



ISSN 23939729

CLAWS

No. **147**

2026

MANEKSHAW PAPER

Weaponising Social Media: India Exposed in the War of Mind Space

Devendra Pratap Pandey

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam “Bahadur”, was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw’s contributions to the Indian Army are legendary. He was a soldier’s soldier and a General’s General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India’s best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.



**Field Marshal SHFJ Manekshaw, MC
1914-2008**

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

Weaponising Social Media: India Exposed in the War of Mind Space

DEVENDRA PRATAP PANDEY



Centre for Land Warfare Studies
New Delhi



Editorial Team : CLAWS

ISSN : 23939729



Centre for Land Warfare Studies

RPSO Complex, Parade Road, Delhi Cantt, New Delhi | 10010

Phone +91-| 1-| 5691308 Fax: +91-| 1-| 5692347

Email: landwarfare@gmail.com, website: www.claws.co.in

CLAWS Army No.33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

© 2026, Centre for Land Warfare Studies (CLAWS), New Delhi.

Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore may not be quoted or cited as representing the views or policy of Government of India, or the Ministry of Defence (MoD), or the Centre for Land Warfare Studies.

Published in Bharat by



Sabre & Quill Publishers, New Delhi, India

www.sabreandquill.com/sabreandquill@gmail.com

Contents

• Abstract.....	5
• Introduction	5
• From Destroying the Enemy to Shaping the Mind.....	8
• Information Warfare is Older Than Information Technology.....	10
• The First Strategic Use of Information Infrastructure as a Weapon.....	12
• Why the Shift from Information Warfare to Cognitive Warfare is Transformational?.....	17
• Recent Events Illustrate the Potential Consequences.....	19
• Why Social Media has become the New Cognitive Battlespace	21
• The Weaponisation Cycle: From Grievance to Behaviour	27
• India Stands Exposed	30
• Who is Weaponising Social Media?	36
• India: A Particularly Fertile Cognitive Battlespace.....	45
• The Strategic Problem: India Does Not Control the Battlespace	47
• India's Problem in Managing Social Media Space: The Political-Class and Institutional	51
• What Should India Do?.....	56
• Conclusion: From Information Control to the Battle for the Mind.....	63
• References	66

Weaponising Social Media: India Exposed in the War of Mind Space

Abstract

Warfare is moving beyond the traditional physical domains of land, sea, air, space, and cyberspace into the human mind. This paper examines the emergence of “Mind Space” as a new battlespace in which perceptions, beliefs, emotions, behaviour and decision-making can be influenced without the use of kinetic force. It argues that while information and psychological warfare are centuries old, digital connectivity, social media, artificial intelligence, algorithms, deepfakes and behavioural analytics have transformed their scale, speed, precision and reach. Social media has consequently become a powerful instrument for shaping narratives, amplifying grievances, exploiting societal divisions and influencing national will. Using historical and contemporary examples, the paper highlights India’s vulnerabilities and argues for a comprehensive cognitive security architecture capable of protecting the information environment, countering hostile influence and safeguarding the minds and decision-making of its population.

Introduction

For millennia, warfare was fought over territory. Armies fought to capture and hold land. Then came the Navies, seeking control of

the seas. In the last century, Air Forces emerged to dominate the skies, followed by the contest for Space. With the emergence of Cyberspace as a new frontier through which information flows and the command and control of forces, economies, and societies increasingly operate, it too became a domain of contest.

Today, however, warfare is breaching its ultimate frontier, and that is to directly contest for the human mind. The new battlespace is Mind Space, where the contest is to influence perceptions, shape beliefs, alter behaviour, and ultimately affect how individuals, societies and nations think and decide.

While the United States, China and the Big Tech giants have moved far ahead in investing in technologies, platforms and capabilities to influence and potentially control this space, India risks becoming a vast battlespace with little leverage or control of its own. It is a contest so nuanced and pervasive that an adversary can achieve strategic effects without firing a single shot.

A country that accounts for one-sixth of humanity is the third most powerful country in the comprehensive power index, fourth-largest economy, fourth-largest military power,¹ and the world's most populous country, and finds itself with little say in a battle in which the minds of its 1.4 billion people are the target. Even India's adversaries in the region, along with non-state actors inimical to its interests, have recognised the potential of this new battlespace. They have invested heavily in the means to exploit it and, in the process, have already gained ground by influencing minds.

Over the past decade or so, the chinks in India's armour have been exposed repeatedly. As recently as the CJP protests, a few individuals launched a major protest at Jantar Mantar, challenging the Central Government's authority. After the Chief Justice of the Supreme Court of India called them 'cockroaches' on 15 May 2026, the context shifted: a new party, the Cockroach Janata Party,

launched online on 16 May 2026.² It generated millions of followers in no time.

Launched on X (formerly Twitter) on 16 May 2026, the original handle quickly crossed 200,000 followers before being withheld in India.³ A new handle (@Cockroachisback) was subsequently set up, which holds around 392,800 followers. The party launched on Instagram on May 17, 2026, with the account (@cockroachjantaparty) and saw an explosive jump in followers. It jumped from 11 million to 14 million followers within days and has since scaled to over 26 million.

The speed and scale of this phenomenon are a warning in themselves. A completely new political formation built a mass digital following almost instantaneously, forcing the Prime Minister of India to switch to Instagram to engage with students and youth and, according to the events described, forcing the resignation of the Indian Education Minister on Jul 25, 2026. Within two months, a new party had tasted blood. The Indian Government had no clue or answer.

Meta's complicity was evident when its officials accepted payment to manipulate content after being called in for suppressing the content of India's Prime Minister on July 23, 2026.⁴ Whether viewed as a manifestation of organised influence, platform vulnerability, or the sheer power of digitally amplified narratives, the episode demonstrates the extent to which control over the information environment can translate into real-world political effects.

The recent past was not so glorious either. To counter the anti-CAA and NRC movement, the Government of India struggled to sell the positive narrative despite the good intentions and outcomes. The positives of the post-abrogation of Article 370 period, and even the extremely successful management of the

COVID period, remained sluggish in the narratives around their outcomes.

The military success of Operation Sindoor was similarly confronted by a battle that extended well beyond the physical battlefield. The military gains were challenged in the battle of narratives, not only before the world but also within the country, against an exceptionally well-coordinated campaign by Pakistan, Turkey, China and their proxies combined.⁵

The warning is unmistakable. India may possess the military, economic, demographic and technological weight of a major power, yet remain vulnerable in the one battlespace where the decisive contest increasingly takes place, and that is of the human mind; the mind of 1.4 billion is the target.

If the battle space is the mind, India has no means to control or protect or even have a say in it because it neither has the tools, wherewithal, an organisation or the very strategic mindset to understand the threat.

India must know that the next war will not begin with missiles, aircraft or artillery. It is already ongoing with narratives.

From Destroying the Enemy to Shaping the Mind

Historically, warfare sought to defeat the adversary by overwhelming his physical capacity to fight. Victory was measured in captured territory, destroyed forces, damaged infrastructure, and denied resources. Yet beneath these physical measures lay a more enduring objective, and that was to compel the adversary to accept one's will.

The decisive battlefield, therefore, was never entirely physical. Will, perception, morale and decision-making have always mattered. The aim was to break the enemy's will to fight, erode his

morale, disrupt his ability to think and decide, and ultimately bring him to a point where resistance was no longer sustainable. For centuries, this was achieved primarily through the scale, speed, and violence of kinetic operations – using superior tactics, strategy, and combat power to overwhelm the adversary physically and psychologically.

What has changed in the modern era is not the objective of warfare, but the pathway to achieving it. The paradigm is shifting from destroying the adversary's ability to fight to shaping his ability to think, decide, and act. Increasingly, the first objective is to subdue, disorient, divide or fracture the adversary even before the first shot is fired. The battlefield is no longer confined to territory; it extends into the minds of populations, leaders, institutions and societies. The objective now is to influence perception, manipulate narratives, exploit vulnerabilities, undermine trust, amplify divisions and distort decision-making, thus compelling the adversary, and even his allies, to act within a reality shaped by the opponent.

What has enabled this paradigm shift? The technology has transformed the scale and potency of this endeavour. Digital networks, social media, artificial intelligence, algorithms, deepfakes, behavioural analytics and ubiquitous connectivity provide unprecedented speed, scale, precision and reach for influencing human cognition. A message that once took days to travel can now reach millions within seconds; a carefully crafted narrative can be personalised to individuals, amplified by algorithms and reinforced repeatedly until perception begins to resemble reality.

Thus, the character of warfare is changing profoundly. Yesterday, armies sought to break the enemy's will by destroying his physical power. Today, adversaries increasingly seek to shape

that will before they even employ physical power. The ultimate prize remains the same: the adversary's will and decision-making. What has changed is the battlefield, the weapons and, most importantly, the speed and scale at which the human mind itself can be contested.

Many feel that Information and control over it was always a way of warfare, and therefore why should the new form of warfare that is the contest for cognition be any distinct concept? And why has social media become its most important contemporary battlespace?

Information Warfare is Older Than Information Technology

While Information warfare is often presented as a phenomenon of the Internet age, information has historically been an instrument of power.

In the 6th century, Sun Tzu's famous dictum, "all warfare is based on deception," captures a principle that long predates modern technology. Ancient rulers understood that what the adversary believed could shape the outcome of conflict even before armies met on the battlefield. Rumours, intimidation, deception, symbolic displays of power and psychological manipulation were employed to undermine an opponent's confidence, weaken his will and influence his decisions.⁶

Genghis Khan demonstrated this principle with extraordinary effectiveness. His campaigns were not based solely on the physical destruction of armies and cities; they were also designed to create a reputation for overwhelming power and ruthless retaliation. The Mongols often gave opponents a stark choice. Submit and survive, or resist and face destruction. Communities that surrendered could receive relatively lenient treatment, while those that resisted could

face extreme violence. The deliberate contrast between clemency and terror served a strategic purpose. News of what happened to one city was meant to influence the next city's decision.

Thus, Genghis Khan often did not have to fight every battle to win it. The battle was frequently won in the minds of those who had yet to fight. The movement of his armies, the reputation that preceded them, the messengers sent ahead and the consequences demonstrated to those who resisted created a psychological effect that could induce surrender before the physical battle began.⁷ His campaigns illustrate an enduring principle of warfare. If the adversary can be persuaded that resistance is futile, the physical application of force becomes secondary. It enabled the Mongols and Genghis Khan to avoid unnecessary fights, thus conserving combat power.

Chanakya more than two millennia ago, recognised that an adversary could be defeated not only by destroying his armies, but by manipulating what he knew, what he believed and how he decided. The *Arthaśāstra* describes using spies to spread false information, create suspicion, sow dissension, and deceive the enemy. In one passage, Kautilya explicitly refers to “spreading the false news” of danger to the enemy. “What has changed in the twenty-first century is not the principle, but the scale, speed and precision.”⁸ Kautilya needed spies to carry deception into the enemy's camp; today's adversary can place the deception directly into millions of minds through a smartphone.⁹

Even a subtle form of projecting power was followed by Romans. The Romans used coins, monuments, art and architecture to communicate imperial power and legitimacy. In each case, information shaped the adversary's perception of reality.¹⁰

The industrial age transformed the scale of this activity. Newspapers, telegraphy, posters, radio and cinema enabled

governments to communicate with mass audiences. During the First and Second World Wars, propaganda became an organised instrument of national mobilisation. The objective was not simply to deceive the enemy but also to strengthen morale at home, maintain support for the war and influence neutral populations.

The First World War also demonstrated that control of information infrastructure itself could become a source of strategic power. Control over communications channels allowed states to intercept, restrict, and manipulate information flows. The principle remains relevant today. Whoever controls the infrastructure through which information moves possesses a degree of strategic leverage over the information environment.

The First Strategic Use of Information Infrastructure as a Weapon

The roots of modern Information Warfare trace back to the First World War, when control of communication infrastructure was deliberately turned into a strategic instrument. A particularly significant example occurred on 5 August 1914, when Britain severed Germany's undersea telegraph cables connecting it to the wider world. This was among the earliest examples of a state deliberately exploiting both information and communications technology to gain strategic advantage.

By 1914, Britain possessed the world's most extensive undersea telegraph network, linking the British Isles with its colonies and commercial centres across the globe. The network was not merely a tool of commerce and communication; it was strategic infrastructure that gave Britain considerable influence over the flow of information. Once war broke out, London recognised that control of this infrastructure could be converted into an intelligence advantage.¹¹

The British objective was therefore twofold. Firstly, to isolate Germany from independent global communications and secondly to compel German communications to pass through channels that Britain could monitor and control for manipulation.

The operation was accompanied by the establishment of a worldwide censorship and interception system. As the cables were cut, officials designated as "Censors" began appearing at critical communications nodes across the British Empire. At Porthcurno in Cornwall, where transatlantic telegraph cables came ashore on a secluded beach, a censor took up position at the cable station. In Hong Kong, another "secret censor" arrived at the Eastern Telegraph Company's offices. Similar officials were deployed across the far-flung British communications network, from Malta and Gibraltar to Singapore and other strategic locations.

Once the system was activated, these officials were instructed to signal London with the message "Fixity London, Fixed", indicating that the censorship arrangements were operational.

What followed was, in effect, the creation of a global communications-surveillance architecture. British censorship was explicitly designed to prevent intelligence from reaching the enemy and to disrupt communications between the enemy and its agents. Britain's dominance of the international telegraph infrastructure therefore gave it something much more valuable than a communications advantage, and that was the ability to observe, filter and influence the flow of information across an interconnected world.

The scale was unprecedented for its time. About 50,000 messages passed through the hands of about 180 censors in British offices every day, while another 400 censors worked at about 120 stations overseas. By the end of the war, an estimated 80 million messages had been censored.

The strategic consequences were considerable. By cutting German cables and forcing German communications onto networks that Britain could monitor, Britain created what can be described as an intelligence windfall. Communications that would otherwise have remained beyond British reach became accessible to interception, analysis, and exploitation.

One of the most consequential examples was the Zimmermann Telegram, which British intelligence intercepted during the war. The message revealed Germany's proposal to Mexico for an alliance against the United States, including the prospect of Mexico recovering territories lost to the United States. Its disclosure contributed significantly to the political environment that preceded America's entry into the First World War on the Allied side.¹²

The significance of this episode extends far beyond telegraph technology. It demonstrates a fundamental principle that remains relevant to Information Warfare today, and that is whoever controls the infrastructure through which information flows can acquire the ability to control, monitor, manipulate, and exploit the information itself.

The British did not merely attack German communications; they altered the information environment in which Germany was forced to communicate. They combined the physical action of cutting cables with technological dominance, interception, censorship, and intelligence exploitation. In doing so, they demonstrated an early form of what would today be recognised as information warfare conducted through control of critical communication infrastructure.

The lesson is particularly relevant in the digital age. Undersea cables, satellites, data centres, cloud infrastructure, social-media platforms, search engines and telecommunications networks have replaced much of the telegraph infrastructure of 1914. Yet the

underlying strategic principle has changed little. Control the channels, shape the information flow; shape the information flow, and influence perception, decision-making and behaviour.

The First World War thus provides an important historical reminder. Information Warfare is not a product of the internet age. The internet has merely multiplied its speed, reach, scale, and sophistication. The digital age and social media platforms have only further expanded the scale in the past decade.

India, bereft of any such infrastructure or controls, is at the mercy of the tech Giants and the Social Media platforms for intelligence operations to understand the perception, behavior, angst, and grievances, and use them to scale to influence decisions and trigger responses.

Later during the Cold War, information warfare evolved into ideological competition. The United States and Soviet Union did not merely compete militarily; they competed to demonstrate the superiority of competing political and economic systems. Radio, television, education, culture, literature and international broadcasting became instruments of influence. Thus, the historical progression is not from "no information warfare" to "information warfare." It is from low-speed interpersonal influence to mass communication and finally to digitally networked influence.

The contemporary information environment has since transformed due to technology, and it differs principally in three respects: speed, scale, and personalization or precision. The technology has changed the scale of information management and manipulation but the underlying purpose remains the same. Subdue the enemy and adversary, manage the allies, and partners, and seek control over the population. Essentially technology changed the means, not the underlying purpose as is tabulated below as a distinction over the time and mediums used:

Era	Principal medium	Character
Ancient	Rumour, messenger, symbolism	Deception & intimidation
Industrial	Newspapers, posters, telegraph	Mass persuasion
World Wars	Radio, cinema, propaganda	Mass mobilisation
Cold War	Radio, television, education, culture	Ideological competition
Internet	Websites, email, forums	Networked influence
Social media	Platforms, influencers, algorithms	Personalised influence
AI era	Deepfakes, synthetic media, autonomous systems	Scaled cognitive manipulation

As history makes evident, every major revolution in communication has also produced a corresponding revolution in warfare. From the telegraph and radio to television, the internet and social media, each transformation has altered how information is generated, transmitted, controlled and weaponised.¹³ Today, however, the transformation runs even deeper. Control over the information infrastructure itself has become a source of strategic power. The threat of cutting the internet cables in the Hormuz has become an important leverage by Iran after the US decided to attack in Feb 28, 2026.¹⁴

This is perhaps the most consequential transition in the contemporary battlespace of mind. The contest is no longer merely over the information that flows through networks, but increasingly over the platforms, algorithms, technologies and digital ecosystems

that determine what information is created, amplified, suppressed and ultimately seen by billions. The ability to control or influence these Big Tech platforms is therefore no longer simply a commercial advantage; it is emerging as an instrument of strategic power and a critical determinant of influence in the battle for mind space.

Why the Shift from Information Warfare to Cognitive Warfare is Transformational?

The shift from Information Warfare to Cognitive Warfare is not merely a change in terminology; it represents a fundamental shift in the battlespace, the target, and the desired outcome.

In Information Warfare, the strategist and practitioner are primarily concerned with the information environment as to what information the adversary or the intended target receives, what information it seeks, and through which channels that information can be transmitted. The effort then focuses on monitoring, controlling, manipulating, and managing the information that flows through these networks. The centrality, therefore, remains information and the communication networks through which it is transmitted.

Psychological warfare takes the contest a step further. Its practitioner is less concerned merely with what information reaches the target and more concerned with how the target feels and responds to that information. The timing, mode, context and form of communication can produce very different psychological effects. The objective is therefore to influence emotions, attitudes and perceptions in ways that affect the target's response.

Cognitive Warfare goes deeper still. Its ultimate concern is the cognitive process through which information is perceived, interpreted, processed and converted into judgement and decision. It seeks to influence perception, interpretation, reasoning,

judgement and decision-making, and ultimately behaviour. The difference is subtle but fundamental: Information Warfare seeks to control the information environment; Cognitive Warfare seeks to influence what the human mind does with that information.¹⁵ With respect to Cognitive Warfare, NATO's Strategic Warfare Development Command summarises, "Cognitive Warfare integrates cyber, information, psychological, and social engineering capabilities. These activities, conducted in synchronization with other Instruments of Power, can affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary."¹⁶

This is where contemporary technology has created a transformational advantage. Digital platforms can analyse what an individual or a group consumes, identify patterns of behaviour and preference, and deliver content tailored to produce a desired response. What was once largely a mass and relatively blunt exercise in propaganda can now become direct, personalised, scalable and extraordinarily rapid. Different messages can be directed simultaneously at different individuals, communities and population segments, each designed to evoke a different response. The same information environment can therefore produce different realities for different audiences.

In simple terms, the evolution can be seen as a progression:

Physical Networks → Cyberspace → Information Domain → Psychological Operations → Cognitive Warfare

This is not a linear replacement of one by another. The earlier domains and methods continue to exist, but technology has progressively expanded the battlespace and moved the centre of gravity closer to the human mind. Warfare has evolved from contesting physical spaces and communication networks to

contesting the information environment, then psychological responses, and finally the cognitive processes that determine how people perceive reality, form beliefs and make decisions.

Cognitive warfare, therefore, is not simply ‘better propaganda’. It seeks to influence attention, perception, memory, identity, emotion, beliefs, interpretation, judgement, decision-making and, most importantly, behaviour. The transformational element is the ability of technology to undertake this at speed, scale and precision that were previously impossible.

Recent Events Illustrate the Potential Consequences

In Nepal, youth anger over corruption—an issue that had existed for years—was intensified by the government's social media ban. Within days, the mobilisation contributed to the overthrow of an elected government in September 2025.¹⁷ The drivers have been described as geopolitical, while social media—most prominently the relatively little-known platform Discord—became an important instrument of mobilisation. The significance lies not simply in the existence of public anger, but in how rapidly digital platforms were able to aggregate, amplify and convert that sentiment into collective action.

A similar phenomenon was witnessed in Bangladesh, where the government of Sheikh Hasina rapidly collapsed in August 2024 following weeks of protests. Social media played a significant role in mobilisation and amplification, alongside the actions of radical elements on the streets.¹⁸

India too has witnessed the growing power of digitally generated narratives and mobilisation. The recent efforts to challenge the Modi government through the effective use of social media platforms, manipulation of content and the coming together of a large number of opposition parties with the newly launched

CJP demonstrated how rapidly a new political formation could occupy the digital mind space. The education minister's resignation was a partial success, but the more significant development has been their ability to capture attention and shape the conversation through social media. Its leadership, all in their 20s, has subsequently been celebrated across media channels and public events, while senior political figures have increasingly taken a back seat.

This assumes even greater significance in India because more than 66% of the population is below 35 years of age,¹⁹ a generation that has grown up with smartphones, social media and instantaneous access to information. For this generation, the digital environment is not an additional source of information; it is increasingly the environment in which information, identity, opinion and social interaction are formed.

This presents a profound challenge to India's security establishment. The traditional security architecture has been designed largely to protect territory, borders, infrastructure, institutions and physical populations. The emerging challenge is protecting the cognitive space where perceptions form, narratives compete, trust is created or destroyed, and decisions are made. This is why India should consider Cognitive Warfare a distinct domain or battlespace, as the world already is.

The target of Information Warfare is the information environment. The target of Psychological Warfare is the psychological response to information. The target of Cognitive Warfare is the cognitive process through which human beings convert information into perception, belief, judgement, decision and action.

That distinction is fundamental as is the strategic implication equally fundamental. The contest is no longer merely over who

controls the information. It is increasingly over who influences what the human mind believes, how it interprets reality, what decisions it makes, and ultimately how it behaves.

Why Social Media has become the New Cognitive Battlespace

In cognitive warfare, social media is one of the most contested terrains in the cognitive domain. There are, of course, many instruments through which cognition can be shaped—education, historical books and references, religious and ideological narratives, cultural influences and the deliberate shaping of collective memory. The recent appropriation and claiming of the Indus Valley Civilisation and Harappan Civilisation by Pakistan is one such example.²⁰ Pakistan was carved out of Bharat in 1947 and, until relatively recently, sought to distance itself from histories that extended beyond its Islamic past. Selective interpretation and projection of history, ideological narrative-shaping, and deliberate misrepresentation or selective extrapolation have long been used to influence societies. The British employed such methods extensively during the colonial era across the countries under their control, with particular emphasis on India through the education system.

Legacy media has also been an important instrument in the cognitive domain. However, its processes were comparatively slow, selective and institutionalised. In legacy media, information traditionally flowed through a structured chain—from the reporter to the editor and thereafter to the audience. The process could be slow and deliberative, but it remained powerful and influential. Print and television media operated within frameworks of professional responsibility and accountability, even when owned or controlled by independent businesses, states or organisations with particular ideological orientations.

The gatekeeper concept was central to this system. Information passed through editorial processes governed by professional norms, judgement and, at least in principle, institutional accountability. This created delays, but those delays also provided opportunities for verification, contextualisation, analysis and editorial responsibility.

Social media has fundamentally altered this model. Social media platforms operate on a radically different pattern. It is the one characterised by scale, speed, personalisation and continuous amplification. Anyone with a smartphone can record an event and upload it instantly to one or multiple platforms, often without context, verification, or consideration of its wider impact. The content's emotional or sensational value can determine how quickly it attracts attention. Algorithms can then amplify it through interconnected networks and direct it towards individuals or mass audiences based on consumption patterns that platforms have already analysed.

This creates an entirely different information ecosystem. The audience no longer merely receives information; it simultaneously creates, consumes, shares, and amplifies it. A smart content creator can exploit the logic of algorithms by using particular keywords, timing, emotional triggers and carefully constructed narratives to maximise reach while at times maintaining anonymity.

The result is the erosion of the traditional gatekeeper. A reporter and editor are no longer necessarily required before information reaches millions. An individual, an anonymous account, an influencer, an organised group or even an automated system can potentially perform the role of publisher, distributor and amplifier simultaneously.

Why is the social-media model being radically different and dangerous? Social media can also follow a more subversive and

self-reinforcing cycle, as has been witnessed in recent conflicts including the Israel-Hamas war, the Iran-US conflict and the Russia-Ukraine war. Information, whether fabricated, manipulated or genuine but presented without context, can originate from fake or genuine accounts, reach influencers, and then be amplified through digital networks. Once picked up by mainstream media, it can enter the wider public discourse, influence perceptions and generate pressure for governmental and institutional responses. The information cycle can therefore move from an obscure digital post to mainstream media, from mainstream media to public discourse, and from public discourse to government action. This represents a profound transformation in the relationship between information and power.

In the contemporary world, every citizen with a smartphone can potentially become a journalist, content creator, influencer or amplifier. More importantly, social media can increasingly drive the agenda of mainstream legacy media rather than merely follow it. What begins as a digital narrative can migrate into television studios, newspaper headlines, political debates and policy discussions. This is what makes social media uniquely weaponisable in the cognitive battlespace.

Its power lies not simply in the quantity of information it carries, but in the way it combines speed, scale, personalisation, emotional amplification and algorithmic distribution. Information can reach millions before institutions have even established whether it is true. Narratives can gain momentum before authorities understand their origins. Emotional reactions can precede rational assessment.

Information now travels faster than verification. Emotion travels faster than evidence. And in that gap lies an extraordinary opportunity for cognitive warfare. The consequence is profound.

The side that controls the narrative, or can shape what people see, feel, and believe, can influence the cognitive environment in which governments, institutions, and societies make decisions.

The individual is no longer merely an audience member. He or she can simultaneously be a consumer, producer, commentator and distributor of information. This has several strategic consequences. First is the Scale. Social-media platforms can reach hundreds of millions or billions of people. India alone had approximately 500 million social-media user identities in October 2025, while internet users numbered approximately 1.03 billion (DataReportal, 2026).²¹ The second is Speed. Information can cross national boundaries in seconds. Verification usually takes longer. This creates a fundamental asymmetry: the speed of information increasingly outpaces the speed of verification. The third is the Low cost. Traditional influence operations required printing, broadcasting infrastructure, or physical distribution. Social media drastically reduces the cost of global communication. Fourth is Personalisation. Traditional propaganda often broadcasts one message to millions. Digital platforms permit highly differentiated messages to different audiences. One group may receive a religious message; another an economic grievance; another a nationalist appeal; another a message based on regional identity. The objective is therefore not merely mass persuasion. It is precision influence.

The fifth is Algorithmic amplification provided by platforms, where the most strategically important actor may not always be the person who creates content. The algorithm may determine who sees it. Recommendation systems determine what appears in feeds, what becomes visible, what trends, and what disappears. The European Union's Digital Services Act explicitly recognises that recommender systems, advertising systems, data practices and algorithmic amplification can contribute to systemic risks,

including the spread of misleading or deceptive content (European Union, 2022).²²

The sixth factor is emotional amplification, in which content that generates anger, fear, outrage, humiliation, or excitement is particularly capable of generating engagement. Research by Vosoughi, Roy, and Aral (2018), based on approximately 126,000 verified news stories shared on Twitter between 2006 and 2017, found that false news travelled farther, faster, and more broadly than true news, with the effect particularly pronounced for political falsehoods. The researchers also found that human users played a major role in spreading false news. This is an important finding because it challenges the assumption that the problem is simply "bots".²³ The weapon is often not the bot. The human being voluntarily amplifies the message.

Seventh is the factor of Echo chambers and confirmation bias. Algorithms can repeatedly expose individuals to content consistent with their existing beliefs.²⁴ The result can be information bubbles in which individuals encounter increasingly similar views and become less exposed to alternative interpretations. This creates a vulnerability that cognitive warfare can exploit. The objective is not necessarily to change someone's worldview completely. It may be enough to make an existing belief more extreme.

The last two, but more dangerous, are repetition and permanence. The technology of repetition, and the permanence of digital media are ominous. A long-forgotten statement by a politician can be replayed when the stance changes. Claims made by an individual in weaker moments can come back to haunt. The recall value and repetition are impactful for shaping and reinforcing minds.

Social media has combined the reach of mass media, the intimacy of interpersonal communication, the targeting capability

of intelligence systems, and the speed of real-time broadcasting. This combination makes it qualitatively different from television or newspapers and explains why it has become the preferred platform for cognitive warfare.

When applied to the target population, the numbers and economics fundamentally shift the advantage toward social media. At the start of April 2026, 6.12 billion people used the internet, 73.8 percent of the world's total population. Social media users totaled 5.79 billion, representing 69.9 percent of the global population, and 2.42 billion active generative AI users, or 29.2 percent.²⁵ In 2023, Annabelle Nyst reported 5.17 billion social media users worldwide, representing 63.7 percent of the global population and close to 95 percent of all internet users.²⁶ The number has grown substantially since then.

While a significant number of people continue to read newspapers and watch television for news, the centre of gravity has steadily shifted towards social media. The fundamental difference is that legacy media primarily enables one-way transmission of news, whereas social media enables continuous conversation, participation, reaction and amplification.

Over time, this has also contributed to a growing perception that legacy media is controlled by large businesses and corporate houses, and that many media organisations are aligned with particular political parties or ideological positions. Consequently, some sections of society have come to believe that news independence can be compromised.

Social media, in contrast, has created a powerful ecosystem in which influencers and individual contributors can create, distribute and monetise content,²⁷ while platforms themselves benefit from the scale of engagement and the number of views generated.²⁸ The interests of the individual content creator and the platform can

therefore become mutually reinforcing. The more content attracts attention, the more it is consumed; the more it is consumed, the more it is amplified; and the more it is amplified, the greater the economic value to both the creator and the platform.

This combination of reach, participation, personalisation, amplification and economic incentive has progressively pushed social media to the centre of the contemporary information environment and, consequently, to the centre of the emerging cognitive battlespace.

The Weaponisation Cycle: From Grievance to Behaviour

The Cognitive Weaponisation Cycle can be understood as a sequence through which an existing grievance is identified, converted into a compelling narrative, amplified through digital networks, transformed into an emotional response and ultimately converted into collective behaviour. The eight-step cycle follows a pattern: identify the audience, identify the grievance, construct the narrative, seed the narrative, amplify through networks and algorithms, Trigger emotion, normalize through repetition, and convert perception into behavior.

The Nepal street protest is not a classic case of weaponising social media in the military sense or from a warfare perspective. It is, however, a typical case study of an existing local issue of corruption and a social media ban turning into a cycle of grievance to behavior. Such a cycle can be weaponized, particularly in India, where many fault lines exist. Inimical agencies can exploit grievances over governance, corruption, and elitism to weaponize social media for cognitive warfare.

The Nepal Gen-Z protests of September 2025 illustrate how this cycle can operate in practice.

Identify the audience - The youth. Nepal had a large and digitally connected young population. The protesters were predominantly young people, many of them students, who were already active in the digital information environment. The audience was therefore not created; it already existed as a connected and receptive community.

Identify the grievance. Corruption, unemployment, and the social media ban were key grievances. The country had seen repeated government changes. The underlying grievances were not new. Young Nepalis had longstanding frustrations over corruption, limited economic opportunities and the perceived failure of the political establishment. The government's decision to block several major social media platforms provided the immediate trigger. For many young people, the ban was perceived not merely as a regulatory measure but as an attack on freedom of expression and an attempt to silence them.

Construct the narrative. The disparate grievances could now be brought together under a simple and emotionally powerful narrative, and that was, 'a corrupt and unresponsive political establishment was attempting to silence the youth.' The social media ban therefore became more than an administrative decision; it became a symbol around which accumulated anger could be organised.

Seed the narrative. The government attempted to restrict the very digital networks that seeded the narrative. Youth leaders and groups used alternative digital channels to communicate, organise and call people to action. On September 8, youth leader Sudan Gurung announced the Discord channel "Youths Against Corruption" as a "central communication system" for the protest.

Amplify through networks and algorithms. Once the narrative entered connected digital communities, it could spread rapidly

through peer-to-peer networks. The traditional requirement for an institutional media organisation to disseminate the message was removed. Individuals became communicators, amplifiers and organisers simultaneously. The movement quickly moved beyond Kathmandu and spread nationwide.

Trigger emotion. The narrative linked political grievances to powerful emotions: anger, frustration, humiliation, and then a sense of being silenced. The government's response to the protests, including the use of force and the resulting deaths and injuries, further intensified those emotions. What began as opposition to a social media ban became a much broader confrontation with the political establishment.

Normalise through repetition. As the narrative was repeatedly communicated, reinforced and discussed across digital networks and then entered the wider media environment, the perception of a corrupt and unresponsive establishment became increasingly normalised among participants. The protest was no longer an isolated reaction to a government decision; it had become a collective movement with its own identity, symbols, leaders and demands.

Convert perception into behaviour. The final transition was from belief to action. Thousands of young people came onto the streets. Demonstrations spread rapidly, government buildings were attacked, and the political crisis escalated dramatically. Within roughly 28 hours of the protests escalating on September 8, Prime Minister K.P. Sharma Oli's government had collapsed.

The Nepal experience demonstrates the central proposition of the cognitive weaponisation cycle. The objective is not merely to transmit information. It is to convert information into perception, perception into emotion, emotion into collective belief, and collective belief into behaviour.

The technology does not create every grievance. It creates the architecture through which an existing grievance can be identified, organised, amplified and rapidly converted into collective action. That is the transformational power of the cognitive battlespace.

India Stands Exposed

In India, the conditions for cognitive contest are already present. Grievances exist, social and political fault lines exist, competing political interests seek narrow gains, and geopolitical actors seek to influence governments and public opinion in favour of particular alignments, trade relationships and strategic alliances. What has changed is the technological environment, which now enables these existing vulnerabilities to be exploited.

India's vulnerability is compounded by the fact that the dominant social media platforms are not based in India and remain beyond its direct control. Unlike China, which has created a tightly controlled digital ecosystem, India has neither comparable technological barriers nor the same degree of control over the platforms through which information increasingly flows. At the same time, India's democratic system, with constitutional protections for freedom of expression and an open information environment, places legitimate limits on how far the State can regulate, control, or block content.

This combination presents a unique strategic challenge. India is an open, democratic and digitally connected society operating in an information environment over which it has limited control.

The challenge is enormous in scale. India has a population of 1.4 billion, with more than 65% under 35. Millions of people continue to emerge from poverty, becoming increasingly empowered, aspirational and digitally connected. They are seeking opportunities, entitlements, recognition and a better quality of life.

This is an extraordinary national strength. However, in the cognitive battlespace, it can also become a vulnerability if grievances, aspirations and expectations are deliberately manipulated.

The Worst-Case Scenario: From Political Contestation to Strategic Paralysis. The worst-case scenario is that the objective of cognitive manipulation within India is not merely political mobilisation, but political polarisation for electoral gains and vote-bank consolidation. This follows a pattern that has existed in India since independence, but technology has the potential to make it faster, wider and more difficult to contain.

Political polarisation can lead to street mobilization by exploiting one or more existing fault lines simultaneously, such as communal, caste, class, regional, linguistic, or ideological. What may begin as an electoral strategy can progressively deepen social tensions and, over time, erode public confidence not merely in a particular political party or government, but in the institutions of the State itself.

Once institutional trust begins to weaken, the consequences can extend beyond electoral politics. As political influence is exerted and institutions become progressively weakened, ideological recruitment and radicalisation become greater possibilities. In the resulting environment, inimical external agencies and non-state actors can exploit it to deepen existing divisions and weaken the State from within.

The most dangerous outcome is strategic paralysis, a situation in which the government reaches a point where acting and not acting both carry severe consequences. Every decision becomes politically costly; every intervention risks further escalation; and the State becomes hesitant to exercise legitimate authority because of the anticipated social and political consequences.

The Farmers' Agitation of 2020–21 illustrates this dilemma. Faced with the potential for serious political and social consequences, the State ultimately chose not to use force to end the prolonged agitation. While this avoided an immediate escalation, the prolonged disruption imposed high costs on the wider economy and exposed the difficulty of the State in managing a politically sensitive mobilisation. The economic loss has been estimated at more than Rs 70,000 crore.²⁹ More significantly, such situations can create a perception that institutions are unable to resolve prolonged internal challenges.

This is precisely where cognitive warfare can become strategically consequential. An adversary does not necessarily need to defeat the State directly; it can seek to create conditions in which the State progressively weakens itself. By amplifying grievances, deepening polarisation, eroding institutional trust and exploiting political divisions, inimical agencies can contribute to an environment in which governance becomes increasingly difficult and decisive action increasingly costly.

The emergence, over the past few years, of documents and narratives associated with George Soros-funded organisations and allegations concerning the Adani Group, corruption and financial payouts provides another illustration of how external influence can potentially shape public perceptions. Such narratives have surfaced at politically critical moments, including around elections, and political parties, interested media organisations, and social media networks have subsequently amplified them.

The significance of such episodes lies not necessarily in whether every allegation is true or false, but in how information of this nature can be selectively amplified to create doubt, suspicion and distrust among the population. When politically interested actors and media organisations adopt, repeat and amplify such narratives

through social media platforms, their reach and impact can increase exponentially.

This illustrates a broader vulnerability of the cognitive battlespace. An external actor does not necessarily need to manufacture an entirely false narrative. It can exploit an existing controversy, selectively amplify information, connect disparate allegations and inject it into an already polarised political environment. The resulting doubts can then acquire a life of their own as they move through political discourse, mainstream media and social media.

The strategic effect is the same. Influence perceptions, deepen distrust and shape public opinion at moments when political and institutional confidence is particularly consequential. These create doubts and mistrust in the very institutions that are there to serve the people. Over time, such external influence can wither down economic strength, disrupt development and progress, weaken institutional authority and consume the political and administrative energies of the State achieving strategic effects without conventional military confrontation.

The ultimate danger, therefore, is not simply social unrest. It is a condition in which a nation remains materially powerful but becomes increasingly incapable of converting that power into effective national action.

The recent CJP movement, although rooted in a genuine grievance over alleged leakages and irregularities in the National Testing Agency examinations, particularly NEET, provides another illustration of the Grievance-to-Behaviour cycle. An existing grievance gained momentum in the digital space, drew attention, sparked emotional responses, and translated into real-world political consequences. The significance of the episode lies not merely in the grievance itself, but in the speed with which a

grievance can be amplified, transformed into a narrative, converted into collective sentiment and ultimately translated into behaviour.

When India launched airstrikes against a suspected JeM camp in Pakistan two weeks after it's terrorist cell attacked a paramilitary convoy with an improvised explosive device (IED) in February 2019. It rapidly escalated into a military crisis. "Pakistan quickly weaponized its social media space, spreading disinformation or "fake news," using old photographs and videos of downed jets and destroyed equipment, implying their wreckage resulted from the recent aerial duel between its air force and Indian fighter jets. In doing so, the Pakistani security establishment successfully used social media and television to spread disinformation and chaos through multimedia content, and turned the Indian public against its own political leadership, in what seems to have been – until now – a rare example of organized state-sponsored weaponization of social media – during an active military crisis.³⁰

Debasis further writes for War Room Journal of Army War College, USA, "social media has been used before to stir trouble, but the extent to which social media was weaponized throughout a crisis response is potentially revolutionary. Pakistan combined its social media capabilities with a calibrated disinformation campaign to offset India's superior conventional military capability. The Pakistani security establishment unleashed chaos with concerted and coordinated action, led by its Director General of Inter-Services Public Relations (DG-ISPR), with the active support of the Pakistani intelligentsia plus a few Indian opportunists.³¹

A similar vulnerability became evident after Operation Sindoor. India achieved clear military objectives in its contest with Pakistan. Yet, alongside the conventional contest, a parallel battle unfolded in the mind space. Pakistan, Turkey and China, together with their affiliates and non-state actors across the world, mounted

a collaborative campaign aimed at influencing perceptions and narratives surrounding the conflict.³² The campaign exploited ideological sentiments within India and leveraged the country's existing political and social divisions.

The contrast is stark. India possessed overwhelming conventional capabilities, but its response in the cognitive domain was neither commensurate nor adequately integrated with its military effort. The Indian establishment seemed to have no effective answer to either challenge.

These three episodes, one political and two military, each very different in nature, point towards the same vulnerability. India's ability to exercise conventional power has not yet been matched by an equivalent ability to protect, contest and shape the cognitive domain. The full weight of India's comprehensive national power of political, technological, informational, diplomatic, economic and military has not yet been brought to bear in this new battlespace.

The lesson is therefore not that India lacks power. It is that India has yet to learn how to convert its considerable national power into cognitive power. India therefore faces a paradox. The very demographic, democratic and digital characteristics that constitute its national strength can also provide fertile ground for cognitive manipulation.

Territorial wars for land, water and airspace can be fought and, potentially, won through the application of conventional military power. India possesses the military strength to defend its territorial interests. But brute force has little utility against an onslaught in the social media and cognitive domain. Tanks, aircraft, ships and missiles cannot defeat a narrative, reverse a manipulated perception or restore trust once it has been systematically eroded.

India's vulnerability is further accentuated by this new battlespace's asymmetry. It does not presently possess comparable platforms, technologies, capabilities and resources to contest the cognitive domain against well-organised and technologically enabled state and non-state actors. The adversary does not necessarily have to defeat India's military; it can seek to shape the perceptions, divisions, anxieties and decisions of the society that supports it.

This is where India's conventional superiority can become irrelevant. India may be capable of winning a war for territory, yet remain vulnerable in a war for the mind. And unlike the territorial battlespace, the cognitive battlespace has no clearly defined border, no front line and no warning before the attack begins.

Who is Weaponising Social Media?

The weaponisation of social media is not the preserve of any single actor. States, non-state organisations, political actors, commercial interests and individuals can all exploit the same digital ecosystem, although their objectives may be very different. What makes social media particularly potent is that these activities often intersect, reinforce and amplify one another.

The three Indian examples discussed earlier illustrate this phenomenon. A hostile state or external actor may initiate a narrative to discredit India's institutions or Armed Forces. Political opponents may then appropriate and amplify that narrative for domestic political advantage, while opportunistic individuals, influencers or media platforms may further magnify it because it generates attention and engagement. The original narrative and its subsequent political and commercial amplification may therefore become indistinguishable.

Thus, the real danger is not merely who originates a narrative, but who amplifies it, who benefits from it and how the algorithm distributes it. Broadly, five categories of actors are capable of weaponising social media:

- States and state-sponsored actors
- Non-state armed and terrorist organisations
- Political parties and political networks
- Commercial actors and social-media platforms
- Individuals, celebrities and influencers

Their motivations may range from geopolitical competition and political warfare to ideological mobilisation, electoral advantage, commercial profit, personal influence and even revenge.

States and State-Sponsored Actors. States are among the most sophisticated users of social media as an instrument of strategic influence, foreign interference, psychological operations, political warfare and, during armed conflict, military deception.

The objective rarely stops at spreading false information. More often, the objective is to shape the information environment in which a population, government or military makes decisions. A state may attempt to influence the domestic population of an adversary, shape international opinion, create distrust between citizens and institutions, influence electoral or political processes, amplify social, religious, ethnic or regional divisions, create fear and uncertainty, undermine confidence in military capability, influence the adversary's decision-making or/and reduce the political will to sustain a particular policy.

The Russia-Ukraine conflict illustrates this contest. Different European countries, political groups and external actors have used

social-media ecosystems to promote competing narratives concerning military assistance, escalation, negotiations and ceasefire. These narratives are directed simultaneously at domestic populations, allies, adversaries and international audiences.

Similarly, issues such as Tibet, trade, border disputes and bilateral relations between India and China can acquire multiple layers of information competition. Governments, diaspora groups, activists, foreign interest groups, political actors and media networks may all attempt to influence the narrative for different purposes.

The ultimate objective of state-sponsored information operations may therefore not be to convince an audience of one particular "truth", but to create enough uncertainty, distrust, or polarisation to make collective decision-making harder.

Non-State Armed and Terrorist Organisations. If states possess resources, institutions and technological capabilities, non-state armed and terrorist organisations possess something equally important, and that is adaptability.

Some of the most innovative exploitation of digital communication has been demonstrated by terrorist and extremist organisations. Al-Qaeda recognised the strategic value of cyberspace well before today's social-media environment matured. Through websites, online forums and digital propaganda, it created ideological communities that extended far beyond its physical presence. Al-Qaeda showed that territorial presence wasn't essential to exercising influence. An organisation could operate from remote locations while projecting its ideology across continents.

The Islamic State (ISIS) subsequently took this model to another level. Its propaganda ecosystem combined recruitment, ideological

indoctrination, intimidation, mobilisation and the projection of organisational strength. Professionally produced videos, graphics, multilingual content and rapidly distributed material transformed propaganda into a sophisticated psychological instrument.

The objective varied by audience. To supporters, it projected strength and belonging, to recruits, it projected purpose and adventure, to opponents, it projected fear and to undecided audiences, it projected momentum and inevitability. This was strategically important because it demonstrated that a non-state actor did not need the communication resources of a state to compete in the information domain. It needed only a narrative, a grievance, a network and an audience.

The asymmetry becomes even more significant when you consider the constraints under which different actors operate. Democratic governments are required to function within constitutional and legal boundaries involving freedom of expression, privacy, judicial oversight, human rights and political accountability. Terrorist and extremist organisations operate without comparable restraints.

Consequently, the contest is inherently asymmetric. A government may require months to establish a policy, clear legal procedures and communicate an official position. A terrorist organisation can produce, modify and disseminate a narrative within minutes. When one platform becomes difficult to exploit, hostile actors can migrate to another. When open platforms improve moderation, closed groups, encrypted applications or alternative platforms can become more attractive. For the non-state actor, the technology changes but the objective does not.

The remarkable feature of this asymmetry is that non-state actors can exploit communication infrastructure created through

billions of dollars of investment by governments and corporations without having to own that infrastructure themselves.

Political Parties and Political Networks. Political actors are perhaps the most obvious users of social media because politics itself is fundamentally a contest over ideas, perceptions, identities and public opinion. They also adapt quickly to survive and remain relevant.

Political parties, campaign organisations, partisan networks, political consultants, activists and political influencers can use social media to mobilise supporters, influence voting behaviour, shape public perceptions of opponents, frame political issues, exploit grievances, create polarisation, discredit institutions or individuals and influence political agendas.

The important transformation is that political communication is no longer controlled by political parties or traditional media organisations. A political narrative can originate with a party, an activist, a journalist, a celebrity, or an anonymous account and then take on a life of its own.

The growing political role of prominent technology entrepreneurs and social-media personalities has added another dimension. Individuals who command enormous digital audiences can potentially influence political discourse at a scale once available only to governments and major media organisations. Electoral politics in several countries shows that social-media influence can cross geographical boundaries, allowing domestic political narratives to become international and foreign narratives to enter domestic contests. This makes social media not merely a communication medium for politics, but increasingly a contested battlespace for political perception.

Commercial Actors and the Attention Economy. A fourth category consists of commercial actors, particularly the owners and operators of major social-media platforms. Unlike states or terrorist organisations, their primary objective is generally not political warfare. Their principal incentive is commercial to maximise attention, engagement, and therefore monetisation.

The basic economic chain can be sequenced as attention, engagement. Data generation, advertising, and then revenue. This creates what has come to be called the attention economy. Without revenue, any system will fail.

The critical point is that algorithms are generally designed to maximise engagement. Content that generates strong emotional reactions, such as anger, fear, outrage, excitement, controversy, or fascination, can therefore receive greater visibility than content that is merely accurate but less emotionally compelling.

This creates a structural vulnerability that is exploited by the social media platforms, states, non-states, individual influencers and political entities alike. False, sensational, provocative or divisive content can become highly successful because it attracts attention. A hostile actor does not necessarily need to "control" a platform to exploit it. It may simply learn how the platform rewards attention and then design content accordingly.

This produces a paradox wherein the platform may be commercially optimised for engagement, while the hostile actor is strategically optimised for influence. The two objectives can unintentionally reinforce each other. As the platform seeks more engagement, the influencer seeks more followers, the political actor seeks more support and the hostile actor seeks greater disruption. And yet all four may benefit from the same phenomenon: of greater visibility of emotionally powerful content.

Therefore, the weaponisation of social media does not always require a hostile government sitting behind the operation. The attention economy's economic architecture can create incentives to amplify content that is emotionally provocative, polarising, or misleading.

Individuals, Celebrities and Influencers. Perhaps the most revolutionary development in the social-media era is the emergence of the individual as a mass-media institution. A celebrity, influencer, or even an anonymous account can reach an audience larger than a newspaper, television channel, or government press conference. This represents a fundamental collapse of traditional information hierarchies.

In the traditional information environment, authority was largely hierarchical, with the government leading, feeding news agencies, which in turn informed citizens and the world. Social media has transformed this into something far more horizontal wherein anyone can inform everyone. A person carrying a smartphone can spread information within seconds, forcing the governments to respond.

An individual with millions of followers can therefore bypass traditional gatekeepers and communicate directly with a global audience. The significance becomes clear when you compare the reach of leading global personalities with that of political leaders. Celebrities such as Cristiano Ronaldo, Lionel Messi, Taylor Swift, Selena Gomez, Kylie Jenner and Rihanna command enormous audiences across social-media platforms. Political leaders such as Narendra Modi, Donald Trump and Barack Obama also possess exceptionally large followings, but their influence is often associated more directly with political communication.

For record, on Instagram the leading influencers are Ronaldo and Messi; after them, the next set are singers and others like the

Kardashians, Swift, Kylie Jenner, and Selena Gomez, with followers from 670 to 280 million. If Kim Kardashian's 13-year-old daughter gets pregnant, she turns all advice from society and doctors to dust. While PM Modi has 105 million and Trump 70 million, their influence is restricted only to information.

Similarly on X, the followers of Elon Musk is 241 million, Obama 119 million, Ronaldo, Trump 111 million, Modi 107 million. They are followed closely by influencers such as Rihanna, Katy, Swift, and Lady Gaga. Facebook of Meta has 3 billion followers, YT has 3.5 billion, WhatsApp of Meta 2 billion, Insta of Meta again has 2.8 billion, Tik Tok of Tencent has 1.5 billion followers. Most are influencers, followed by ordinary citizens worldwide, without national boundaries. Influencers in a similar age bracket as 60% of the world, most of whom are on social media, influence more than political leaders because of the obvious connection.

The distinction is important. A political leader generally speaks with an identifiable political purpose. A celebrity may not intend to influence policy at all. Yet when a celebrity weighs in on a war, election, social issue, or political controversy, the message can cross national boundaries and reach millions almost instantly.

For younger audiences in particular, familiarity can sometimes create credibility that formal authority cannot. This produces a new form of influence in which attention precedes authority. A person does not necessarily need political office, professional expertise or institutional authority to influence public opinion. They need an audience.

The rise of social-media entrepreneurs and ordinary individuals who have built audiences running into millions demonstrates the scale of this transformation. Some have converted digital popularity into substantial commercial success,

international recognition, and access to elite platforms that would have been unimaginable through traditional media.

Algorithms reinforce this process: popular content attracts more engagement, which generates greater visibility, which attracts more followers, which produces even more engagement. It becomes a self-reinforcing cycle of visibility, followers, engagement, algorithmic amplification, greater visibility, and, of course, relevance and revenue. This is why an individual influencer can become an unexpected participant in national and international information contests.

The Convergence: The Real Weapon Is the Ecosystem. These five categories should not, however, be viewed as isolated actors. The real power of social-media weaponisation lies in their interaction. A state can initiate a narrative, a political party can appropriate it, an influencer can popularise it, a commercial platform can algorithmically amplify it, an ordinary user can reproduce it millions of times. At that point, identifying the original source may become almost irrelevant. This creates the most important characteristic of the modern information environment. The convergence of interests among actors who may have entirely different motivations.

Therefore, the central question in the age of social-media weaponisation should not simply be as to "Who created this information?" It should also be as to "Who amplified it, why was it amplified, who benefited from the amplification, and how did the algorithm transform a message into influence?" and that is where the responsibility and accountability should be borne by the states.

That is where the true battlefield of Information Warfare lies, which is not merely in the creation of information, but in the competition to control its reach, interpretation, and behavioural consequences.

India: A Particularly Fertile Cognitive Battlespace

Indian vulnerability comes from demography and connectivity. Both of which should be the dividends however. The combination of a huge young population that is connected with smartphones and inexpensive data are most exploitable due to the impressionable age, energy, aspirations for quick results and a detachment from the older generations of political and other leadership of the country. It is not unique to India but the numbers are.

The vulnerability gets entrenched and magnified also because India has moved into the social-media age without fully transforming its information-security architecture. India continues to struggle with old, archaic structures and a political class steeped in Cold War legacy media systems.

Whereas the young Indians, more than 600 million, want responsive and agile systems and structures as they perceive exist all across the world. The country is challenged to bring together diverse entities for equitable growth. The diversity that was celebrated as a strength has also been exploited for political machinations. Diversity in language, religion, region, caste, class, political identity, and historical grievances has become an exploitable fault line. In an environment of a vociferous and active political discourse, this has exposed India to exploitation by internal and external inimical forces.

India's Social Media Reach: A Strategic Vulnerability.³³ India's scale of social-media adoption makes it an exceptionally important information environment and, consequently, a potentially significant battlespace for Information Warfare. India is now one of the world's largest markets for virtually every major digital platform.

According to the latest available data, India had approximately 500 million social-media user identities at the end of 2025. Instagram alone had an estimated 481 million users, making India its largest national audience. YouTube had approximately 500 million users, while Facebook had about 403 million. Snapchat had approximately 213 million users, and LinkedIn reported around 170 million members in India. X had a much smaller estimated advertising reach of about 22 million users.

Platform	Approximate users/reach in India
Instagram	481 million
YouTube	500 million
Facebook	403 million
Snapchat	213 million
LinkedIn	170 million members
X	~22 million

The scale is extraordinary. India had approximately 1.03 billion internet users at the end of 2025, and around 500 million social-media user identities. Reuters, citing industry data, similarly reported approximately 500 million unique social-media users in India and noted that Instagram and YouTube each had audiences approaching 500 million.

The significance goes beyond the numbers. India's virtually entire young population is deeply embedded in the digital information ecosystem, making social media an increasingly important source of news, entertainment, political messaging, social interaction and identity formation. A 2026 Reuters report, citing research on Indian digital consumption, estimated that Indians spend about 3.2 hours a day on social-media applications.

This represents a profound transformation in the country's information environment. The centre of gravity of public communication is progressively moving from newspapers, television and official communication channels to smartphones, social-media platforms and algorithmically curated feeds.

For Information Warfare, the implication is significant. A message no longer needs access to a television studio, newspaper newsroom or government broadcasting network to reach millions of Indians. It needs only a smartphone, an audience and an algorithm capable of amplifying it.

India's enormous digital audience therefore represents both an opportunity and a vulnerability. The same platforms that enable democratic participation, economic activity and rapid dissemination of information can also be exploited for disinformation, psychological operations, polarisation, political influence, mobilisation and the amplification of hostile narratives.

The challenge, therefore, is not to restrict social media, but to ensure India's information ecosystem is resilient enough to distinguish influence from manipulation, legitimate dissent from coordinated deception, and organic public sentiment from artificially amplified narratives. If one generation receives most of its understanding of the world through algorithms, whoever influences those algorithms possesses enormous strategic power.

India doesn't control the algorithmic processes. Those earning billions control them, and they are not all based in India.

The Strategic Problem: India Does Not Control the Battlespace

As discussed earlier, India is a major digital society, but it does not control most of the global platforms through which its citizens communicate, consume information, and increasingly conduct

their social, economic, and political lives. The paradox is striking. India possesses enormous digital scale, yet has limited control over much of the technological architecture that mediates that scale.

Most major social-media platforms operating in India are owned and controlled by foreign corporations. While these platforms must comply with Indian laws and regulations in many areas, key elements of the digital ecosystem remain largely outside Indian ownership and control. These include algorithms, recommendation engines, data architectures, content-moderation systems, advertising mechanisms, platform policies, account controls, visibility rules and the technical infrastructure that determines how information becomes viral.

This creates a new form of strategic asymmetry. India provides the users, data, attention and enormous commercial market, while many of the companies that mediate this ecosystem retain substantial control over the technology and architecture through which that value is generated.

The issue therefore goes beyond social media. Technological dependency itself can become a source of strategic leverage. Satellite communications, cloud computing, undersea cables, data centres, search engines, semiconductor supply chains, social-media platforms and increasingly Artificial Intelligence systems are no longer merely commercial assets. When a country depends on foreign-controlled technological infrastructure for critical functions, that infrastructure can take on geopolitical and strategic significance.

Strategic Dependence is Vulnerability: The Starlink Example.

The growing importance of satellite-based communications illustrates this well. Starlink is a highly capable communications architecture, with applications ranging from civilian connectivity

and business communications to emergency services and military operations.

The Russia-Ukraine war demonstrates the strategic significance of such infrastructure. Satellite communications became a key part of Ukraine's wartime connectivity, while public controversies over the availability and potential restriction of Starlink services highlighted a fundamental reality. There came a point that Elon Musk threatened Ukraine with shutting down of star link services as Ukraine advanced into Russian territory in July 2025.³⁴ When critical communications infrastructure is privately owned and controlled outside the country that depends on it, decisions made elsewhere can constrain strategic autonomy.

The lesson is not that any particular technology is inherently unsafe, nor that every communication transmitted through a foreign-controlled system is necessarily compromised. The deeper lesson is one of dependency and assured access.

The issue of concern is that a foreign controlled technology may be available today but restricted tomorrow, a commercial relationship may exist today but change with circumstances a company's policy may remain stable in peace but change during crisis and legal commitment may provide assurance but cannot eliminate strategic uncertainty. These real-world challenges are not new to India, which has faced them in various crises and wars.

Strategic vulnerabilities are therefore not static. They evolve with technology, ownership, geopolitical relationships, and crisis circumstances.

Control of Infrastructure Means Control of Leverage. The lesson was visible as early as the First World War. When Britain controlled much of the world's undersea telegraph infrastructure, it could exploit that position to intercept, monitor, and influence the

flow of information. The technology was primitive by today's standards, but the strategic principle remains remarkably relevant. Whoever controls critical information infrastructure gains strategic leverage over those who depend on it.

The contemporary information environment has multiplied this leverage. The infrastructure is now vastly more sophisticated and interconnected. Information flows through telecommunications networks, undersea cables, satellites, cloud platforms, data centres, search engines, social-media platforms and AI-enabled systems. Control over any critical node can potentially influence the availability, speed, visibility or integrity of information.

India therefore faces a strategic dilemma. It is one of the world's largest digital markets and possesses enormous human and technological potential. Yet much of the architecture through which its citizens communicate and consume information remains dependent upon technologies, platforms and infrastructure developed or controlled outside the country.

This does not mean that India is powerless. India has considerable regulatory, technological and market leverage. It can establish laws, impose compliance requirements, develop indigenous capabilities and shape the behaviour of companies operating within its jurisdiction. But regulatory control is not the same as technological sovereignty.

This distinction matters especially in the context of Information Warfare. A democratic state must balance national security with freedom of expression, privacy, individual rights, judicial oversight and democratic accountability. It cannot simply exercise unrestricted control over information flows. More authoritarian systems may impose much tighter control over platforms, data and communications infrastructure.

However, India cannot and should not seek to replicate such models. And therefore, the challenge is more demanding: how does a democratic India build strategic resilience in an information environment whose critical infrastructure it does not fully control?

The answer cannot lie merely in regulating social-media content after it has gone viral. By then, the cognitive effect may already have occurred. India needs to progressively build technological capacity, indigenous platforms and infrastructure, data resilience, assured communications, algorithmic understanding, cyber capability and information literacy, while retaining the democratic principles that distinguish an open society.

The objective should not be to control the information space in the authoritarian sense. It should ensure that India is not strategically dependent on those who control it. That is the real strategic problem. India has the audience, but does not yet control enough of the architecture through which that audience is influenced.

India's Problem in Managing Social Media Space: The Political-Class and Institutional

Like most democracies, India inherited political and institutional structures designed for an information environment fundamentally different from today's. Information once moved relatively slowly, through identifiable institutions and established channels. Governments issued statements, officials conducted press briefings, newspapers and television channels interpreted the information, and citizens consumed it. That information hierarchy has now been disrupted.

Information has outpaced institutions. Political leaders, including the Prime Minister of India and others, have increasingly

adapted to this environment and use social-media platforms to communicate directly with citizens and the world. Yet the government's institutional machinery has not always evolved at the same pace. The experience of Operation Sindoor offers an instructive case of this challenge.

After the escalation between India and Pakistan in May 2025, multiple actors and channels shaped communication about the cessation of hostilities. The Pakistani Director General of Military Operations communicated with his Indian counterpart, and subsequent developments were publicly announced in a rapidly evolving information environment. The episode demonstrated how quickly an external political actor could enter the information space and shape the international narrative. President Donald Trump publicly announced the cessation of hostilities on social media, creating an immediate global narrative around the development.³⁵

Whatever the merits or circumstances of the diplomatic communication, the larger lesson is that, in today's information environment, whoever communicates first can gain disproportionate influence over how an event is interpreted.

The operational achievement of compelling an adversary to seek an end to hostilities can be overshadowed if the narrative around it is defined elsewhere. Once a particular interpretation becomes established in the public mind, subsequent official clarification often struggles to displace it. This was not simply a communications problem. It is an institutional problem in India.

From the Information Hierarchy to the Information Network. The traditional model of government communication was always relatively linear. From Government → Press Briefing → Newspaper/Television → Public. That model has now been

fundamentally disrupted. The contemporary model increasingly looks like:

Event → Smartphone → Social Media → Influencer/Network
→ Algorithmic Amplification → Public → Television/Legacy
Media → Government Response

An individual with a smartphone can record an event and upload it within seconds. An influencer can amplify it to millions. Algorithms can distribute it to audiences far beyond the original location. Television channels may then pick up the social-media narrative, after which the government may find itself responding to a story that it did not originate and does not control.

The gatekeepers have multiplied and the information hierarchy has flattened. The consequence is profound. Governments can no longer assume that they will be the primary source of information about an event simply because they are the legitimate authority. Authority and information dominance are no longer synonymous. More importantly, governments often respond to a narrative only after it has already shaped public perception.

The Democratic Advantage is also Vulnerability. This transformation is not entirely negative. In fact, social media has created an unprecedented degree of citizen empowerment and institutional accountability. A pothole ignored for months can become a viral video and attract immediate administrative attention. Citizens can instantly expose poor public services. Social media can bring influential individuals' misconduct into public view. Citizens can document public officials' absence or negligence and, in some cases, trigger rapid government action. This is one of social media's great strengths in a democracy. It creates a direct feedback mechanism between citizen → government, bypassing layers of bureaucracy and traditional media.

The same mechanism, however, becomes a vulnerability during crisis, conflict, and geopolitical competition. The same smartphone, platform, and algorithm can be used by the citizen who exposes a genuine problem and the hostile actor who manufactures a false narrative. And that is a critical dilemma. A democratic government cannot simply suppress information because it is inconvenient. Nor can it respond to every allegation, rumour or manipulated video. Doing so risks amplifying the very content it seeks to counter.

The Speed Asymmetry. The fundamental problem is therefore a speed asymmetry. The adversary operates at the speed of the algorithm while the state often operates at the speed of bureaucracy. A hostile actor can create a narrative in minutes. Verification may take hours. Institutional approval may take longer. A formal government response may therefore arrive after the narrative has already been consumed, interpreted, and emotionally internalised by millions.

In cognitive warfare, this delay can be decisive. The objective of an information operation is often not to establish a permanent falsehood. It may simply create confusion, doubt, anger, or distrust during the critical window when people form their initial perception of an event. Once that perception is established, correcting it becomes much harder.

This is why the conventional distinction between "information" and "communication" is no longer sufficient. States require the institutional ability to detect, verify, contextualise and communicate at the speed of the information environment, particularly during crises.

The Need for Institutional Adaptation. India therefore needs to reform not merely its communication machinery but its institutional architecture for information competition. The objective should not be to create a government-controlled

information environment. Such an approach would conflict with India's democratic character and could undermine public trust.

The objective should be to create a state that is:

- fast enough to communicate before hostile narratives become dominant;
- credible enough to be trusted when it speaks;
- technologically capable enough to detect coordinated manipulation;
- institutionally integrated enough to provide a coherent national response;
- legally restrained enough to protect legitimate freedom of expression; and
- strategically sophisticated enough to distinguish between genuine public criticism, misinformation, disinformation, and deliberate cognitive attacks.

This requires moving from a reactive communication model to a proactive information strategy. Government agencies must be able to communicate verified facts rapidly while still allowing time for authentication when operational security demands it. Military and civilian communication structures need mechanisms to coordinate rapidly during crises. Strategic communications cannot remain an afterthought handled only when an incident becomes public.

Most importantly, the state must learn that silence is not always neutrality. In an information vacuum, somebody else will fill the space. The answer, however, is not to respond to every falsehood. Excessive reaction can itself provide amplification. The more intelligent approach is to identify narratives that have the potential

to cause material harm to national security, public order, institutional credibility or social cohesion, verify the facts, and respond proportionately. The institutional objective should therefore be to detect early, verify quickly, communicate credibly and respond proportionately.

India's challenge is not a lack of information. Information moves faster than its institutions are currently designed to process it. The transformation required is therefore deeper than establishing more social-media handles or issuing faster press releases. It requires a fundamental shift in institutional culture, from communicating after decisions to making communication an integral part of decision-making. In the age of cognitive warfare, the battle may be won or lost in the interval between an event occurring and the public deciding what that event means.

What Should India Do?

India needs to fundamentally rethink how it responds to the information environment. The objective should not be to control information, but to build the institutional, technological and societal resilience required to operate effectively in a flat, instantaneous and contested information space.

In the cognitive domain, delay can be strategically costly. Once a perception takes hold, subsequent facts often struggle to displace it. India therefore needs to move from a predominantly reactive approach to one based on preparedness, resilience, technological capability and credible communication.

Seven broad measures can help build a national response architecture for cognitive warfare.

Create a National Cognitive Security Architecture. The easiest response would be to create yet another government media organisation. That, however, may add another layer rather than

solve the problem. India would be better served by integrating and synchronising existing capabilities across defence, intelligence, cyber security, technology, diplomacy, strategic communications, behavioural sciences, linguistics, Artificial Intelligence and social-media analysis. The purpose should be neither propaganda nor political messaging. It should be to establish a national capability for:

Early Detection → Attribution → Assessment → Decision → Response → Evaluation

Such an architecture should identify emerging narratives, determine whether they are organic or coordinated, assess their potential impact on national security and social cohesion, identify the actors behind them where attribution is possible, and recommend an appropriate response. The architecture should function across the entire spectrum, from peace and competition to crisis and conflict, rather than activating only after a major incident.

Move from Reactive Communication to Narrative Preparedness. Governments often prepare for physical contingencies but remain comparatively unprepared for the information campaigns that accompany them. Many potential narratives, however, are predictable.

India has experienced recurring challenges involving terrorism, communal tension, border incidents, elections, disasters, economic disruptions, military operations and governance failures. Adversaries and domestic opportunists are likely to exploit many of the same fault lines repeatedly. India should therefore build a national repository of predictable narratives and counter-narratives, based on experience and continuous analysis.

For foreseeable contingencies, authorities should have readily available:

- verified factual databases;
- multilingual information packages;
- maps, graphics and visual explainers;
- frequently asked questions;
- trusted subject-matter experts and spokespersons;
- pre-cleared factual material;
- rapid-response communication teams; and
- mechanisms for continuous monitoring and feedback.

Prepared material should not become a rigid script. It should provide a validated factual foundation that can be adapted rapidly to circumstances. This matters because the information environment does not wait for institutional approvals. Prepare before the crisis, adapt during the crisis, and communicate before others capture the narrative.

The objective is not to manufacture a narrative. It is to ensure that the first credible account of an event is available before speculation and manipulation occupy the information vacuum.

Build Indigenous Technological Capability. Strategic autonomy in the cognitive domain ultimately depends upon technological capability. India has demonstrated that it can build and scale major technological ecosystems when government policy, private enterprise and national ambition converge. The rapid expansion of mobile connectivity and the availability of some of the world's most affordable data demonstrate what can be achieved when infrastructure is built at scale. The same ambition needs to be applied to the technologies underpinning the information environment.

India should progressively develop greater strategic autonomy in:

- Artificial Intelligence and large language models;
- cloud and data infrastructure;
- semiconductor manufacturing and supply chains;
- social-media intelligence and analytics;
- deepfake and synthetic-media detection;
- content provenance and authentication;
- secure communications;
- satellite communications;
- cyber security; and
- indigenous digital platforms.

This does not mean attempting to isolate India from global technology ecosystems. Nor is it realistic to recreate every major platform domestically. The objective should instead be to engage globally without becoming strategically dependent.

India should encourage an ecosystem in which Indian companies, start-ups, researchers and institutions can develop technologies suited to India's scale, linguistic diversity, democratic requirements and security environment. Strategic autonomy does not require technological isolation. It requires credible alternatives and assured access.

Regulate Platforms Without Becoming a Censor State. This is perhaps the most delicate requirement. India is a democracy, and its response to cognitive warfare must not undermine the very democratic freedoms that it seeks to protect. Freedom of

expression, legitimate political criticism, independent journalism, and democratic debate must remain protected.

At the same time, an open society cannot become indifferent to coordinated foreign interference, terrorist propaganda, bot networks, impersonation, malicious deepfakes, synthetic-media manipulation, fraud and deliberate campaigns designed to cause societal harm. The distinction must therefore be carefully maintained by regulating harmful behaviour and demanding transparency. The government should not regulate political opinion simply because it is inconvenient.

Platform regulation should focus on areas such as transparency of algorithms and recommendation systems, disclosure of coordinated inauthentic behaviour, provenance of synthetic content, protection of users from manipulation, accountability for illegal content and appropriate mechanisms for independent oversight. The test should be legality, transparency, proportionality and due process.

A democratic cognitive-security architecture will derive its legitimacy not from how much information it can suppress, but from how effectively it can protect citizens while preserving their right to disagree.

Build a National Digital and Cognitive Literacy Mission. Ultimately, the strongest defence may not be regulation or technology. It will be the citizen of India, well informed and aware of the advantages and pitfalls of the social media platforms. India should consider a national digital-literacy and cognitive-resilience mission that begins in schools and universities and extends to government employees, the Armed Forces, media professionals and the wider population. Citizens should be taught how to:

- verify the source of information;

- distinguish evidence from opinion;
- recognise manipulated photographs and videos;
- conduct basic reverse-image verification;
- identify deepfakes and synthetic content;
- understand how recommendation algorithms work;
- recognise emotional and psychological manipulation;
- identify coordinated amplification;
- distinguish satire from misinformation; and
- pause before forwarding emotionally provocative content.

The objective should not be to teach citizens what to believe but to be able to pause, think, fact check and then believe or share. A sceptical but informed citizen is one of the strongest lines of defence against cognitive warfare.

Engage the Influencer Ecosystem. The information environment has fundamentally changed. Governments can no longer communicate effectively only through ministers, bureaucrats, military spokespersons and traditional media.

Millions of citizens, particularly younger audiences, receive much of their information through scientists, academics, educators, doctors, entrepreneurs, athletes, artists, veterans, journalists and regional-language creators. India should therefore develop a broader ecosystem of credible voices.

This must not become an exercise in government-sponsored propaganda or an attempt to control influencers. Such an approach would rapidly destroy credibility but instead, government institutions should create mechanisms through which credible

independent experts can access verified information and provide informed perspectives in their own voices.

Credibility cannot be manufactured overnight. Young audiences are often more likely to listen to individuals whom they perceive as authentic and independent than to official government messaging. The answer is therefore not to replace government communication, but to expand the ecosystem of trusted voices capable of explaining complex issues accurately and credibly. Trust needs time and significant investment, more so when the narratives will be based on existing problems and fault lines which will be real and well known.

Build Societal Resilience, Not Information Control. The ultimate objective of cognitive security should be a resilient society, not a controlled society. Citizens should develop the habit of pausing before believing, verifying before forwarding and questioning before reacting. A resilient citizen does not automatically believe everything the government says. Equally, the citizen does not automatically believe everything that criticises the government.

That distinction is fundamental. The purpose of a democratic cognitive-security strategy is not to tell citizens what to think. It is to ensure that citizens possess sufficient knowledge, critical thinking and information literacy to decide for themselves.

The desired end-state is therefore not an obedient population but a cognitively resilient population but one that can encounter propaganda, misinformation, disinformation, deepfakes and psychological manipulation without being easily deceived or emotionally mobilised. This is the critical difference between democratic cognitive security and authoritarian information control.

Authoritarian systems seek to control what their citizens believe. Democratic systems must build citizens who are difficult to make believe what they have not independently judged to be true. India's answer to cognitive warfare should therefore not be greater control of the information space. It should be greater resilience within the information space.

The strategic objective should be simply to secure the infrastructure, strengthen the institutions, prepare the narrative, protect democratic freedoms, educate the citizen, build trusted voices and make Indian society resilient enough that adversaries cannot easily determine what Indians think, feel or believe.

Aggressive Actions to Dominate the Digital Landscape. Populate Indian content on digital space and social media in a manner that interests youth of the culture and history and the direction that the country as a civilizational force needs to take. These should be based on historical facts with experts involved. Content after due research must be populated by Indian experts and authors. Search engines will show the content most populated, current, and searched for. The experts and youth who understand the functioning of the AI and other models must be engaged. This could be led through a **PMO monitored project**.

Conclusion: From Information Control to the Battle for the Mind

The history of warfare demonstrates that the battle has never been confined to the physical domain. Long before the arrival of the internet, armies and states sought to deceive the adversary, influence populations, undermine morale and shape decisions. What has changed is the speed, scale, precision and reach with which this can now be achieved.

The evolution can therefore be understood as a progression:

Information Warfare → control the information

Psychological Warfare → influence emotions and attitudes

Social-Media Weaponisation → achieve unprecedented scale, speed and targeting

Cognitive Warfare → influence perception, reasoning, judgement and decision-making

Strategic Objective → influence behaviour and ultimately national will

This progression is important because it represents more than a change in terminology. It represents a movement from attempting to control what people know, to influencing how they feel, then to shaping how they interpret reality, make decisions and ultimately behave.

Social media has become the bridge between these domains. It has democratised access to mass communication while simultaneously creating an environment in which states, terrorist organisations, political actors, commercial platforms and individuals can compete for attention and influence. A smartphone can now become a sensor, a broadcasting station, a propaganda tool and, potentially, a weapon of psychological and cognitive influence.

The greatest transformation, however, is not technological. It is cognitive. In the physical battlespace, the objective is generally to destroy, deny, occupy or control. In the cognitive battlespace, the objective may be subtler. It is to alter what an adversary perceives as reality, what it believes to be possible, whom it trusts, what it fears and ultimately what decisions it is willing to take. NATO's emerging cognitive-warfare framework similarly places human

cognition, decision-making and behaviour at the centre of the contest.³⁶

A nation can therefore be defeated without occupying its territory. Its institutions can be weakened without firing a shot. Its social cohesion can be fractured without a conventional attack. Its political will can be eroded by continuously creating doubt, distrust and division. This is what makes cognitive warfare particularly relevant to democracies.

An authoritarian state may attempt to protect itself by controlling information. A democracy cannot and should not take that route. Its strength must instead come from institutional credibility, technological resilience, trusted communication, an informed citizenry and the ability to distinguish legitimate disagreement from deliberate manipulation.

For India, the challenge is especially significant because of its enormous digital population, linguistic and cultural diversity, geopolitical environment, and dependence on global information technologies. India's vulnerability does not stem from its people's inability to resist manipulation. It arises because the information environment is evolving faster than many of the institutions designed to operate within it.

The answer, therefore, is not to control the citizen's mind, but to strengthen it.³⁷ India must learn to operate at the speed of the information environment without sacrificing the values of an open society. It must develop the technological capability to understand the digital battlespace, the institutional agility to respond to emerging threats, the credibility to communicate before hostile narratives dominate, and the societal resilience to withstand manipulation.

The ultimate contest in cognitive warfare is therefore not between information and misinformation alone. It is between trust and distrust, resilience and vulnerability, independent judgement and manipulated perception.

The most important battlefield of the future may not be a physical piece of territory. It may be the space between an event occurring and a society deciding what that event means. And the ultimate objective will remain what it has always been in war, and that is not merely to defeat the adversary's forces, but to influence the adversary's will to act.

In the age of cognitive warfare, however, the route to that objective increasingly runs through information, perception, cognition, decision, and behaviour. Control the information, and you influence what people know; influence emotion, and you shape what they feel; shape cognition, and you influence how they think; influence decisions, and you shape what they do and when you shape behaviour, and ultimately, you can influence national will.

That is, warfare has evolved from controlling information to competing for the human mind. The adversary will seek to enter not through our borders, but through our phones. And they are doing it now, effectively.

References

- 1 <https://power.lowyinstitute.org/countries/india/>,
- 2 <https://www.cnbc.com/2026/06/04/indias-cockroach-cjp-party-what-investors-need-to-know.html>, Priyanka Salve, June 4, 2026
- 3 <https://www.thehindu.com/news/cities/Delhi/with-cjp-getting-millions-of-followers-kejriwal-changes-messaging-style/article71324510.ece>, Nikhil M Babu, August 09, 2026
- 4 <https://www.opindia.com/2026/08/meta-admits-to-being-paid-to-boost-certain-types-of-content-deliberate-content-manipulation-mark-zuckerberg->

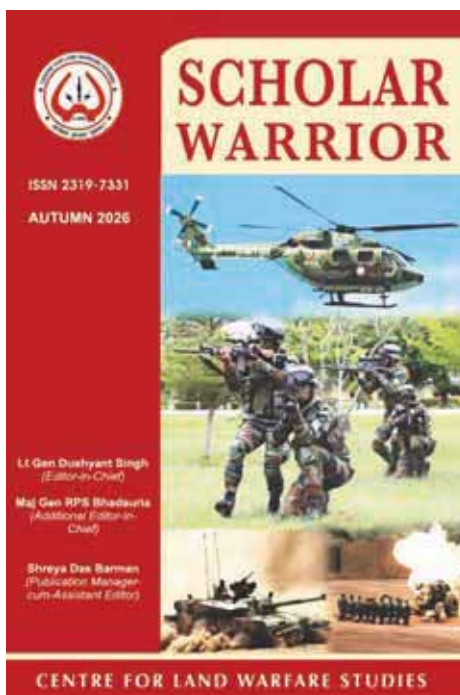
apologises/, Meta admits to being paid to boost certain types of content: How it amounts to an admission of deliberate content manipulation and misuse of Indian laws, Jitin Jain, August 5, 2026

- 5 <https://www.indiatoday.in/india/story/operation-sindoor-brahma-chellaney-india-pak-conflict-mps-delegations-abroad-narrative-2731617-2025-05-28>, Prateek Chakraborty, May 28, 2025
- 6 Sun Tzu. (1910). *The art of war* (L. Giles, Trans.)
- 7 Weatherford, J. (2004). *Genghis Khan and the making of the modern world*. Crown.
- 8 https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=14708&lid=9045, From Propaganda to Algorithms: The Evolution of Cognitive Warfare in the Age of Artificial Intelligence, Azra Shahab, 24 July 2026
- 9 Kautilya. (1956). *Kautilya's Arthashastra* (R. Shamasastri, Trans.). Mysore, India: Government Press. (Original work composed c. 4th century BCE)
- 10 https://www.bbc.co.uk/history/ancient/romans/romanpropaganda_article_01.shtml, The Official Truth: Propaganda in the Roman Empire, By Dr Neil Faulkner, Feb 17, 2011
- 11 https://www.fbcoverup.com/docs/library/2017-12-15-How-Britain-pioneered-cable-cutting-in-World-War-One-by-Gordon-Corera-BBC-News-Dec-15-2017.pdf?utm_source=chatgpt.com, How British Pioneered Cable Cutting in World War One, Gordon Corera, Dec 15, 2017
- 12 https://www.fbcoverup.com/docs/library/2017-12-15-How-Britain-pioneered-cable-cutting-in-World-War-One-by-Gordon-Corera-BBC-News-Dec-15-2017.pdf?utm_source=chatgpt.com, How British Pioneered Cable Cutting in World War One, Gordon Corera, Dec 15, 2017
- 13 <https://journalism.university/media-and-society/evolution-communication-radio-digital-revolution/>, The Evolution of Communication: From Radio to Digital Revolution, January 30, 2026
- 14 <https://www.theguardian.com/world/2026/may/18/iran-threat-internet-cables-strait-hormuz>, How realistic is threat of Iran charging to use internet cables under strait of Hormuz?
- 15 <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/>, Cognitive Warfare: Strengthening and Defending the Mind, April 5, 2023

- 16 <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/>, Cognitive Warfare: Strengthening and Defending the Mind, April 5, 2023
- 17 <https://carnegieendowment.org/research/2025/09/nepal-gen-z-topple-government>, From Streets to Discord: How Nepal's Gen Z Toppled a Government, Amish Raj Mulmi, Sep 24, 2025
- 18 <https://www.reuters.com/world/asia-pacific/bangladeshs-sheikh-hasina-falls-grace-nation-her-father-founded-2024-08-05/>, Bangladesh's Sheikh Hasina falls from grace in nation her father founded, Sudipto Ganguly, August 5, 2024
- 19 <https://www.orfonline.org/expert-speak/national-youth-policy>, National Youth Policy – Will it help India reap the promised demographic dividend? Aug 02, 2023
- 20 <https://www.opindia.com/2026/06/ancient-pakistan-identity-crisis-ancient-indian-history-appropriation/>, 'Ancient Pakistan': Why, after decades of claiming to be Arabs, Turks, Pakistanis suddenly jumped to appropriate ancient Indian history? Shraddha Pandey, June 29, 2026
- 21 <https://datareportal.com/reports/digital-2026-india>
- 22 <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>
- 23 <https://www.pbs.org/newshour/science/false-news-travels-6-times-faster-on-twitter-than-truthful-news>, False news travels 6 times faster on Twitter than truthful news, Mar 9, 2018
- 24 <https://www.ebsco.com/research-starters/communication-and-mass-media/echo-chamber-effect>, Echo Chamber Effect, Bill Kte'pi, 2021
- 25 <https://datareportal.com/global-digital-overview>
- 26 <https://www.searchenginejournal.com/social-media-statistics/480507/>, 134 Social Media Statistics You Need To Know For 2023, Annabelle Nyst, July 14, 2023.
- 27 <https://reutersinstitute.politics.ox.ac.uk/news-creators-influencers/2025/mapping-news-creators-and-influencers-social-and-video-networks>, Mapping news creators and influencers in social and video networks, Nic Newman, Dr Amy Ross Arguedas, Mitali Mukherjee, Dr Richard Fletcher, October 28, 2025

- 28 <https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx>, How Facebook (Meta), X Corp (Twitter), Social Media Make Money From You, Greg McFarlane, May 16, 2026
- 29 <https://timesofindia.indiatimes.com/india/factsheet-farmers-protest-in-numbers/articleshow/87805415.cms>, Factsheet: Farmers' Protests in Numbers, Nov 19, 2012
- 30 <https://warroom.armywarcollege.edu/articles/organized-weaponization-of-social-media/>, Facing A Future with Organized Weaponization of Social Media, Debasis Dash, May 31, 2019
- 31 <https://warroom.armywarcollege.edu/articles/organized-weaponization-of-social-media/>, Facing A Future with Organized Weaponization of Social Media, Debasis Dash, May 31, 2019
- 32 <https://insightful.co.in/2025/06/08/operation-sindoor-exposed-true-color-of-china-and-turkey/>, Operation Sindoor Exposed the Nefarious China-Pakistan-Turkey Nexus, Commander Sandeep Dhawan, June 8, 2025
- 33 <https://www.reuters.com/business/media-telecom/indias-vast-internet-social-media-apps-market-2026-01-29/>, India's vast internet, social media apps market, Reuters, January 29, 2026
- 34 <https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/>, Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia, Joey Roulette, Cassell Bryan-Low and Tom Balmforth, July 25, 2025
- 35 <https://www.hindustantimes.com/india-news/it-didn-t-leak-from-us-ex-cds-hints-pakistan-may-have-leaked-operation-sindoor-ceasefire-details-to-us-101787708795162.html>, 'It didn't leak from us': Ex-CDS hints Pakistan may have leaked Operation Sindoor ceasefire details to US, Abhimanyu Kulkarni, Aug 26, 2026,
- 36 https://www.act.nato.int/article/cognitive-warfare-beyond-military-information-support-operations/?utm_source=chatgpt.com, Cognitive warfare: Beyond military information support operations, NATO Allied Command Transformation, May 9, 2023
- 37 https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full?utm_source=chatgpt.com, Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept, Adlakha-Hutcheon, 2024

SUBSCRIBE NOW



SUBSCRIPTION RATES

IN INDIA

□ Rs.500/- per copy

□ Rs.1000/- Annual Subscription (2 issues)

SAARC COUNTRIES

□ US \$ 15 per copy

OTHER COUNTRIES

□ US \$ 20 per copy

TO SUBSCRIBE SEND YOUR REQUEST TO



Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi - 110010
Tel: +91-11-25691308
• Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com
www.claws.co.in

The next war may not begin with missiles, aircraft or artillery. It may begin with a message on a smartphone.

Warfare is moving beyond the physical battlefield into the human mind—where perceptions can be shaped, beliefs manipulated, emotions triggered, and decisions influenced without a shot being fired. Social media, artificial intelligence, algorithms, deepfakes and ubiquitous connectivity have created a battlespace of unprecedented scale, speed and reach.

This paper traces the evolution from information and psychological warfare to the emerging contest for “Mind Space” and examines how social media is being weaponised to influence societies and national will. Drawing upon historical experience and contemporary developments, it highlights India's growing vulnerability and the urgent need to understand, anticipate, and counter threats in the cognitive domain.

The battle for the mind has already begun. The question is whether India is



Lieutenant General Devendra Pratap Pandey, PVSM, UYSM, AVSM and VSM (Retd), former Commander Chinara Corps and head of the Indian Army's Strategic Communications Division, has extensive experience in Information Warfare, strategic communication and Cognitive Warfare. He has held key appointments in operations, intelligence, strategic communication and

military education, including Director Military Intelligence (Foreign Division), and culminated his military career as Commandant of the Indian Army War College. He was also the first Director General of the Territorial Army. A practitioner and strategic thinker, he has worked extensively on countering radicalisation, shaping narratives, and leveraging digital and social-media platforms in conflict.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributors aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Website: www.claws.co.in

Contact us: landwarfare@gmail.com

