Cognitive Warfare: India's Approach to Influencing Perception and Behaviour

Commander Arun Kumar Yadav[@]

Abstract

Warfare has evolved from conventional kinetic battles to multi-domain, hybrid conflicts where perception, cognition, and narrative dominance are as decisive as physical force. Cognitive warfare—recognised by North Atlantic Treaty Organization as the '6th Operational Domain'—targets human cognition by influencing perceptions, emotions, and decision-making through disinformation, psychological operations, artificial intelligence, and digital platforms. For India, a diverse democracy operating in a complex security environment, cognitive warfare presents both a challenge and an opportunity. Adversaries exploit social fault lines, digital ecosystems, and media vulnerabilities to shape narratives and erode institutional trust. While India has embedded elements of cognitive defence within its information warfare doctrines, gaps remain in unified command structures, technological integration, and resilience mechanisms. This essay analyses the evolving concept of cognitive warfare, assesses India's threat landscape through comparative and critical feature analysis, and proposes a whole-of-government roadmap to strengthen narrative dominance, institutional coordination, technological capability, and societal resilience in the emerging battlespace of the mind.

[@]**Commander Arun Kumar Yadav** was commissioned in the 'Executive Branch' of the Indian Navy and is a 'Navigation and Direction' specialist. He has held various operational, training and staff appointments during his service career. The officer is presently posted at Naval Headquarters.

This is the First Prize winning entry of the USI Gold Medal Essay Competition 2025.

Journal of the United Service Institution of India, Vol. CLVI, No. 643, January-March 2026.

Introduction

Warfare in recent times has undergone a profound transformation as compared to the old days of conventional, kinetic battles fought primarily on land, sea, and air. Earlier, military victory was defined by territorial control, numerical strength, and physical destruction of the enemy's forces. Today, however, conflicts are increasingly multi-domain and hybrid, blending traditional combat with cyber operations, information warfare, economic coercion, and cognitive influence campaigns. Modern warfare prioritises speed, precision, and perception—where disrupting an adversary's decision-making, controlling narratives, and influencing public opinion can be as decisive as battlefield victories. The rise of digital technologies, social media, Artificial Intelligence (AI), and long-range precision systems has blurred the lines between war and peace, state and non-state actors, and frontlines and home fronts. This shift reflects a transition from wars of attrition to wars of cognition, where the decisive battles are often invisible and fought in the information and psychological domains.

Towards addressing the changing concepts of modern warfare, the Indian Armed Forces have so far been able to maintain with the global curve and address the security threats posed by its adversaries. However, being the world's largest democracy, India faces a complex security environment. Adversaries have sought to exploit India's social, political, and cultural diversities through disinformation campaigns, psychological operations, and digital influence strategies. Therefore, cognitive warfare is emerging as both a challenge and an opportunity.

While the concept of attacking the mind is ancient[1], the term 'Cognitive Warfare' emerged only in recent years. It appeared in the North Atlantic Treaty Organization (NATO) reports in 2020.[2] The terms and concept of 'National Cognitive Security' and 'Mind Superiority' have been mentioned in Chinese doctrines.[3] It represents an evolution beyond psychological or information warfare, targeting human cognition more deeply using advanced technologies and cross-domain strategies. It extends beyond traditional information warfare, aiming not merely to control the information space but to shape the adversary's cognition itself.

Cognitive warfare has gained increasing prominence in both global and Indian strategic discourse. NATO's recognition of the concept as the '6th Operational Domain' highlights its centrality in shaping future conflict scenarios. Unlike traditional forms of information warfare that focus on information infrastructure, cognitive warfare directly targets the human mind by manipulating perceptions, emotions, and decision making. This battlefield of ideas and narratives has blurred the boundaries between war and peace, compelling states to develop resilience against manipulation as well as their own capabilities to project influence.

For India, a nation navigating a complex security environment, cognitive warfare presents both an existential challenge and a unique opportunity. This essay analyses India's approach to cognitive warfare, situating it within broader global trends.

Cognitive Warfare

Defining Cognitive Warfare. The term cognitive warfare has not been clearly defined, except in NATO Allied Command Transformation 2023, wherein it has been defined as "Activities conducted in synchronisation with other instruments of power, to affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary".[4]

Absence of Formal Doctrine. It is essential to underscore that while there are articles and analysis reports from Indian think tanks (e.g., Manohar Parrikar Institute for Defence Studies and Analyses) discussing cognitive warfare, the Indian Government and the Indian Armed Forces have not yet published a formal doctrinal or policy document that explicitly defines cognitive warfare in the same way that NATO has.

Nature of Cognitive Warfare. Cognitive warfare represents the manipulation of perceptions, behaviours, and decision-making processes to achieve strategic objectives without kinetic force. It blends disinformation, propaganda and psychological operations with advanced technologies such as AI, social media platforms, and big data analytics.

Types of Cognitive Warfare. Like any other warfare, cognitive warfare, which is often described as the 'Battle for the human mind', has both offensive and defensive approaches. While

offensive cognitive warfare is concerned with manipulating the adversary's mind, defensive cognitive warfare seeks to secure one's own cognitive domain by anticipating, exposing, and neutralising hostile influence efforts. The key differences in the approaches for these two types of cognitive warfare are as summarised below:

Dimension	Offensive Cognitive Warfare	Defensive Cognitive Warfare
Aim	Manipulate adversary's cognition to influence decisions and strategic behaviour	Protect and reinforce one's own cognitive re silience and clarity
Tactics Employed	Reflexive control, psychological pressure, narrative shaping, legal and media manipulation	Pre-bunking, AI detection, adaptive doctrines, coordinated societal defences
Ethical Framing	Often exploit ambiguity and lack of accountability	Bound by ethical and legal norms; focused on protection, not coercion
Exiting Policy and Doctrines	Russia's doctrine of reflexive control, and China's 'Three Warfares'[5] strategy	Democracies and alliances (e.g., NATO) focusing on transparency, media literacy, and awareness[6]

Table 1: Comparative Dimensions of Offensive and Defensive Cognitive Warfare

Cognitive Warfare: Components and Tactics. There are numerous examples from history where attacks were directed at the information systems and the mindset of an adversary's general public. However, cognitive warfare is a relatively new term that manifests in psychological, informational, technological, cultural, and narrative forms. It blends traditional information and propaganda warfare with cutting-edge tools like AI, social media manipulation, and neuroscience to influence thought and behaviour. The common tactics used for waging cognitive warfare during wartime, peacetime, and no-war-no-peace situations have been covered below:

- **Wartime Cognitive Warfare Tactics**. During open conflicts, cognitive warfare is integrated with kinetic operations to weaken enemy morale, disrupt decision making, and manipulate perceptions. Some of the commonly used cognitive warfare tactics used in wartime are mentioned below:
  - **Psychological Operations (PSYOPS)**. Propaganda, false narratives, and misinformation targeting soldiers and civilian populations to erode willpower.
  - **Deception (Maskirovka, Camouflage, Feints)**. Creating false perceptions of troop movements, strength, or intentions.
  - **Information Denial**. Censoring, jamming, or manipulating communication channels to restrict adversary's situational awareness.
  - **Shock and Awe (Perception of Overwhelming Force)**. Demonstrating overwhelming firepower to psychologically break resistance.
  - **Exploitation of Civilian Media**. Disseminating images and stories of suffering, casualties, or destruction to reduce public support for the war.
  - **Targeting Leadership Perception**. Spreading disinformation to confuse enemy decision-makers and weaken command cohesion.
- **Peacetime Cognitive Warfare Tactics.** In peacetime, the aim is long-term shaping of perceptions, influencing societies, and preparing the ground for future advantage without overt conflict. Some of the commonly used cognitive warfare tactics used in peacetime are mentioned below:
  - **Narrative Building**. Promoting national ideology, history, or 'Civilisational' values through media, academia, and diplomacy.
  - **Disinformation Campaigns**. Spreading subtle propaganda to polarise societies, erode trust in institutions, and manipulate foreign audiences.

- **Cultural Diplomacy and Soft Power**. Using movies, literature, education exchanges, and cultural symbols to create favourable perceptions.

- **Economic Influence as Cognitive Tool**. Framing investments, loans, or trade dependency as benevolence, shaping psychological loyalty.

- **Digital Manipulation**. Social media bots, trolls, and influence campaigns to mould opinions and attitudes gradually.

- **Civilian Targeting**. Indoctrination, psychological conditioning, or selective exposure of populations to controlled narratives.

- **No-War-No-Peace (Grey Zone) Cognitive Warfare Tactics**. In ambiguous situations (e.g., border tensions, insurgencies, hybrid warfare), the cognitive domain becomes a decisive battlefield to blur lines between war and peace. Some of the commonly used cognitive warfare tactics used in no-war-no-peace situations are mentioned below:

  - **Ambiguity Creation**. Preventing clear attribution of hostile acts (cyberattacks, sabotage, fake news), confusing both governments and public.

  - **Rumour Propagation**. Fuelling mistrust and suspicion in contested regions or between allies.

  - **Hybrid Propaganda**. Combining military posturing with information campaigns to psychologically intimidate without escalation.

  - **Legitimacy Warfare**. Questioning the legitimacy of governments or movements, influencing international opinion and legal narratives.

  - **Information Saturation**. Flooding with contradictory narratives to create confusion ('Firehose of Falsehood' tactic).

  - **Exploitation of Local Fault Lines**. Amplifying ethnic, religious, or political divisions to weaken the target from within.

India's Strategic Threat Landscape: Cognitive Warfare

Threat Analysis. In the Indian context, cognitive warfare intersects with a long-standing history of information influence and perception management. Analysis of the cognitive threat landscape would involve considering following aspects:

- India has been a consistent target of disinformation campaigns, particularly from Pakistan, where its military's media wing Inter-Services Public Relations (ISPR) has deployed propaganda to undermine New Delhi's legitimacy in Kashmir and to exploit communal fault lines.[7] Pakistan, through its ISPR, has perfected disinformation campaigns targeting Kashmir and India's democratic institutions.[8]

- Chinese influence operations, by contrast, are more subtle, relying on economic leverage, media partnerships, and the 'Three Warfares' doctrine to build pro-China narratives in South Asia.[9]

- India's democratic nature makes it both resilient and vulnerable in the cognitive sphere. On one hand, pluralistic media environment provides room for diverse narratives; on the other, it creates space for adversarial actors to seed misinformation and polarising content.[10]

- Non-state actors exploit digital platforms for radicalisation. Emerging technologies like AI-driven deepfakes and bot networks multiply the scale of these threats.[11]

- India's fragmented cyber and media regulatory mechanisms are inadequate in the face of AI-driven threats such as deepfakes and bot amplification.[12]

Comparative Capability Analysis. It is understood that there are no permanent friends and enemies in global geopolitics and the domain of cognitive warfare lies beyond the kinetic warfare, which provides enough latitude to potential adversaries to maintain deniability. Therefore, the threat in the form of cognitive warfare can be posed by any country. However, towards analysing the cognitive warfare capability of India, a comparative analysis with

present day adversaries has been undertaken and the outcome is as tabulated below:

Country	Strategic Objectives	Doctrinal Basis	Key Tools and Methods	References
China	Shape global opinion on Indo-Pacific disputes, delegitimise adversaries, expand the Communist Party of China's ideological influence.	'Three Warfares' doctrine (psychological, media, legal warfare) integrated into People's Liberation Army strategy.	State-controlled media (Xinhua News Agency, China Global Television Network), cyber ops, lawfare, Confucius Institutes, influence ops on social media.	Jamestown Foundation (2016)[13] ; Wilson Centre (2017).[14]
Pakistan	Destabilise Indian democracy, internationalise Kashmir issue, erode India's legitimacy.	ISPR-led information warfare targeting India, especially Kashmir.	Disinformation campaigns, fake social media accounts, jihadist propaganda networks, diaspora mobilisation.	Strategic Studies Institute, National Defence University Pakistan (2021)[15] ; Observer Research Foundation (2021).[16]
India	Defend democracy, secure digital space, counter adversarial narratives, project Indian soft power globally.	Joint Doctrine of Armed Forces (2017); Computer Emergency Response Team (CERT)-In advisories; Election Commission of India (ECI) social media guidelines; Digital Personal Data Protection Act (2023).	Narrative-building via soft power (Bollywood, yoga, diaspora), cybersecurity mechanisms, counter-disinformation task forces, AI/natural language processing projects like Bhashini.	Ministry of Defence (MoD) (2017)[17] ; Ministry of Electronics and Information Technology (MeitY) (2023)[18] ; Manohar Parrikar Institute for Defence Studies and Analyses (2023).[19]

Table 2: Comparative Analysis of Cognitive Warfare Capabilities

Critical Feature Analysis (CFA)

Critical Features. Development of India's approach to Cognitive warfare entails analysis of the critical features, i.e., Critical Capabilities (CCs), Critical Requirements (CRs), and Critical Vulnerabilities (CVs). The CCs are those capabilities which could contribute towards achievement of the objective. The CRs are those resources, means, or conditions which are necessary pre-

requisites in order to generate or apply 'Critical Capability'. CVs are those critical weaknesses or their elements that are especially vulnerable to enemy action.

Outcome of CFA. The outcome of the analysis is tabulated below:

Critical Feature	Concept	Ways and Means
CCs or key pillars of India's cognitive warfare approach	Strategic Narrative Construction.	Use of *'Vishwa Guru'* (Global Guide)[20] and 'Digital India' narratives. Projection of India as the world's largest democracy.
	Information Dominance. Research and Analysis through centres dealing with national and international information towards preventing propagation of disinformation by adversary.	Following centres are likely to play a key role, particularly with respect to maritime information: ■ Information Fusion Centre–Indian Ocean Region (IFC-IOR)[21] through collaboration with partner countries ■ National Maritime Domain Awareness Centre[22] through collaboration between national maritime stakeholders.
	Augmentation of cyber infrastructure.	Establishment of Defence Cyber Agency (2019).
	Intelligence and Surveillance[23]	National intelligence grid integration, AI-enabled open-source intelligence for counter-terror narratives, Use of Defence Research and Development Organisation's (DRDO) cyber labs for threat anticipation.
	Cultural and Civilisational Leverage[24]	Through following soft power assets: ■ Use of Yoga Day at the United Nations ■ Bollywood ■ Indian diaspora.
	Presenting an Indian perspective on global news	Indian-owned, based, and operated international broadcasters and media houses.
CRs	Robust Legal-Policy Framework	Formulation of following doctrines or strategies: ■ Unified cognitive warfare doctrine ■ Comprehensive information warfare strategy.
	Technological Infrastructure[25]	AI-based fact-checking (Press Information Bureau [PIB], MyGov); Indigenous 5G rollout to secure communications.

Critical Feature	Concept	Ways and Means
	Skilled Human Capital	Academic programs at Indian Institutes of Technology, Indian Institutes of Management, or other academic institutions on AI and psychology; Defence PSYOPS units.
	Public Resilience Mechanisms	Digital literacy campaigns (G20 Cyber Safety for Children); Fact-check initiatives (PIB Fact Check, BOOM Live).
	Strategic Alliances	Bilateral and multilateral partnership on disinformation countermeasures. Institutions and centres like IFC-IOR can play a significant role.
	Funding and Research and Development	DRDO's AI and robotics projects; Digital India Innovation Fund; Startup India for deep-tech in cognitive tools.
	Usage of Social Media platforms	Indigenously developed social media platforms of international standards.
CVs	Fragmented Institutional Response	Cyber warfare spread across the domains of MoD, Ministry of Home Affairs (MHA), MeitY, Ministry of External Affairs (MEA) without a unified command and control set-up.
	Digital Ecosystem Dependency	Reliance on Meta, X (Twitter), YouTube for narratives; vulnerability to foreign platform policies and manipulation.
	Internal Societal Faultline	Exploitation of communal tensions, caste politics, separatist sentiments (e.g., Khalistan online propaganda).[26]
	Cybersecurity Gaps	Exposure to deepfakes, bot-driven disinformation, and ransomware targeting political narratives (e.g., 2021 power grid cyberattack linked to China).

Table 3: Critical Factor Analysis (India's Approach to Cognitive Warfare)

India's Cognitive Warfare Strategy

Current Landscape. It is worth noting that some of the critical capability gaps have already been addressed as a part of India's cognitive warfare strategy, embedded within its doctrines of information warfare and perception management. The various measures instituted as a part of India's cognitive warfare strategy and gaps observed have been enumerated in subsequent paragraphs.

Doctrinal Level. At the doctrinal level, the Indian Armed Forces have increasingly acknowledged the importance of cognitive influence as under:

- The Joint Doctrine of the Indian Armed Forces (2017) explicitly recognises information as a warfighting domain and stresses the need for dominance in PSYOPS and perception management.[27] However, analysts note that implementation has been slow, with the Indian Armed Forces yet to operationalise a dedicated Information Operations Command akin to those in the United States or China.[28]

- Joint Doctrine for 'Multi-Domain Operations' has been launched recently and maps the way forward for synergised employment of the Indian Armed Forces across land, sea, air, space, cyber, and cognitive domains towards strengthening jointness amongst them and ensuring future readiness.[29]

Participation of Civilian Institutions. Civilian institutions, particularly the ECI and CERT-In, have attempted to fill these gaps by issuing social media guidelines, countering deepfake threats, and conducting awareness campaigns. These reflect India's recognition that cognitive warfare is as much a governance challenge as it is a military one.

Inclusive Digital AI Initiatives. MeitY has launched initiatives such as the IndiaAI Mission and Bhashini (an AI-powered language platform) to ensure inclusivity in India's digital ecosystem.[30] These programs are designed to strengthen India's narrative projection by enabling content creation in regional languages and enhancing digital literacy. It has been acknowledged by some of the analysts that such measures are critical not only for digital inclusion but also for insulating citizens from disinformation campaigns that exploit linguistic diversity.[31]

Recommended Roadmap: Augmenting India's Cognitive Warfare Capabilities

Methodology Adopted. Formulation of way forward for augmentation of cognitive warfare capabilities has primarily been derived from the threat assessment and critical features analyses. The aim is to exploit the CCs to their potential, protect the CVs,

and meet the CRs which are pre-requisites for the CCs to be applied against the adversary.

Whole-of-Government Approach. The evolving nature of cognitive warfare necessitates a whole-of-government approach, as the challenge extends far beyond the mandate of the armed forces alone.[32] Cognitive warfare targets the perceptions, behaviours, and decision making of individuals and societies, exploiting vulnerabilities in domains such as media, education, technology, and governance. India, with its diverse socio-political fabric and complex security environment, requires a coordinated framework that integrates the efforts of defence, intelligence, cyber, information, diplomatic, and economic institutions. Thus, a whole-of-government approach is essential to protect India's information ecosystem while leveraging cognitive tools for influence in the regional and global arena.

Centralised Command and Control. Ministries like MoD, MEA, MHA, MeitY as well as agencies regulating social media, education, and strategic communications must operate in synergy to counter disinformation, strengthen societal resilience, and project India's narrative globally. A fragmented or siloed response risks leaving gaps that adversaries can exploit through propaganda, misinformation, and perception management campaigns. Thus, a mechanism with centralised command is required to create a unified national cognitive strategy.

Capability Development. Capability development for cognitive warfare involves building the tools, structures, and expertise necessary to shape, disrupt, or defend the perceptions, beliefs, decision making, and behaviour of adversaries, while protecting one's own population and forces. Since cognitive warfare sits at the intersection of military, psychological, technological, and societal domains, capability development must be multi-layered and interdisciplinary. The key components of the cognitive warfare capability development are enumerated below:

- **Human Capital Development**.
  - **Training and Education**. Specialised training for military, intelligence, and diplomatic personnel PSYOPS, influence operations, behavioural science, and narrative warfare. Cross-training with academia in neuroscience,

psychology, behavioural economics, sociology, and anthropology.

- **Specialised Units**. Creation of dedicated cognitive warfare units (like NATO's Innovation Hub[33] or China's Strategic Support Force[34]) that integrate information operations, AI-driven propaganda, and cyber-psychological warfare.
- **Language and Cultural Expertise**. Developing linguists and cultural experts to tailor narratives for different populations.

- **Technological Tools and Infrastructure**.
  - **AI and Big Data**. Tools for monitoring social media sentiment, detecting disinformation, and predicting audience reactions.
  - **Cognitive Persuasion Systems**. Automated systems for generating and disseminating persuasive narratives.
  - **Neurocognitive Technologies**. Brain-computer interfaces, neuro-monitoring, and cognitive load assessment for understanding vulnerabilities in perception and decision making.
  - **Cyber-Cognitive Platforms**. Integration of cyber operations with psychological targeting (e.g., hacking and disinformation release).
  - **Virtual Reality and Deepfake Tech**. Development of immersive and deceptive environments for influence campaigns.

- **Information and Narrative Dominance**.
  - **Narrative Development Cells**. Units tasked with creating coherent national and military narratives for domestic and international audiences.
  - **Strategic Communication**. Coordinated messaging across diplomacy, defence, intelligence, and media.
  - **Control of Information Ecosystem**. Ability to counter adversary propaganda through fact-checking, debunking, and alternative narratives.

- **Institutional and Policy Framework**.
  - **Doctrine and Policy Integration**. Incorporating cognitive warfare into military doctrines, national security strategies, and hybrid warfare frameworks.
  - **Civil-Military Fusion**. Partnerships between defence, academia, tech industry, and media for developing cognitive warfare resilience.
  - **Legal and Ethical Frameworks**. Establishing guidelines for offensive and defensive cognitive operations within international law and human rights norms.
- **Defensive Capabilities (Cognitive Security).**
  - **Resilience Building**. Public education programs to enhance media literacy and critical thinking.
  - **Counter-Disinformation Units**. Dedicated agencies to track, expose, and neutralise hostile influence campaigns.
  - **Psychological Defence**. Support structures to counteract stress, fear, or manipulation among military personnel and civilians.
- **Research and Innovation.**
  - **Academic Partnerships**. Investment in brain sciences, human-machine interaction, AI ethics, and cognitive resilience.
  - **Red-Teaming and Wargaming**. Simulations of adversary cognitive attacks to stress-test national systems.
  - **Cross-Domain Integration**. Merging cognitive warfare with cyber, space, and electronic warfare for multi-domain operations.

Conclusion

Cognitive warfare represents the '6th Battlespace' after land, sea, air, cyber, and space. While there has not been a global focus on the cognitive warfare, it is an increasingly relevant domain for

India, given its contested strategic environment with China and Pakistan, both of which deploy sophisticated information operations.[35] Therefore, the requirement of the hour is to think beyond the kinetic warfare towards maintaining an upper-hand over the adversary in the domain of cognitive warfare in addition to other domains of warfare. For India, the primary objective is to defend its democratic values against external manipulation and to develop credible offensive capabilities. By integrating military doctrines, civilian frameworks, and technological innovation, India can secure a balanced cognitive posture that strengthens both resilience and influence in the global order.[36]

Endnotes

[1] Darshan Gajjar, "Cognitive Warfare", *The Geostrata*, 11 Mar 2023, accessed 12 Aug 2025, https://www.thegeostrata.com/post/cognitive-warfare

[2] "Cognitive Warfare: Beyond Military Information Support Operations", *NATO Allied Command Transformation (ACT)*, 09 May 2023, accessed 12 Aug 2025, https://www.act.nato.int/article/cognitive-warfare-beyond-military-information-support-operations/

[3] Abhishek Kumar Darbey, "China and Cognitive Warfare: An Overview", *Manohar Parrikar Institute for Defence Studies and Analyses (IDSA),* 27 Sep 2024, accessed 12 Aug 2025, https://www.idsa.in/publisher/issue-brief/china-and-cognitive-warfare-an-overview

[4] Christoph Deppe and Gary S Schaal, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept", *National Institutes of Health (NIH)*, 01 Nov 2024, accessed 13 Aug 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/

[5] Sukhbir Kaur Minhas,"Cognitive Warfare: Key Aspects" (2022), *Manohar Parrikar Institute for Defence Studies and Analyses (IDSA),* 18 Aug 2025, accessed 13 Aug 2025, https://idsa.in/publisher/issuebrief/cognitive-warfare-key-aspects.

[6] "Cognitive Warfare: A New Domain of Competition" (2021), *NATO Allied Command Transformation (ACT),* accessed 13 Aug 2025, https://www.act.nato.int

[7] Soumya Awasthi, "Pakistan's Information Warfare: Strategic Implications and India's Response", *ORF Issue Brief*, 22 Oct 2025, accessed 13 Aug 2025, https://www.orfonline.org/research/pakistan-s-information-warfare-strategic-implications-and-india-s-response

[8] Ibid

[9] Elsa Kania, "China's Strategic Thinking on the Three Warfares" (2016), *Jamestown Foundation*, 22 Oct 2016, accessed 14 Aug 2025, https://jamestown.org/the-plas-latest-strategic-thinking-on-the-three-warfares/

[10] Minhas, "Cognitive Warfare"

[11] Gary Machado et al, "Indian Chronicles Report" (2020), *EU DisinfoLab,* 09 Dec 2020, accessed 12 Aug 2025, https://www.disinfo.eu/wp-content/uploads/2020/12/Indian-chronicles_FULLREPORT.pdf

[12] Anurag Sharma, "Deepfakes: A Threat to National Security in the Digital Era*, Vivekananda International Foundation*, 11 Jul 2024, accessed 14 Aug 2025, https://www.vifindia.org/article/2024/july/11/Deepfakes-A-Threat-to-National-Security-in-the-Digital-Era

[13] Kania, "China's Strategic Thinking"

[14] Anne-Marie Brady, "China as a Polar Great Power", *Wilson Center,* 18 Aug 2017, accessed 14 Aug 2025, https://www.wilsoncenter.org/book/china-great-polar-power?utm_source=copilot.com

[15] Awasthi, "Pakistan's Information Warfare"

[16] Ibid.

[17] Integrated Defence Staff, "Joint Doctrine of the Indian Armed Forces", *Ministry of Defence, Government of India,* 18 Apr 2017, accessed 15 Aug 2025, https://cms.spacesecurityportal.org/uploads/1718bbb2_cb9c_4ef5_9843_cb670e58afb7_324809bdc3.pdf

[18] Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act and IndiaAI Mission" (2023), *Government of India*, 11 Aug 2023, accessed 15 Aug 2025, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[19] Minhas, "Cognitive Warfare"

[20] The Hindu Bureau, "India has been world teacher from the beginning, says Khuba", *The Hindu*, 20 Feb 2024, accessed 15 Aug 2025, https://www.thehindu.com/news/national/karnataka/india-has-been-world-teacher-from-the-beginning-says-khuba/article67867357.ece

[21] "Integrated Fleet Command–Indian Ocean Region (IFC-IOR Centre)", *Indian Navy*, accessed 15 Aug 2025, https://ifcior.indiannavy.gov.in/

[22] Maritime Gateway, "National Maritime Domain Awareness (NMDA) Project", *Maritime Gateway*, 05 Dec 2022, accessed 16 Aug 2025, https://www.maritimegateway.com/national-maritime-domain-awareness-nmda-project/

[23] Integrated Defence Staff, "Joint Doctrine"

[24] Joseph S Nye, "Soft Power: The Means to Success in World Politics", *PublicAffairs, Harvard University,* Apr 2004, accessed 18 Feb 2026, https://www.wcfia.harvard.edu/publications/soft-power-means-success-world-politics?utm_source=chatgpt.com

[25] MeitY, "IndiaAI Mission and Bhashini"

[26] Pradip R Sagar, "How social media is being used to whip up pro-Khalistan sentiments", *India Today*, 04 Apr 2023, accessed 16 Aug 2025, https://www.indiatoday.in/india-today-insight/story/how-social-media-is-being-used-to-whip-up-pro-khalistan-sentiments-2354415-2023-04-01

[27] Integrated Defence Staff, "Joint Doctrine"

[28] Soumya Awasthi, Abhishek Sharma, "Rethinking India's Cyber Readiness in the Age of Information Warfare"*, Observer Research Foundation,* 17 May 2025, accessed 16 Aug 2025, https://www.orfonline.org

[29] The Times News Network, "Joint Doctrine and Technology Roadmap for Armed Forces Modernization Released", *The Times of India*, 28 Aug 2025, accessed 16 Aug 2025, http://timesofindia.indiatimes.com/articleshow/123551797.cms?utm_source

[30] MeitY, "IndiaAI Mission"

[31] India Development Review, "Unpacking misinformation and what it means for the social sector", *IDR Online*, 17 Dec 2025, accessed 17 Jan 2026, https://idronline.org/article/ecosystem-development/unpacking-misinformation-and-what-it-means-for-the-social-sector/

[32] Minhas, "Cognitive Warfare"

[33] "ACT Marks 10 Years of NATO's Innovation Hub," *NATO Allied Command Transformation (ACT)*, accessed 17 Aug 2025, https://www.act.nato.int/article/act-marks-10-years-of-natos-innovation-hub/?utm_source.

[34] Abhishek Kumar Darbey,"China's Informationalised Combat Capability", *Manohar Parrikar Institute for Defence Studies and Analyses (IDSA)*, 28 Aug 2024, accessed 18 Aug 2025, https://www.idsa.in/publisher/idsa-comments/chinas-informationised-combat-capabilities

[35] Awasthi, Sharma, "Rethinking India's Cyber Readiness"

[36] Neeraj Mahajan, "Cognitive Domain: The Sixth Domain Of Warfare", *DefStrat,* Vol 16 Issue 06; Jan–Feb 2023, accessed 18 Aug 2025, https://www.defstrat.com/magazine_articles/cognitive-domain-the-sixth-domain-of-warfare/