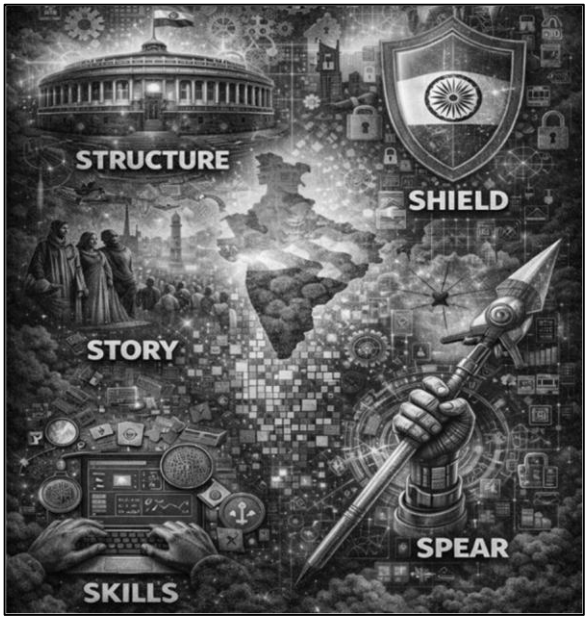


Figure 25: The 5 'S' Model
Source: Created by Authors

India's approach to cognitive warfare can be conceptualised through the five 'S' Model, which provides a structured framework to build resilience and project influence as under:

- **Structure and Doctrine**. They represent the foundational architecture, encompassing institutional mechanisms, inter-agency coordination, and doctrinal clarity to guide national responses in the cognitive domain.

- **Story**. This element emphasises projecting India's plural, resilient, and responsible rise—framing its growth narrative in ways that resonate domestically and globally, thereby creating a positive and authentic counterweight to adversarial propaganda.

- **Shield**. It focuses on defence, involving rapid-response mechanisms, counter-narratives, and information hygiene to blunt disinformation campaigns and hostile influence operations.

- **Spear**. In contrast, this reflects offensive capability—using AI-driven influence operations and data analytics to shape perceptions, seize the initiative, and proactively set the agenda in information ecosystems.

- **Skills**. Finally, this highlights the critical enablers: expertise in semiotics, psychology, and multiple languages, as well as effective leverage of India's vast and diverse diaspora to extend influence.

Together, the five 'S' Model equips India with an integrated strategy that blends defence, offence, narrative control, and human capital to secure cognitive dominance in an increasingly contested information battlespace.

Why India needs a Dedicated Cognitive Warfare Posture

Deterrence in the Cognitive Domain. When Beijing can influence perceptions and shape narratives more quickly than India can respond, the credibility of military deterrence is weakened. To counter this, India must build cognitive deterrence—rapid, credible, and proactive narrative strategies that deny the adversary control over perception and strengthen national resolve.

Resilience Under Denial and Deception. Strengthening cognitive capabilities, including hardened command-and-control systems, redundant ISR assets, and trusted public communication, reduces the impact of adversary EW, cyberattacks, and disinformation campaigns. This resilience is essential to preserve decision-making and public confidence.

Whole-of-government Advantage. Cognitive campaigns cut across diplomacy, economics, media, and law. A purely military approach cannot succeed in this domain. India must therefore integrate defence, diplomacy, strategic communications, and legal instruments into a unified cognitive strategy.

Recommended National Architecture (Organisational Model)

Apex Level. India's cognitive security system can be structured around a National Cognitive Operational Centre (NCOC) led by the National Security Advisor or the Prime Minister's Office to set doctrine, priorities, and risk thresholds.

National Cognitive Resilience. National cognitive resilience is India's capacity to endure and recover from efforts to manipulate public perception, divide society, or distort elite decision-making. It requires building societal immunity to disinformation and psychological pressure, supported by transparent crisis communication, strengthened public trust, and credible institutions—all of which become essential national-security functions. A resilient society makes it far harder for adversaries to trigger panic, polarisation, or strategic paralysis, thereby protecting India's decision-making space during both peace and conflict.

Cognitive Warfare Doctrine. A formal cognitive warfare doctrine provides India with clear definitions, escalation thresholds, responsibilities, and principles for operating in the cognitive domain.[76] Just as cyber or EW doctrines guide technical operations, a cognitive warfare doctrine provides the conceptual basis for both defensive and offensive measures. It must integrate behavioural science, psychology, information operations, cyber tools, and diplomacy

into a unified framework. A clearly defined doctrine also strengthens deterrence by signalling that India views cognitive attacks as strategic threats and is prepared to respond.

Strategic Communication Authority. A national-level Strategic Communication Authority would unify the Government of India's messaging across ministries, security agencies, diplomatic channels, and public communication.[77] This organisation ensures coherence, speed, and accuracy in narrative generation—particularly during crises, external influence campaigns, or moments of national tension. By centralising guidance and content approval, India avoids contradictory narratives, bureaucratic delays, or fragmented public messaging. Such an authority also forms the backbone of proactive narrative shaping, enabling India to set agendas rather than merely respond to adversarial information pressure as under:

- **Strategic Guidance.** Strategic guidance defines India's objectives, threat priorities, and long-term approach to cognitive warfare. It identifies what must be protected, what must be countered, and the global effects India aims to project. This ensures unity of purpose across departments and aligns cognitive efforts with national diplomatic, defence, technological, and internal-security

policies. Strategic guidance serves as the compass that guides operational plans, capability development, and inter-agency coordination.[78]

- **Creation of Multi-Agency Cognitive Ecosystem.** Operationalising cognitive warfare requires an integrated ecosystem linking the NSCS, intelligence organisations, National Technical Research Organisation, Ministry of Information and Broadcasting, Ministry of External Affairs, Ministry of Electronics and Information Technology, cyber coordination bodies, media representatives, Headquarters Integrated Defence Staff, the three Services, and select think tanks with specialised expertise.[79] This ecosystem breaks down silos by enabling real-time information sharing, coordinated response mechanisms, and collaborative narrative design. It ensures that diplomatic, technological, military, and informational inputs feed into a coherent cognitive strategy. Think tanks contribute research, horizon scanning, red teaming, and scenario analysis, strengthening anticipatory decision-making at the national level.[80]

AI-Driven Cognitive Capabilities. To compete in an era of AI-enhanced influence, India must build indigenous capabilities that include automated

content-generation hubs, controlled bot networks for amplification, narrative-simulation engines, and sentiment analysis laboratories.[81] These systems enable India to detect disinformation early, anticipate public reactions, and deliver precise, culturally aligned messaging. Metaverse-based tools can enhance psychological resilience, training, and crisis simulations. Without such capabilities, India risks remaining reactive as adversaries exploit AI-driven influence platforms to shape information ecosystems.

NCOC. The NCOC would serve as India's 24/7 nerve centre for monitoring, detecting, analysing, and countering cognitive threats. It would be supported by a National StratCom Secretariat that designs and coordinates unified government messaging. Day-to-day operations would be carried out by a Cognitive Fusion Centre–India, a continuous multi-agency platform linking intelligence, cyber, diplomatic, defence, and media authorities.[82] To ensure democratic legitimacy, an Independent Oversight Board of retired judges, technologists, and ethicists would monitor authorities, audit actions, and release annual transparency reports. The NCOC would fuse cyber intelligence, social-media analytics, psychological operations, diplomatic cues, and security assessments into a single picture, enabling rapid, unified responses to influence attacks. As India's cognitive-security command post, it would shift the nation from fragmented, reactive measures to a proactive, anticipatory defence model.

Social Media Literacy and Use. It involves equipping government personnel, specialised cadres, and strategic communicators with the skills needed to shape, defend, and rapidly influence the information environment. The information operations to project and protect information include traditional and social media, diplomacy, psychological warfare, cyber warfare, and electronic warfare.[83] Strong regional language and cultural proficiency enhance India's ability to engage its neighbourhood. Rapid-response media teams must be able to deliver accurate, unified messaging within 30 minutes of any trigger event. This should be supported by a specialised cross-domain cadre from the Indian Armed Forces, experienced veterans, and trusted diaspora influencers who can amplify narratives, counter disinformation, and expand India's cognitive presence across global platforms.

Military Domain. In the military domain, India requires a coherent and institutionalised structure to plan, execute, and integrate cognitive operations across all levels of warfare. A Tri-Service Cognitive Operations Command should function as the apex military body for cognitive security, supported by dedicated Cognitive Operations Directorates within each service and theatre cognitive cells aligned to operational commands. These structures must work closely with defence public relations offices and information warfare cells to ensure unified messaging, effective counter-narratives, and real-

time cognitive support to operations. A dedicated Cognitive Warfare Course should train officers in influence strategies, behavioural science, social-media operations, and information-psychological techniques, embedding cognitive warfare in Joint Military operations. Clear career incentives, recognition pathways, and specialist appointments are essential to attract and retain talent, building a professional cadre that strengthens India's cognitive advantage.

Cognitive Warfare Strategy for India

India's cognitive warfare strategy combines information operations, psychological ploys, and technological innovation, leveraging AI and ML to counter disinformation, predict behaviours, and craft targeted messaging. With over 700 million internet users, India's digital ecosystem serves as a key battleground for both defensive and offensive cognitive tactics. India needs to adopt a multi-layered cognitive warfare strategy across military, intelligence, cyber, and societal domains to effectively manage perceptions and counter adversarial influence.

To address cognitive threats, India must integrate strategy, structures, systems, and skills into its military doctrine, adopting a whole-of-nation approach. India must strengthen technological capabilities, information operations, and public-private partnership to counter cognitive threats. Investing in AI-driven analytics, cyber forensics, and ML will help detect and neutralise adversarial

narratives. Enhancing strategic communication, counterintelligence operations, and counter-propaganda will reinforce national security, while leveraging cultural diplomacy and digital literacy initiatives will bolster resilience against misinformation.

Purpose (Strategic Aim). To preserve India's strategic autonomy and decision-space by denying adversary attempts to shape India's public discourse, elite decision calculus, and coalition durability; to protect societal cohesion and military effectiveness; and—where necessary and lawful—to generate cognitive effects that deter or degrade hostile influence campaigns.

Strategic Objectives. India's strategic objectives in the cognitive domain can be articulated through five core pillars, each addressing a critical aspect of defence, resilience, and influence:

- **Deny**. Prevent early territorial anchoring of hostile narratives across domestic and regional information ecosystems.
- **Detect and Attribute**. Rapidly detect, forensically attribute, and expose coordinated influence campaigns (digital and covert).
- **Deter**. Impose legal, diplomatic, economic, and reputational costs for malign cognitive operations.

- **Resilient Influence**. Build and sustain India's own legitimate narrative capacity—culturally credible, evidence-based, and internationally resonant.

- **Integrate**. Institutionalise cognitive planning into joint military, diplomatic and whole-of-government processes.

Strategic Principles. India's cognitive warfare posture is anchored in a set of strategic principles that guide its response and resilience, namely:

- **Whole-of-State Response**. Cognitive effects are generated and countered by an integrated civil-military approach, not by military action alone.

- **Speed and Pre-emption**. The tempo of rebuttal and pre-bunking must match or exceed adversary foothold timelines.

- **Proportionality and Legality**. Responses must adhere to domestic law, international law, and democratic safeguards.

- **Transparency and Resilience**. Invest in public-facing, trusted channels, and media literacy to immunise populations.

- **Adaptive Red-teaming**. Continuously stress-test narratives, platforms, and technical vectors.

India needs more than military readiness; it requires a strategic communication plan that integrates law, policy, and narrative discipline. This includes:

- Institutional counter-disinformation mechanisms that trace and expose narrative sabotage.
- Digital hygiene education that trains citizens to recognise ideological manipulation.
- Legal deterrence against agenda-driven misinformation that seeks to divide India internally while benefiting external actors.[84]

Conclusion

Figure 26: Cognitive Warfare: The Battle for the Human Mind in Strategic Competition

Source: Created by Authors

Cognitive warfare marks a fundamental shift in the character of conflict, where the decisive battlespace is no longer physical but psychological—the struggle to shape perception, belief, and will. China's systematic pursuit of interpretive dominance through propaganda, cyber intrusions, legal narratives, and long-term cultural influence represents a calibrated grey-zone strategy designed to weaken adversaries without open confrontation. Rooted in its Three Warfares doctrine, Beijing's model fuses philosophy, technology, and propaganda into an integrated system of influence that erodes cohesion, paralyses decision-making, and normalises its strategic ambitions. Its strength lies in speed, persistence, and

integration—combining multiple levers of statecraft to achieve psychological and political effects at scale.

For India, the challenge is both immediate and existential: to defend against persistent cognitive intrusion while simultaneously developing the capacity to project credible and resilient influence. The response cannot be piecemeal or reactive; it must be holistic, integrating civil, military, and societal instruments into a whole-of-nation cognitive security architecture. The proposed structures—the National Cognitive Security Council, Strategic Communications Secretariat, Cognitive Fusion Centre, and a Tri-Service Cognitive Command—can institutionalise preparedness, attribution, and narrative dominance. Together with state-level resilience cells, academic partnerships, and international coordination, they form a layered, agile, and accountable ecosystem to protect and strengthen India's infosphere.

The contest between China and India in the cognitive domain will not be decided by technology or doctrine alone, but by credibility and cohesion. China's strength lies in control; India's lies in openness, diversity, and democratic legitimacy. If India invests in societal resilience, empowers trusted voices, and aligns state and civil capabilities around a unified yet plural narrative, it can transform vulnerability into strategic strength. In doing so, India will not only resist adversarial influence but also emerge as a responsible cognitive power in the Indo-

Pacific and beyond—securing decision advantage in an era where the battlefield is the mind, and victory is measured in trust.

Endnotes

[1] Philip R. Fortuno, "Cognitive Domain: A Neoteric Space for Warfare", *Phillippine Army*, 13 Sep 2023, accessed 26 Nov 2025, https://www.army.mil.ph/atr/index.php/component/content/article/ 20-cognitive-domain-a-neoteric-space-for-warfare?catid=13&Itemid=101

[2] "Introduction", in Sun Tzu, *The Art of War*, translated by Samuel B Griffith, (London: Oxford University Press), 1963.

[3] Ibid.

[4] Chapter I, "Laying Plans", in Sun Tzu, *The Art of War,* translated by Griffith.

[5] Ibid.

[6] Book Summaries, "The Art of War Summary", *James Clear*, accessed 26 Nov 2025, https://jamesclear.com/book-summaries/the-art-of-war

[7] Ibid.

[8] "10 Essential The Art of War Lessons", *Asymmetric*, 01 Oct 2024, accessed 26 Nov 2025, https://asymmetric.pro/10-essential-the-art-of- war-lessons-you-need-to-know/

[9] Quyet Thi Nguyen, Lan Thi Pham, and Nam Van Lai ,"Confucius's political philosophy of governing the country: Historical and contemporary considerations", *Slovenská Vzdelávacia a Obstarávacia*, Jun 2023, accessed 26 Nov 2025, https://xlinguae.eu/files/XLinguae3_2023_1.pdf

[10] Confucius, *The Analects*, trans. Edward Slingerland (Indianapolis: Hackett Publishing), 2003, https://hackettpublishing.com/analects

[11] Ibid.

[12] Mateo Martínez Zubillaga, "Confucianism and International Relations", *University of Navarra,* Sep 2025, accessed 26 Nov 2025,https://www.unav.edu/documents/16800098/17755721/confucia nism-in-international-relations.pdf

[13] Shang Yang, *The Book of Lord Shang*, translated by JJL Duyvendak, (Beijing: Foreign Languages Press), 2017; Han Fei, *Han Feizi: Basic Writings*. trans. Burton Watson, (New York: Columbia University Press), 2003.

[14] Han Fei, *Han Feizi: Basic Writings*, translated by Burton Watson, (New York: Columbia University Press), 2003.

[15] Yuri Pines, "Legalism in Chinese Philosophy", *Stanford Encyclopedia of Philosophy*, 10 Dec 2014, accessed 25 Dec 2025, https://plato.stanford.edu/entries/chinese-legalism/

[16] Han Fei, *Han Feizi*, trans. Burton Watson, (New York: Columbia University Press), 2003.

[17] Mark Edward Lewis, *The Early Chinese Empires: Qin and Han* (Harvard University Press), 2007.

[18] Kerry Brown, "Confucianism, Legalism, and Chinese Political Culture", *Chatham House*, 01 Mar 2017, accessed 25 Dec 2025, https://www.chathamhouse.org/publications/papers/chinas-political- traditions

[19] Shang Yang, *The Book of Lord Shang;* Han Fei, *Han Feizi: Basic Writings*.

[20] Harro von Senger, *The Book of Stratagems: Tactics for Triumph and Survival,*
(New York: Penguin Books), 1991.

[21] Ralph D Sawyer, *The Tao of Deception: Unorthodox Warfare in Historic and Modern China,* (Boulder: Westview Press), 2007

[22] "Journal of Chinese Military History", *Brill,* accessed 14 Jan 2026, https://brill.com/view/journals/jcmh/jcmh-overview.xml

[23] Kerry Brown, *China's World: What Does China Want?* (London: I.B. Tauris), 2017.

[24] Elena Barabantseva, "China's Legalist Tradition and Modern Statecraft", *Routledge*, 29 Jul 2010, accessed 14 Jan 2026.

[25] Mao Zedong, *Selected Works of Mao Tse-tung*, Vol. II, *Marxists* (Beijing: Foreign Languages Press), 1965, accessed 14 Jan 2026, https://www.marxists.org/reference/archive/mao/selected-works/volume-2/

[26] Mao Zedong, "On Protracted War", in *Selected Works*, Vol. II, *Marxists,* (Beijing: Foreign Languages Press), 1965, accessed 14 Jan 2026, https://www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_09.htm

[27] David Shambaugh, *China's Communist Party: Atrophy and Adaptation* (Berkeley: University of California Press), 2008.

[28] Andrew Scobell, Edmund J. Burke, Cortez A. Cooper III, and et al.,"China's Grand Strategy Trends, Trajectories, and Long-Term Competition", *RAND,* 24 Jul 2024, accessed 14 Jan 2026, https://www.rand.org/pubs/research_reports/RR2798.html

[29] Dean Cheng, "Winning Without Fighting: Chinese Legal Warfare", *The Heritage Foundation*, 21 May 2012, accessed 14 Jan 2026 https://www.heritage.org/asia/report/winning-without-fighting- chinese-legal-warfare

[30] Elsa B Kania, "The Chinese Military Reforms and Transforms in the "New Era", *Jamestown Foundation,* 14 Aug 2019, accessed 14 Jan 2026, https://jamestown.org/the-chinese-military-reforms-and- transformations-in-the-new-era/

[31] David Shambaugh, *Modernizing China's Military: Progress, Problems, and Prospects* (University of California Press), 2002.

[32] David Shambaugh, *Modernizing China's Military: Progress, Problems, and Prospects* (University of California Press), 2002.

[33] Yao-yuan Yeh, "The Strategic Deployments of China's Cognitive Warfare Under Xi Jinping", *Taiwan Strategists*, 21 Dec 2021, accessed 14 Jan 2026, https://www.pf.org.tw/wSite/public/Attachment/003/f1646809 67179 1.pdf

[34] Nathan Beauchamp-Mustafaga, “Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations”, *The Jamestown Foundation*, 06 Sep 2019, accessed 14 Jan 2026, https://jamestown.org/program/cognitive-domain-operations-the-plas- new-holistic-concept-for-influence-operations/

[35] Meia Nouwens, “China’s New Information Support Force”, *International Institute for Strategic Studies*, 03 May 2024, accessed 14 Jan 2026, https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/

[36] Bruce R. Orvis, Craig A. Bond, Daniel Schwam, et al.,“Resources Required to Meet the U.S. Army Reserve's Enlisted Recruiting Requirements Under Alternative Recruiting Goals, Conditions, and Eligibility Policies”, *RAND,* 14 Jul 2022, accessed 14 Jan 2026, https://www.rand.org/pubs/research_reports/RRA1304-1.html

[37] Frank Hoffman, “Assessing ‘Cognitive Warfare”, *Small Wars Journal*, 14 Nov 2025, accessed 14 Jan 2026, https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/

[38]Rohit Ram, “The Chinese Approach to Strategic Thought Through the Game of Wei Qi” *The World Mind*, 29 Nov 2019, accessed 14 Jan 2026, https://www.theworldmind.org/deepdive-archive/2019/11/29/the-chinese-approach-to-strategic-thought- through-the-game-of-wei-qi

[39] Abhijit Singh, “China’s ‘Three Warfares’ and India”, *Manohar Parrikar Institute for Defence Studies and Analyses*,13 Oct 2013, accessed 14 Jan 2026, https://idsa.in/system/files/jds_7_4_AbhijitSingh.pdf

[40] Libby Lange, “Decoding China’s AI-Powered ‘Algorithmic Cognitive Warfare’”, *Special Competitive Studies Project,* 21 Nov 2024, accessed 14 Jan 2026, https://www.scsp.ai/wp-content/uploads/2024/11/Decoding- Chinas-AI-Powered-%E2%80%98Algorithmic-Cognitive-Warfare- Final.pdf

[41] SIA Naqvi, "China's Global Civilization Initiative: A Backing for BRI in a Divided World?", *Modern Diplomacy*, 22 Oct 2024, accessed 14 Jan 2026, https://moderndiplomacy.eu/2024/10/22/chinas-global- civilization-initiative-a-backing-for-bri-in-a-divided-world/

[42] "Decoding China's AI-Powered 'Algorithmic Cognitive Warfare", *Special Competitive Studies Project* 21 Nov 2021, accessed 14 Jan 2026, https://www.scsp.ai/wp-content/uploads/2024/11/Decoding-Chinas- AI-Powered-%E2%80%98Algorithmic-Cognitive-Warfare-Final.pdf

[43] Abhishek Kumar Darbey, "China and Cognitive Warfare: An Overview", *Manohar Parrikar Institute for Defence Studies and Analyses*, 27 Sept 2024, accessed 14 Jan 2026, https://www.idsa.in/publisher/issuebrief/china-and-cognitive-warfare- an-overview

[44] Hung, Tzu-Chieh, and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti- Disinformation Wars", *Oxford Academic,* 19 Jul 2022, accessed 14 Jan 2026, https://doi.org/10.1093/jogss/ogac016

[45] "The essence of cognitive warfare: Focusing the lens toward Chinese strategies", *Observer Research Foundation Expert Speak*, 8 Apr 2024, accessed 14 Jan 2026, https://www.orfonline.org/expert-speak/the-essence-of-cognitive-warfare-focusing-the-lens-toward-chinese-strategies/

[46] Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations", *Jamestown,* 06 Sept 2019, accessed 14 Jan 2026, https://www.jamestown.org/program/cognitive-domain-operations- the-plas-new-holistic-concept-for-influence-operations/

[47] Abhishek Kumar Darbey, "China and Cognitive Warfare: An Overview", *Manohar Parrikar Institute for Defence Studies and Analyses*, 27 Sept 2024, accessed 14 Jan 2026, https://www.idsa.in/publisher/issuebrief/china-and-cognitive-warfare-an-overview

[48] "Cognitive Warfare: Strengthening and Defending the Mind", *NATO's Strategic Warfare Development Command,* 05 Apr 2023, accessed 14 Jan 2026, https://www.act.nato.int/article/cognitive-warfare-strengthening-and- defending-the-mind/

[49] Glenn Tiffert, "China's Global Media Influence and Borrowed Boat Strategy", *U.S.–China Economic and Security Review Commission,* 21 Mar 2023, accessed 14 Jan 2026, https://www.uscc.gov/sites/default/files/2023-03/Glenn_Tiffert_Testimony.pdf

[50] Christoph Deppe and Gary S. Schaal, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Approach", *Frontiers,* 01 Nov 2024, accessed 14 Jan 2026, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full

[51] Major Joseph D Levin, JD "Lessons on Public-Facing Information Operations", US Army University Press, accessed 14 Jan 2026, https://www.armyupress.army.mil/Journals/Military-Review/English- Edition-Archives/March-April-2025/Information-Operations/

[52] Su Yung-yao and Jonathan Chin, "China uses AI as cognitive warfare tool, official says", *Taipei Times*, 24 Sept 2025, accessed 14 Jan 2026, https://www.taipeitimes.com/News/taiwan/archives/2025/09/24/200 3844335

[53] Emilio Iasiello, "Cognitive Warfare in Cyberspace: A Brief Look at China, Russia, and the United States", *OODA Loop*, 17 Sept 2025, accessed 14 Jan 2026, https://www.oodaloop.com/analysis/decision-intelligence/cognitive-warfare-in-cyberspace-a-brief-look-at-china- russia-and-the-united-states/

[54] Berk Büyükarslan, "The AI War Machine: Chinese State-Conscious Cybernetics and the Evolution of Military Intelligence", *Finabel*, 19 Mar 2025, accessed 14 Jan 2026, https://finabel.org/the-ai-war-machine- chinese-state-conscious-cybernetics-and-the-evolution-of-military-intelligence/

[55] Kyaw Jaw Sine Marma, "Cognitive Warfare: The Invisible

Frontline of Global Conflicts", *Modern Diplomacy*, 12 Feb 2025, accessed 14 Jan 2026, https://moderndiplomacy.eu/2025/02/12/cognitive-warfare-the-invisible-frontline-of-global-conflicts/

[56] K Chan and Chris Alden, "The Diaspora: China's United Front Work and Overseas Influence", *Taylor & Francis,* 24 Feb 2023, accessed 14 Jan 2026, https://www.tandfonline.com/doi/full/10.1080/2474736X.2023.21794 09

[57] Ryan Fedasiuk, "How China's United Front System Works Overseas", *Australian Strategic Policy Institute*, 13 Apr 2022, accessed 14 Jan 2026, https://www.aspistrategist.org.au/how-chinas-united-front-system- works-overseas/

[58] Philip R Fortuno*,* "Cognitive Domain: A Neoteric Space for Warfare", *Phillippine Army*, 13 Sep 2023, accessed 14 Jan 2026, https://www.army.mil.ph/atr/index.php/component/content/article/ 20-cognitive-domain-a-neoteric-space-for-warfare?catid=13&Itemid=101

[59] J Baughman, *How China Wins the Cognitive Domain,* (Maxwell Air Force Base, AL: Air University Press), 2023.

[60] Harris A Eyre et al., *From Neuroweapons to 'Neuroshields': Safeguarding Brain Capital for National Security* (Houston: Rice University's Baker Institute for Public Policy), 10 Aug 2023.

[61] Tin Pak and Yu-cheng Chen, "Weaponizing the Electromagnetic Spectrum: The PRC's High-Powered Microwave Warfare Ambitions", *Jamestown*, 9 May 2025, accessed 14 Jan 2026, https://jamestown.org/weaponizing-the-electromagnetic-spectrum-the- prcs-high-powered-microwave-warfare-ambitions/.

[62] Ibid.

[63] Julian Borger, "Microwave weapons: could be behind 'Havana Syndrome', experts warn", *The Guardian*, 02 Jun 2021, accessed 14 Jan 2026, https://www.theguardian.com/science/2021/jun/02/microwave- weapons-havana-syndrome-experts

[64] Emily Weinzheimer, "Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat", *Small Wars Journal*,

16 Sep 2022, accessed 14 Jan 2026, https://smallwarsjournal.com/jrnl/art/neuro- cognitive-warfare-inflicting-strategic-impact-non-kinetic-threat

[65] Iida Masafumi, "China's Chilling Cognitive Warfare Plans", *The Diplomat*, 05 May 2024, accessed 14 Jan 2026, https://thediplomat.com/2024/05/chinas-chilling-cognitive-warfare- plans/

[66] Drew Donnelly, "China Social Credit System Explained – What is it & How Does it Work?", *Remote People,* 14 Feb 2026, accessed 10 Mar 2026, https://remotepeople.com/china-social-credit-system-explained/

[67] Juha A Vuori and Lauri Paltemaa, "Chinese Internet Control over Social Media Discourse", in *The Routledge Handbook of Chinese Discourse Analysis*, ed. Chris Shei (London: Routledge), 2019, accessed 10 Mar 2026, https://www.routledge.com/The-Routledge-Handbook-of-Chinese- Discourse-Analysis/Shei/p/book/9781032401706

[68] Hoang Huy Nguyen Tb, *ASEAN and the Rise of China: Perspective from* Thailand: Walailak University), Apr 2022.

[69] Sumitha Narayanan Kutty, "India–China Rivalry and the Strategic Importance of the Maldives, Mauritius, and Seychelles", in *India–China Maritime Competition: Strategic Implications for Regional Security*, ed. Rajesh Basrur and Sumitha Narayanan Kutty (London and New York: Routledge), 2021, accessed 10 Mar 2026, https://www.taylorfrancis.com/chapters/edit/10.4324/9780429444227
-6/india%E2%80%93china-rivalry-strategic-importance-maldives-mauritius-seychelles-sumitha-narayanan-kutty

[70] "China's Activities and Influence in South and Central Asia", *United States–China Economic and Security Review Commission,* 14

Nov 2022, accessed 10 Mar 2026, https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_3--Chinas_Activities_and_Influence_in_South_and_Central_Asia.pdf?utm_source=chatgpt.com

[71] Jonathan Stromseth, "The Testing Ground: China's Rising Influence in Southeast Asia and Regional Responses", *Brookings Institution*, Nov 2019, accessed 10 Mar 2026, https://www.brookings.edu/wp-content/uploads/2019/11/FP_20191119_china_se_asia_stromseth.pdf

[72] "Foreign Policy Survey 2024: Young India and the China Challenge", *Observer Research Foundation*, 08 Jul 2025, accessed 10 Mar 2026, https://www.orfonline.org/research/foreign-policy-survey-2024-young- india-and-the-china-challenge

[73] "Mapping China's Footprints and Influence Operations in India", *Law and Society Alliance*, 05 Sep 2021, accessed 10 Mar 2026, https://tibet.net/wp-content/uploads/2021/09/MAPPING-CHINESE-FOOTPRINTS-AND-INFLUENCE-OPERATIONS-IN-INDIA2.pdf /

[74] Harichandan Arakali, "Hungama Digital Raises $25 Mln in Funding Led by China's Xiaomi", *Forbes India,* 04 Apr 2016, accessed 10 Mar 2026, https://www.forbesindia.com/article/special/hungama-digital-raises-%2425-mln-in-funding-led-by-chinas-xiaomi/42877/1

[75] "Deals | Following Xiaomi's Hungama Deal, Tencent Led $115M Round in India Gaana", *KrASIA,* 28 Feb 2018, accessed 10 Mar 2026, https://kr-asia.com/following-xiaomis-hungama-deal-tencent-led- 115m-round-in-india-gaana-2?

[76] Divyanshu Jindal, "The War on Conscience", *Observer Research Foundation,* 12 Jul 2021, accessed 10 Mar 2026,

https://www.orfonline.org/expert-speak/the-war-on-conscience/

[77] Soumya Awasthi and Abhishek Sharma, “Rethinking India’s Cyber Readiness in the Age of Information Warfare”, *Observer Research Foundation*, 17 May 2025, accessed 10 Mar 2026, https://www.orfonline.org/expert-speak/rethinking-india-s-cyber- readiness-in-the-age-of-information-warfare

[78] Sukhbir Kaur Minhas, “Cognitive Warfare: Key Aspects”, *Manohar Parrikar Institute for Defence Studies and Analyses*, 18 Aug 2025, accessed 10 Mar 2026, https://www.idsa.in/publisher/issuebrief/cognitive-warfare-key-aspects

[79] Ibid.

[80] Lt Gen (Dr) R S Panwar , “IW Structures for the Indian Armed Forces – Part I”, *Future Wars*, 31 Mar 2020, accessed 10 Mar 2026, https://futurewars.rspanwar.net/iw-structures-for-the-indian-armed- forces-part-i/

[82] Sukhbir Kaur Minhas, “Cognitive Warfare: Key Aspects”, *Manohar Parrikar Institute for Defence Studies and Analyses*, 18 Aug 2025, accessed 10 Mar 2026, https://www.idsa.in/publisher/issuebrief/cognitive-warfare-key-aspects

[83] Divyanshu Jindal, “The War on Conscience”, *Observer Research Foundation,* 12 Jul 2021, accessed 10 Mar 2026, https://www.orfonline.org/expert-speak/the-war-on-conscience/

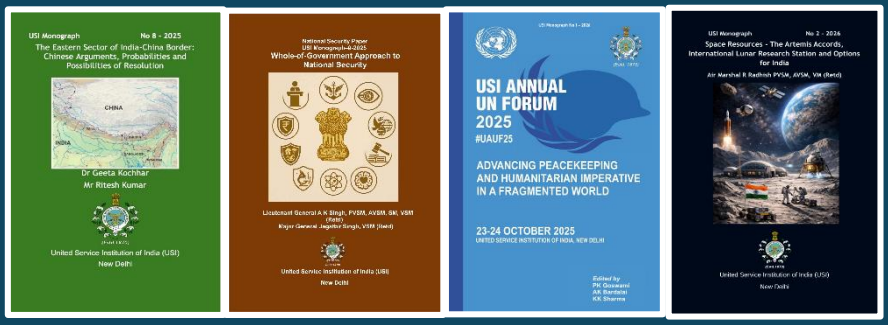
[84] Rohan Giri, “India Needs Cognitive Warfare Plan”, *Centre for Integrated and Holistic Studies*, 10 May 2025, accessed 10 Mar 2026, https://www.cihs.org.in/india-needs-cognitive-warfare-plan/

About the Monograph

Cognitive Warfare by China and India's Response examines the emergence of cognition as the decisive battlespace in 21st Century strategic competition. Cognitive warfare integrates psychology, information, and technology to influence perception, trust, and decision-making—achieving dominance without kinetic conflict. China has institutionalised this approach through its Three Warfare (psychological, public-opinion, and legal) strategy, drawing on classical philosophy, Maoist doctrine, and a modern techno-authoritarian ecosystem that fuses media control, artificial intelligence-driven propaganda, lawfare, and covert influence into a seamless, multi-domain campaign. Its India-centric operations exploit cultural, economic, and digital vectors to erode national cohesion and narrative autonomy while encircling India cognitively through regional partnerships. The monograph analyses China's cognitive warfare architecture—from party-level direction to People's Liberation Army's Strategic Support Force execution—and identifies its integration with cyber, electronic, and psychological operations. In response, it proposes an Indian Cognitive Warfare Doctrine built on democratic legitimacy and resilience, articulated through the Five 'S' Model—structure, story, shield, spear, and skills. Anchored in a whole-of-nation architecture—comprising a National Cognitive Security Council, Cognitive Fusion Centre, and Tri-Service Cognitive Operations Command—the monograph outlines how India can safeguard decision space, strengthen societal resilience, and project credible influence across the Indo-Pacific in a contest where the ultimate battlefield is the human mind.

About the USI

USI was founded in 1870 by a soldier scholar, Colonel (later Major General) Sir Charles MacGregor 'For the furtherance of interest and knowledge in the Art, Science and Literature of National Security in general and Defence Services, in particular'. It commenced publishing its Journal in 1871. The USI also publishes reports of its members and research scholars as books, monographs, and occasional papers (pertaining to security matters). The present Director General is Vice Admiral Sanjay J Singh, SYSM, PYSM, AVSM, NM, PhD (Retd).



Rao Tula Ram Marg, Opposite Signals Enclave, New Delhi-110057

Tele: 2086 2316/ Fax: 2086 2315, E-mail: dircpl@usiofindia.org

₹350