RESEARCH PAPERS

Hold The Fort, India: The Information Battlefield

Author: Mahima Katiyar • **Published:** September 04, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

In an era where wars are fought as much through perception as through force, India's information space remains dangerously exposed. From Pulwama to Operation Sindoor, repeated crises have revealed the consequences of leaving this domain without a fully developed defensive or offensive architecture. The question is no longer whether India's cognitive space will be contested, but whether it is prepared to hold the fort.

1. The Breach

> *3:15 PM. February 14, 2019.*

A bus. A convoy of seventy-eight vehicles carrying more than 2,500 men [1]. A car, waiting, loaded with explosives. The distance between it and them closes in seconds. Forty men are martyred before the nation knows there is anything to mourn. [1]

What happens in the following hours is not one event. It is three separate operations, running in parallel, each exploiting a different vulnerability in the mind of the citizen receiving it.

The first is fast and foreign. JeM claims responsibility for the attack before India has finished confirming its own dead [2]. This isn't misinformation, it's narrative capture: an adversary completing its message before the state completes its facts, so that for a window of hours, the only coherent account of what happened to India belongs to the organization that killed the men. In cognitive warfare terms, this is a contest over who closes the loop first: an entity able to complete the OODA cycle faster than an opponent, gains a decisive strategic advantage over that opponent [8]. India's account arrives late. The adversary's does not wait for permission.

The second is old and recycled, built for confusion rather than conviction. Footage of a 2007 explosion in Iraq is fed to the country as CCTV of the attack site [3]. A car bombing near the Turkish-Syrian border, filmed two days earlier, is fed to the country as Pulwama [3]. Nobody needs to believe these deeply. They only need to be uncertain for long enough, long enough that the mind, faced with contradictory footage from every direction, stops trying to locate the truth and settles instead for picking a side. This is the quieter damage: not persuasion, but exhaustion. A citizen who no longer trusts any single source has not been convinced of a lie. They have been talked out of believing anything at all, which, for an adversary, works almost as well.

The third is domestic, and it is the most successful, because it borrows the credibility India itself built. A photograph, a stranger's face grafted onto a police uniform, is published as the slain mastermind by India Today, and repeated without question by ABP News, Zee News, India TV, Outlook, and The Economic Times [4]. The face beneath the graft belongs to an American musician [4]. This is not an adversary exploiting a gap in India's information space. This is India's own most trusted institutions lending their authority to a lie, and in doing so, manufacturing belief no foreign actor could have manufactured alone. Falsehood consistently travels farther, faster, and deeper than truth online, an effect driven less by who spreads it than by the novelty and emotional charge it carries [9]. A citizen has no reason to doubt five networks agreeing with each other. That doubt is exactly what never gets triggered and that's exactly the point.

Then grief itself becomes a weapon aimed inward. A doctored image places an opposition leader beside the bomber. A manipulated video edits his sister's press appearance to make her seem to laugh while the country honours its martyrs [5]. This is not about Pakistan or JeM, or any adversary abroad. These are India's own political actors turning a national wound into ammunition against each other, in the same hours the dead are still being named. The fort's outer wall was breached by an enemy. Its inner walls were undone from within.

By the fourth day, the CRPF, the institution that lost the forty men in the first place, issues a public advisory pleading with citizens to stop circulating fabricated images of soldiers' bodies "to invoke hatred" [6]. Not the enemy asking to be believed. The state itself, reduced to asking its own people not to believe what their own eyes are showing them.

A fact-checker who lived through a comparable information crisis years later described what this kind of collapse feels like from inside it: a month's worth of disinformation, arriving in the space of a few hours [7]. Not a slow siege. A flood arriving faster than any single sentry could raise the alarm.

No single actor declared war on India's mind that week. It didn't need declaring. Three different operations, one foreign, one confused, one domestic, walked through the same open gate within the same seventy-two hours, and nothing at the gate asked any of them for their papers. What follows in this paper is an attempt to explain why that gate has stayed open ever since.

2. The Ungarrisoned Fort

India did not lose the fort because India never garrisoned it in the first place. A siege implies defenders, manned walls, watched gates, and a command structure deciding when to hold and when to answer. But what unfolded within the first 72 hours after Pulwama was not a siege that we lost. It was an unguarded courtyard into which three separate actors

wandered for three separate reasons because nothing stood at the entrance that could stop them. The adversary that moved first did not have to defeat a defence; it simply arrived in a space that we had left undefended. India suffers cumulative cognitive damage, and it is not from one doctrinal failure but from two, both connected rather than parallel.

The first is defensive. In the hours after a crisis hits, we have no reflexive, pre-positioned system to fill our own citizens' information vacuum with anything credible and fast enough to matter. This is Wall One, and its failure is what allows confusion and manufactured content to take hold domestically: recycled footage passed off as new and live, fabricated identities laundered through trusted networks, and grief converted into political ammunition. None of this requires a sophisticated adversary; an information vacuum and enough time are enough.

The second is offensive. Currently, India has no doctrine, no institutional structure, and no standing will either to seed a narrative into the contested space before an adversary acts or to contest an adversary's narrative internationally once it has one. This is the Second Wall, and its failure is what allows an adversary's claim to remain uncontested in the hours before India's explanation reaches people. It shapes how a crisis is first understood beyond its borders.

These two failures are not separate problems requiring separate fixes; they are interconnected. A state with no offensive doctrine has nothing to draw on when caught flat-footed defensively, because it has never built the institutional muscles, trained personnel, and credible reserves that sustained offensive operations generate over time. At the same time, a state with no defensive resilience cannot sustain any offensive campaign, because its own population arrives at each crisis already fractured, already primed to distrust official channels, and already half-convinced by whatever reached them first the last time. Each failure starves the other of what it needs to exist. We do not have one wall standing and one fallen; we have neither wall standing in the first place.

The main issue is not who fills the vacuum. Tools change, actors change, and language changes. It could be a militant group, a foreign-backed troll network, or a domestic opportunist chasing engagement. The problem is that the gate has remained open for years because India never built a proper system to close it. The five crises mentioned in this paper are therefore not five completely different failures; rather, they are examples of the same basic weakness appearing at different times. It is one absence, standing in the same two places, wearing five different dates.

3. Theoretical Ramparts

Every fort is built on a plan. Before the walls or gates are constructed, there is a ground plan that decides where the walls will go and what they must be built to survive. So what we need is a strategy for handling information and conflict.

The foundation is speed. John Boyd's OODA loop (Observe, Orient, Decide, and Act) describes conflict as a race between two minds trying to complete the same cycle faster than the other [8]. An entity that completes these four steps faster than its opponent does not win by force; it wins by getting inside the opponent's decision cycle. By the time the slower side has finished deciding what happened, the faster side has already decided what happens next. Applied to the information domain, these are the walls of the fort. Whoever completes the loop first controls the terrain before the other side has even finished orienting to the fact that the terrain is being contested. In the Pulwama case, JeM quickly claimed responsibility while India was still confirming the body count. The loop wasn't lost by force; it was lost by tempo.

Another important idea is agenda-setting. If the OODA loop is the wall, the gate is controlled by whoever decides what an event means. Agenda-setting theory, first proposed by McCombs and Shaw, found that the press does not merely tell people what to think, but also what to think about. The issues that dominate coverage become the issues the public treats as important, whether or not that ranking reflects reality [10]. Entman sharpened this into framing theory, positing that to frame is to select some aspects of a perceived reality and make them more salient in such a way that they promote a particular problem definition, causal interpretation, or moral evaluation [11]. In simple terms, the gate does

not just decide who enters but also what the event is called once it does. The side that explains a crisis first can influence whether people see it as an act of terrorism, an act of war, a political issue, or something else. When an adversary successfully frames a crisis before the state does, they are not necessarily lying. They are simply the ones who get to define the terms everyone else, including India's own citizens, will use to argue about it afterwards.

This failure to provide reliable information causes long-term damage that needs its own name, because it is not visible the way a battlefield casualty is visible. In his concept of structural violence, Galtung describes harm that is not inflicted by a direct act but is built into the ordinary operation of a system: violence with no clear origin and no single perpetrator, but rather an arrangement that quietly damages the people living inside it [12]. Extending that logic to the information domain, India's repeated failure to fill its own information vacuum can be understood as a form of narrative structural violence, a slow, cumulative erosion of a population's ability to trust what it is told, inflicted by nobody in particular and everybody in aggregate. The damage may be invisible during any single crisis, but becomes undeniable when the same problem recurs repeatedly.

This siege mentality, this sense of permanent, unrelenting reaction, also has a name. Buzan and Wæver, in their securitization theory, explain that an issue becomes something that needs to be treated as an existential threat because an actor successfully frames it that way to an audience willing to accept it, and not because it objectively is one [13]. Once an event is framed in this way, extraordinary actions that might normally seem unacceptable can begin to appear justified [13]. Therefore, whoever securitizes an event first gets to write the rules that follow by defining it as one. When an adversary securitizes that framing before we do, we are not just late to the story; we are also responding within a set of rules created by someone else, essentially arguing inside a house built by someone else.

And finally, beneath all four of these sits the oldest wall of all: one that nobody built on purpose, or rather one that was built for a country that no longer exists, an older strategic culture. India's non-aligned strategic culture, inherited from the Nehruvian era, followed a policy of restraint, moral suasion, and limited aggressive projection of power. This was appropriate at a time when these were genuinely the right instincts for a newly independent state trying not to be pulled into someone else's Cold War. However, that discomfort did not evaporate even when the threat environment changed significantly. Instead, it calcified into an institutional reflex. So what we have now is a fort whose architect once decided, for defensible reasons, not to build walls on that side, and whose descendants have simply never revisited the blueprint.

4. The Two Undefended Walls

A fort is only strong if all of its walls, including those nobody is watching, are protected.

Wall One is defensive; it is the absence of any reflexive, pre-positioned capacity to fill the golden-hour vacuum for India's own citizens. A standing unit whose only job is to observe a crisis breaking and answer it with something true before anything false has time to set. And Pulwama shows what this absence costs at street level: recycled footage from Iraq and Syria passed off as live, a fabricated mastermind's photograph laundered through five national networks, a doctored video weaponizing a family's grief and none of it stopped, none of it slowed because nothing existed whose function was to stop it. This is not a mere technological failure; its a failure of mandate. Nobody was ever assigned to the wall, so nobody was standing there when the ladder went up.

Wall Two is offensive; it is the lack of a permanent system for presenting its own version of events quickly and challenging an opponent's narrative internationally. This is the wall that let JeM's claim of responsibility stand unchallenged for the hours it took India to issue anything at all, not because we lacked facts but because we lacked the reflex. An offensive doctrine doesn't mean matching an adversary's lies with India's own. It means being the first voice in the room often enough that when a crises breaks, the world's default assumption is to wait and hear what India says

and not what gets said about India.

And the point the rest of the paper will keep returning to is that two walls do not fail independently. Wall One's absence guarantees that Wall Two has nothing behind it and Wall Two's absence guarantees that Wall One never gets reinforced. This is not two forts with two separate problems, it’s one fort, built without a single wall on either side because whoever drew the original plans assume wrongly and for reasons that stopped applying decades ago, that nobody would ever come looking for a way in. Every case study that follows is the same courtyard, the same missing walls, wearing a different date.

5. The Sieges

5.1 Pulwama (2019):

The first section of our paper already reconstructed Pulwama in full. Here it stands as the main example: the offensive wall failing in real time, an adversary’s claim outrunning India’s own confirmation of its martyrs and a domestic information ecosystem with no rapid response mechanism standing between grief and exploitation.

5.2 Galwan (2020): the wall that stayed vague

Indian and Chinese soldiers clashed in the valley in the first deadly confrontation on that border in over four decades [14]. What followed was not a battle over facts so much as a battle over the absence of facts. China did not deny deaths; its initial silence on the figures ran for months and when the number eventually emerged from independent investigation rather than official disclosure, it stood at roughly 38, nearly 10 times the four originally acknowledged by Beijing [15]. India, in turn, offered its own official channels far less than a coherent international narrative required. It left a vacuum shaped less by direct Chinese denial than by ambiguity on both sides. Into that ambiguity, coordinated inauthentic activity moved quickly. A network of roughly 400 to 500 fake social media accounts, later traced to Pakistani origin, spread pro-China narratives and false claims tied to the clash, while Chinese state media pivoted to a defensive register that framed India as the aggressor and China's response as restraint [16]. Manipulated satellite imagery and false claims that China occupying Ladakh and killing more than 86 Indian soldiers circulated as part of a broader influence effort [16]. None of this required India to be wrong; it only required India to be quiet or unclear, for long enough that Beijing’s framing became the default one, repeated by international coverage before New Delhi’s account caught up.

5.3 Manipur (2023): the wall that was never there

On May 3, ethnic violence broke out between Meitei and Kuki-Zo communities, eventually killing over 250 and displacing roughly 60,000 people [17]. National media coverage ignored the crisis for its first two and a half months, taking the story seriously only after a viral video forced it into national attention [17]. This silence was immediately and viciously filled by fabricated content on both sides of the conflict. A photograph purporting to show a Meitei woman who had been raped and killed circulated widely, reported to have incited mob violence, including sexual violence against Kuki civilians; the image was later traced to an unrelated 2022 case in Delhi [18]. A separate viral claim that a Kuki girl had been beaten to death in Manipur was traced to unrelated footage from Myanmar [19]. Survivors featured in the July 2023 video, which showed a mob parading two Kuki women naked and finally brought the story to national attention, told reporters that the assault was explicitly framed by perpetrators as revenge for the earlier, fabricated Meitei rape claim [18]. In this case, misinformation did not merely follow the violence; in some documented cases, it directly caused it.

5.4 COVID origin/vaccine narrative (2020-2022): the wall failing without a border

As China's own international image buckled under scrutiny for its early handling of Wuhan outbreak, Beijing pivoted to an aggressive campaign defending its record and redirecting blame, deploying state-linked social media accounts, embassy channels and party-owned outlets such as the Global Times [20]. India wasn't an incidental target but a specific one. Chinese media ran articles carrying negative narratives about Indian governance, foreign policy and India's own handling of the pandemic, including a Global Times piece falsely claiming Tibetan exiles in India wished to return to China due to inadequate medical care there [16]. Simultaneously and often through the same channels, Beijing ran a parallel charm campaign aimed specifically at Indian public opinion, with Global Times editorials positioning China as the only power capable of helping a country as populous as India, while warning Indian media against what it called attempts to "stigmatise" China over the origin of the virus [21]. India's population was not defenseless against this by instinct; many already distrusted Chinese explanation and polling showed majority blamed China [21]. But this public skepticism wasn't the result of a strong Indian institutional counter-narrative. Nothing in India's official communication apparatus was built to name the campaign as a campaign, to contest Global Times' framing in real time or present our own version of events internationally before Beijing did. So it was the population's instinctive distrust which held the line that Wall One and Wall Two were supposed to hold. So it held, but it held by accident, not by design.

5.5 Op. Sindoor (2025): both walls, simultaneously

Within hours of India launching the operation, Pakistan's ISPR directorate moved from denial to a full counter-narrative campaign [23]. Falsely claimed its air force had shot down five Indian fighter jets, a figure escalated by their own Defence Minister when pressed for evidence by the international media, who could offer nothing more than "it's all over social media" [23]. ISPR-aligned accounts circulated a photo of downed IAF MiG-29 as fresh proof of a kill, an unrelated one-year-old 2024 crash in Rajasthan [24]. Claims that a captured female Indian Air Force pilot had been paraded by Pakistan spread widely before India's PIB debunked it directly, producing the pilot, Squadron Leader Shivangi Singh, alongside President Murmu to prove the claim false. Documentation from Indian MIB attributes the fabricated claims of Indian jet losses, false civilian casualty figures, fake government advisories and doctored videos of Indian officials apologizing or surrendering directly to Pak's coordinated information apparatus [23]. Pak didn't act alone; the campaign was amplified internationally by Turkish state media, including TRT World and Anadolu Agency echoing ISPR's unverified claims without evidence and by Chinese-linked amplification of the same messaging [25]. A retired Indian lieutenant general who led forces during the operation later described the mechanism plainly as by flooding the information space with fabricated narratives, Pak sought to portray itself as the victim of unprovoked aggression, calculated to rally domestic opinion and delegitimize India's response internationally [22].

Wall One was held better here than in any prior case, the MoD ran real-time briefings with strike imagery, government fact-checkers flagged and took down thousands of false accounts and URLs within days [24]. But Wall Two is where the operation exposed India's deeper deficit. Pakistani fabricated narratives still reached Turkish state broadcasters and headlines in outlets with no independent means of verifying any of it [25]. India defended its domestic information space with more competence than at any point in the previous cases. It still had no comparable machinery to contest the story once it left Indian borders. The defensive wall was finally, partially manned. But the offensive one was still empty.

6. Why The Walls Were Never Built

India has a cyberspace doctrine. The Defence Cyber Agency was approved in 2018 alongside a parallel Defence Space Agency, following the recommendations of the Naresh Chandra Task Force's 2012 national security review, and became fully operational with dedicated Cyber Emergency Response Teams across all three services by 2021 [26]. In August 2025, the Ministry of Defence released a Joint Doctrine for Cyberspace Operations, officially acknowledging an

offensive Indian military cyber posture for the first time and explicitly integrating offensive and defensive capability under a single framework [27]. The space agency, by contrast, still operates without a comprehensive national space policy to sit underneath it, even years after its creation: proof that even India's better-resourced domains carry gaps of their own [31]. However, a doctrine does exist, even if partial. Someone in the MoD was assigned to write it, budget it, and defend it before a parliamentary committee.

But no equivalent document exists for the cognitive or information domain. There is no single official doctrine, unified command, dedicated budget or clearly responsible organization, even as adversaries weaponize perception and narrative with increasing precision [28]. India's own Armed Forces literature confirms this gap, while think tanks like MP IDSA have published analysis on cognitive warfare, the GOI and the Armed Forces haven't yet published a single formal doctrine or policy document that explicitly defines the concept for India's own use [29]. If we compare this to the international space in which we are operating: US integrates cognitive operations into information as a joint function with multidomain doctrine; China codifies it explicitly through its "Three Warfares" strategy, folding psychological, media and legal operations into one framework; Russia treats it as a permanent state of information confrontation; Israel names it directly as a "cognitive campaign" central to deterrence; even Pak, facing greater resource constraints than India, frames its approach through a named hybrid and 5^{th} generation warfare doctrine [28]. India does recognize that information operations exist but has never formally decided what to do about them. This is important because a formal doctrine is not just a piece of paper. A named doctrine is what creates a budget line, a command structure with officers whose job depends on the mission succeeding, a training pipeline and critically, a body that can be held accountable when the mission fails. Cyberspace has all four in India. Cognitive domain, however, has none. Analysts examining India's cyber posture note that even where formal structures do exist, they remain constrained by institutional fragmentation and the absence of a unified command, limiting effectiveness even inside the domain that has a doctrine [30]. Extending the same fragmentation into a domain with no doctrine at all and the result is what every case study in section V demonstrated in practice: no single body owns the moment a crisis breaks, so multiple bodies each own a fragment of it and fragments do not move at the speed a fort under siege requires.

We did not fail to defend our cognitive terrain because the problem was unrecognised; we failed because recognition never converted into a doctrine, and without a doctrine, nothing converts into budget, command, training or accountability. The fort's other walls were built because someone at some point was given the authority and the obligation to build them, but on this wall no one ever was.

7. Garrisoning The Fort

Here is the second half of our argument. Every recommendation under this heading repairs one of the two walls named in Section IV. None of them is a checklist item.

7.1 Defensive Infrastructure: Repairing Wall One

- **A Permanent Rapid-Response Unit:** India needs a dedicated, multidisciplinary body whose sole mandate is the golden hour: a standing unit already staffed, already briefed, and already trusted enough to be believed the moment it speaks, so that it can quickly provide accurate information before rumours and fake news spread. Every case study discussed in this paper shares one root cause: nothing existed whose only job was to answer inside that window.

- **A National Pre-bunking Program:** Correcting a lie after it has spread is weaker than inoculating a population before it arrives. Psychological research on inoculation theory has found that briefly exposing people to the structure of manipulation techniques before they encounter the real thing measurably improves their ability to detect and resist it later [32]. This effect has now been tested successfully across misinformation about elections, climate, and public health [32]. We have no equivalent standing program.

- **Media Literacy at Scale:** It should be treated as essential public infrastructure, not a classroom add-on. The Manipur case is the clearest evidence of what this absence costs: a fabricated image, believed without question, credited by survivors themselves as the stated justification for real assault.

- **One Clear Crisis-Communication Leader:** At present, different organisations such as the PIB, MEA, and MoD each handle different parts of a crisis. There is often no single body responsible for coordinating the entire response. Naming one owner ends the condition in which a crisis breaks and no single phone rings first.

7.2 Offensive Doctrine: Repairing Wall Two

- **Formal Designation of the Cognitive Domain as a Warfighting Domain:** We already have a template. Cyberspace received exactly this designation and within years produced a dedicated agency, a declassified doctrine, and an offensive posture [27]. The cognitive domain has none of that, not because India lacks the expertise but because no document has ever formally declared that this is now a domain of war.

- **Strategic Narrative Seeding Capability:** Operation Sindoor showed what this looks like when it works partially: real-time briefings with strike imagery blunted the domestic vacuum. It also showed what partial failure looks like: Pakistan's fabricated narratives still reached Turkish state broadcasters and international headlines, with nothing comparable pushing back from India's side once the story left Indian borders.

- **A Dedicated Career Track and Command Structure:** Like the Defence Cyber Agency for cyberspace, the cognitive domain needs its equivalent: trained personnel, a promotion pathway, and a command structure built specifically for offensive and defensive cognitive operations.

These seven solutions are not independent. A rapid-response unit without a named crisis owner has no authority to act; a pre-bunking program without a designated warfighting domain has no budget to scale. Fix one wall and leave the other standing empty, and the fort remains exactly as undefended as it is today, just from a different direction.

8. The Breach, Revisited

> *3:15 PM, 14 February 2019.*

Let us return to it once more, now that the walls have names.

A convoy of 78 vehicles, a car waiting. Forty of our men gone before the nation knows there is anything to mourn. This part, however, was not a failure in the cognitive-warfare sense, as no doctrine on earth outruns an explosive already in motion.

What comes next is where the doctrine was supposed to live and did not. JeM's claim arrives before our own confirmation of our martyrs, not because the militant group was faster by nature but because nothing on India's side was built to close that loop at all. Wall Two, empty exactly as it would remain empty one year later at Galwan and six years later in Operation Sindoor. The recycled footage moves through the country unchallenged, not because it was convincing but because uncertainty needed no institution to spread it, only the absence of one to stop it. The fabricated mastermind's photograph passes through five national networks because nothing required a single check before broadcast, the same absence that let a false claim in Manipur become, in the survivors' own words, the stated justification for a real one four years later. Wall One, empty, in a straight line from Pulwama to Manipur that needed no adversary to expose it.

Four days on, the CRPF's advisory, pleading with its own citizens not to believe what their own eyes were showing them, now reads as anything but a strange footnote. It is the sound an institution makes when it discovers, in public, that it was never given the tools to do the one thing it needed to do first. None of this was inevitable. Cyberspace, faced with the same kinds of threat, received the required formal system, but the cognitive domain received only analysis, think-tank papers, and seven years of case studies that all say the same thing in different uniforms. The difference between a wall that stands and a wall that does not was never written, and everything that the document would have authorised downstream never came to exist because of it.

The fort is still standing, never fully fallen, not yet. But a fort that has never been breached to the ground is not the same as a fort that has been garrisoned. We have survived a large number of sieges on the strength of what its citizens noticed on their own, what a handful of fact-checkers caught in time, and what an adversary failed to fully capitalise on. That is not defence; that is luck, dressed up often enough to be mistaken for a wall.

So, somewhere right now in a country whose information doctrine still does not exist, a gate stands open that no one has been assigned to close. It has long been open. It is still open.

References:

1. The Times of India, "Jaish Terrorists Attack CRPF Convoy in Kashmir, Kill at Least 38 Personnel," February 15, 2019.

2. Neeta Sharma, "Terrorist Lived 10 km From Site Where He Killed 40 Soldiers In Kashmir," NDTV, February 15, 2019.

3. Scroll.in, "From Old Videos to Doctored Photos, a Barrage of Fake News Floods Social Media After Pulwama Attack," February 18, 2019.

4. Scroll.in, "Facebook's Fact Checkers: Post-Pulwama, Three Out of Seven Partners Have Shared Misinformation," March 19, 2019.

5. Quartz India, "'Never Seen Anything Like This,' Says Facebook India's Fake News Buster After Pulwama Attack," 2019.

6. NewsBytes, "How Not to Fall for #FakeNews in Wake of #PulwamaAttack," February 17, 2019.

7. Uzair Rizvi, quoted in Reuters Institute for the Study of Journalism, "'Truth Is the Casualty': How Indian Fact-Checkers Debunked False Claims During the India-Pakistan Crisis."

8. Brett R. Price, "Colonel John Boyd's Thoughts on Disruption," Marine Corps University Journal of Advanced Military Studies, 2023.

9. Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," Science 359, no. 6380 (2018): 1146–51.

10. Maxwell E. McCombs and Donald L. Shaw, "The Agenda-Setting Function of Mass Media," Public Opinion Quarterly 36, no. 2 (1972): 176–87.

11. Robert M. Entman, "Framing: Toward Clarification of a Fractured Paradigm," Journal of Communication 43, no. 4 (1993): 51–58.

12. Johan Galtung, "Violence, Peace, and Peace Research," Journal of Peace Research 6, no. 3 (1969): 167–91.

13. Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis (Boulder, CO: Lynne Rienner Publishers, 1998).

14. Wikipedia, s.v. "2020–2021 China–India Skirmishes," accessed 2026.

15. Anushka Chatterjee, "Authenticity During Conflict Reporting: The China–India Border Clash in the Indian Press," Journalism Practice, 2024.

16. Freedom House, "India: Beijing's Global Media Influence," 2022 Country Report.

17. Wikipedia, s.v. "2023–2025 Manipur Violence," accessed 2026; Media Diversity Institute, "How Disinformation Sparked the Ethnic Violence in a Remote Area of India," 2023.

18. Fact Crescendo, "Manipur Video: How Fake News Caused Violence Against Women," 2023.

19. Logically Facts, "Viral Manipur Video: How Misinformation Ignites Violence Against Women," 2023.

20. ChinaPower Project, Center for Strategic and International Studies, "Is China Succeeding at Shaping Global Narratives About Covid-19?"; Wikipedia, s.v. "COVID-19 Misinformation by China."

21. The Strategist, Australian Strategic Policy Institute, “China’s Covid-19 Charm Offensive Isn’t Fooling India.”

22. The Geostrata, “Operation Sindoor and the Enduring Contest of Narratives.”

23. CESCUBE, “The Use of Disinformation and Propaganda as a Tool of Foreign Policy by the Pakistani State and Military Apparatus: A Case Study of Operation Sindoor.”

24. Vygr News, “Beware! Fact-Checking Pakistan’s Misinformation Campaign After Operation Sindoor,” citing Press Information Bureau Fact Check.

25. India New England News, “Pakistan’s Disinformation Campaign Exposed After India’s Operation Sindoor.”

26. Wikipedia, s.v. “Defence Cyber Agency,” accessed 2026.

27. Natstrat, “Cyber Deterrence in the Indian Context: Constraints, Credibility and Escalation Risks.”

28. Business Standard, “India Needs to Win the War of Minds Before the First Shot,” Blueprint Defence Magazine, January 2026.

29. C. A. K. Yadav, “Cognitive Warfare: India’s Approach to Influencing Perception and Behaviour,” Journal of the United Service Institution of India, 2026, 167–83.

30. C3S India, “Invisible Battlefields of Cyberspace: India’s Strategic Imperative Amid Chinese Ascendancy.”

31. Observer Research Foundation, “India’s Space Cybersecurity Mesh: Criticality and Call of Purple Revolution.”

32. Stephan Lewandowsky and Sander van der Linden, “Countering Misinformation and Fake News Through Inoculation and Prebunking,” European Review of Social Psychology 32, no. 2 (2021): 348–84.

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

Image Source: ChatGPT